Kaspersky Total Security

Περιεχόμενα

<u>Συχνές ερωτήσεις</u>

<u>Νέα στοιχεία</u>

<u>Απαιτήσεις υλικού και λογισμικού</u>

<u>Συμβατότητα με άλλες εφαρμογές της Kaspersky</u>

<u>Πώς να εγκαταστήσετε την εφαρμογή</u>

Έλεγχος για νεότερη έκδοση της εφαρμογής

Εκκίνηση της εγκατάστασης της εφαρμογής

<u>Ανασκόπηση της Άδειας Χρήσης Τελικού Χρήστη</u>

<u>Δήλωση για το Kaspersky Security Network</u>

Εγκατάσταση της εφαρμογής

<u>Συνιστώμενες ρυθμίσεις</u>

Ολοκλήρωση εγκατάστασης

Ενεργοποίηση της εφαρμογής

<u>Εγγραφή και σύνδεση στο My Kaspersky</u>

Ολοκλήρωση ενεργοποίησης

Σφάλμα εγκατάστασης εφαρμογής σε Windows 7 και Windows Server 2008 R2

<u>Εγκατάσταση της εφαρμογής από τη γραμμή εντολών</u>

<u>Πρώτα βήματα</u>

<u>Πώς να ενημερώσετε την εφαρμογή</u>

Εγκατάσταση πάνω από άλλες εφαρμογές της Kaspersky

<u>Μετάβαση από το Kaspersky Total Security σε άλλες εφαρμογές της Kaspersky</u>

<u>Μετάβαση στο Kaspersky Free όταν έχει λήξει η άδεια χρήσης του Kaspersky Total Security</u>

<u>Μετάβαση στο Kaspersky Free κατά την απεγκατάσταση της δοκιμαστικής έκδοσης του Kaspersky</u> <u>Total Security</u>

<u>Πώς να καταργήσετε την εγκατάσταση της εφαρμογής</u>

Εισαγωγή κωδικού πρόσβασης για την κατάργηση της εφαρμογής

Αποθήκευση του κωδικού ενεργοποίησης

Αποθήκευση δεδομένων για μελλοντική χρήση

<u>Επιβεβαίωση κατάργησης της εφαρμογής</u>

Ολοκλήρωση κατάργησης

<u>Εκχώρηση άδειας χρήσης της εφαρμογής</u>

Πληροφορίες για την Άδεια Χρήσης Τελικού Χρήστη

Πληροφορίες για την άδεια χρήσης

Πληροφορίες για την κατάσταση περιορισμένης λειτουργικότητας

Πληροφορίες για τον κωδικό ενεργοποίησης

Πώς να επαναφέρετε τους κωδικούς ενεργοποίησης

<u>Πληροφορίες για τη συνδρομή</u>

<u>Πώς να αποκτήσετε μια άδεια χρήσης</u>

<u>Πώς να ενεργοποιήσετε την εφαρμογή</u>

<u>Πώς να ανανεώσετε μια άδεια χρήσης</u>

<u>Παροχή δεδομένων</u>

<u>Παροχή δεδομένων υπό τους όρους της Άδειας Χρήσης Τελικού Χρήστη</u>

<u>Παροχή δεδομένων υπό τους όρους της Άδειας Χρήσης Τελικού Χρήστη εντός της επικράτειας της</u> <u>Ευρωπαϊκής Ένωσης, του Ηνωμένου Βασιλείου Μεγάλης Βρετανίας ή από κατοίκους της πολιτείας</u> <u>της Καλιφόρνια</u>

<u>Παροχή δεδομένων στο Kaspersky Security Network</u>

Αποθήκευση δεδομένων στην αναφορά λειτουργίας της εφαρμογής

<u>Αποθήκευση δεδομένων για Τεχνική υποστήριξη</u>

<u>Σχετικά με τη χρήση της εφαρμογής στην Ευρωπαϊκή Ένωση, το Ηνωμένο Βασίλειο, τις ΗΠΑ, τη</u> <u>Βραζιλία ή από κατοίκους της πολιτείας της Καλιφόρνια</u>

<u>Γιατί χρειάζεται το My Kaspersky</u>

<u>Πληροφορίες για τον λογαριασμό My Kaspersky</u>

<u>Πώς να δημιουργήσετε λογαριασμό My Kaspersky</u>

Σχετικά με την απομακρυσμένη διαχείριση της προστασίας του υπολογιστή

Πώς να υλοποιήσετε την απομακρυσμένη διαχείριση της προστασίας του υπολογιστή

<u>Πώς να ρυθμίσετε τη διεπαφή της εφαρμογής</u>

Πώς να αλλάξετε το εικονίδιο της εφαρμογής

Πώς να αλλάξετε το θέμα σχεδίασης της εφαρμογής

<u>Σχετικά με τις ειδοποιήσεις της εφαρμογής</u>

Πώς να ρυθμίσετε τις παραμέτρους ειδοποιήσεων της εφαρμογής

<u>Πώς να αλλάξετε το εικονίδιο της εφαρμογής στην περιοχή ειδοποιήσεων ανάλογα με την κατάσταση</u> <u>της εφαρμογής</u>

<u>Τρόπος προστασία της πρόσβασης στις λειτουργίες διαχείρισης του Kaspersky Total Security με</u> χ<u>ρήση κωδικού πρόσβασης</u>

<u>Πώς να επιταχύνετε την απόδοση του υπολογιστή</u>

<u>Αξιολόγηση της κατάστασης προστασίας του υπολογιστή και επίλυση ζητημάτων ασφάλειας</u>

Να ενημερώσετε τις βάσεις δεδομένων και τις λειτουργικές μονάδες της εφαρμογής

<u>Πληροφορίες σχετικά με τις ενημερώσεις βάσεων δεδομένων και λειτουργικών μονάδων της εφαρμογής</u>

<u>Πώς να ξεκινήσετε την ενημέρωση των βάσεων δεδομένων και των λειτουργικών μονάδων της</u> εφαρμογής

<u>Σάρωση του υπολογιστή</u>

Πώς να εκτελέσετε μια Πλήρη σάρωση

<u>Πώς να εκτελέσετε μια Προσαρμοσμένη σάρωση</u>

<u>Πώς να εκτελέσετε μια Γρήγορη σάρωση</u>

Πώς να εκτελέσετε μια σάρωση αφαιρούμενης μονάδας δίσκου

Πώς να εκτελέσετε μια σάρωση αρχείου ή φακέλου μενού περιβάλλοντος

Πώς να ενεργοποιήσετε ή να απενεργοποιήσετε μια σάρωση παρασκηνίου

<u>Πώς να δημιουργήσετε ένα πρόγραμμα σάρωσης</u>

<u>Πώς να αναζητήσετε τρωτά σημεία σε εφαρμογές που είναι εγκατεστημένες στον υπολογιστή σας</u>

Σάρωση αρχείων στον χώρο αποθήκευσης στο cloud στο OneDrive

Τρόπος επαναφοράς ενός αρχείου που διαγράφηκε ή απολυμάνθηκε από την εφαρμογή

Πώς να κάνετε ανάκτηση του λειτουργικού συστήματος μετά από μόλυνση

Ανάκτηση του λειτουργικού συστήματος μετά από μόλυνση

<u>Αντιμετώπιση προβλημάτων του λειτουργικού συστήματος χρησιμοποιώντας τον Οδηγό</u> <u>αντιμετώπισης προβλημάτων των Microsoft Windows</u>

Ανάκτηση έκτακτης ανάγκης του λειτουργικού συστήματος

<u>Προστασία email</u>

Διαμόρφωση Προστασίας email από ιούς

<u>Αποκλεισμός ανεπιθύμητων email (spam)</u>

<u>Προστασία προσωπικών δεδομένων στο Διαδίκτυο</u>

Σχετικά με την προστασία των προσωπικών δεδομένων στο Διαδίκτυο

<u>Πληροφορίες για το Πληκτρολόγιο οθόνης</u>

<u>Πώς να ανοίξετε το πληκτρολόγιο οθόνης</u>

Πώς να διαμορφώσετε την εμφάνιση του εικονιδίου του Πληκτρολογίου οθόνης

<u>Πληροφορίες σχετικά με την προστασία δεδομένων που εισάγονται από το πληκτρολόγιο του</u> <u>υπολογιστή</u>

<u>Τρόπος ρύθμισης των παραμέτρων προστασίας των δεδομένων που εισάγονται από το</u> <u>πληκτρολόγιο του υπολογιστή</u>

<u>Έλεγχος δικτυακού τόπου ως προς την ασφάλεια</u>

Τρόπος αλλαγής των ρυθμίσεων κρυπτογραφημένων συνδέσεων

<u>Πληροφορίες για την ασφαλή σύνδεση σε δίκτυα Wi-Fi</u>

<u>Τρόπος εκτέλεσης του Kaspersky VPN Secure Connection</u>

<u>Διαμόρφωση ειδοποιήσεων σχετικά με τα τρωτά σημεία σε δίκτυα Wi-Fi</u>

Προστασία οικονομικών συναλλαγών και διαδικτυακών αγορών

Πληροφορίες για την προστασία οικονομικών συναλλαγών και διαδικτυακών αγορών

Τρόπος αλλαγής των ρυθμίσεων των Ασφαλών τραπεζικών συναλλαγών

<u>Πώς να ρυθμίσετε τις παραμέτρους της λειτουργίας Ασφαλείς τραπεζικές συναλλαγές για έναν</u> συγκεκριμένο δικτυακό τόπο

Τρόπος αποστολής σχολίων σχετικά με Ασφαλείς τραπεζικές συναλλαγές

<u>Έναρξη του Kaspersky Password Manager</u>

<u>Προστασία παρακολούθησης στο web</u>

Πληροφορίες σχετικά με την Ιδιωτική περιήγηση

Αποκλεισμός συλλογής δεδομένων

Να επιτρέπεται η συλλογή δεδομένων σε όλους τους δικτυακούς τόπους

Να επιτραπεί η συλλογή δεδομένων ως εξαίρεση

Προβολή αναφοράς για προσπάθειες συλλογής δεδομένων

Διαχείριση του στοιχείου Ιδιωτική περιήγηση σε ένα πρόγραμμα περιήγησης

<u>Προστασία προγράμματος Anti-Banner κατά την περιήγηση σε δικτυακούς τόπους</u>

<u>Πληροφορίες για το Πρόγραμμα Anti-Banner</u>

<u>Πώς να ενεργοποιήσετε το στοιχείο Πρόγραμμα Anti-Banner</u>

Να αποκλειστούν τα διαφημιστικά πλαίσια

Να επιτρέπονται τα διαφημιστικά πλαίσια

<u>Πώς να ρυθμίσετε τα φίλτρα στο πρόγραμμα Anti-Banner</u>

<u>Τρόπος διαχείρισης του Προγράμματος Anti-Banner στο πρόγραμμα περιήγησης</u>

<u>Προστασία της Webcam</u>

<u>Σχετικά με την πρόσβαση εφαρμογών στην webcam</u>

<u>Τρόπος αλλαγής των ρυθμίσεων πρόσβασης εφαρμογών στη webcam</u>

<u>Πώς να επιτρέψετε την πρόσβαση των εφαρμογών στην webcam</u>

<u>Προστασία για παιδιά</u>

<u>Σχετικά με την προστασία των παιδιών με χρήση του Kaspersky Safe Kids</u>

<u>Τρόπος εκτέλεσης του Kaspersky Safe Kids</u>

<u>Χρήση του Kaspersky Safe Kids</u>

Χειρισμός άγνωστων εφαρμογών

Έλεγχος αξιοπιστίας εφαρμογής

Έλεγχος των δραστηριοτήτων εφαρμογών στον υπολογιστή και στο δίκτυο

Τρόπος αλλαγής των ρυθμίσεων του Ελέγχου εφαρμογών

<u>Πληροφορίες σχετικά με την προστασία μιας ροής ήχου που προέρχεται από συσκευές εγγραφής</u> <u>ήχου</u>

Τρόπος αλλαγής των ρυθμίσεων προστασίας ροής ήχου

Τρόπος αλλαγής των ρυθμίσεων της Διαχείρισης εφαρμογών

<u>Ενημέρωση εγκατεστημένων εφαρμογών</u>

<u>Πληροφορίες για την Ενημέρωση λογισμικού</u>

<u>Τρόπος αλλαγής των ρυθμίσεων της Ενημέρωσης λογισμικού</u>

Αναζήτηση για ενημερώσεις της εφαρμογής

Πώς να ρυθμίσετε τις παραμέτρους της λειτουργίας αναζήτησης ενημερώσεων

<u>Προβολή της λίστας ενημερώσεων των εφαρμογών</u>

<u>Κατάργηση ενημέρωσης ή εφαρμογής από τη λίστα εξαιρέσεων</u>

Κατάργηση μη συμβατών εφαρμογών

<u>Σχετικά με την κατάργηση μη συμβατών εφαρμογών</u>

Πώς να καταργήσετε την εγκατάσταση των μη συμβατών εφαρμογών

<u>Εκκαθάριση λογισμικού υπολογιστή</u>

<u>Σχετικά με την Εκκαθάριση λογισμικού υπολογιστή</u>

<u>Πώς να εκκινήσετε χειροκίνητα μια ανάλυση αντικειμένων</u>

<u>Πώς να ρυθμίσετε τις παραμέτρους σε προγραμματισμένη ανάλυση</u>

<u>Πώς να επιλέξετε κατηγορίες αντικειμένων για ανάλυση</u>

<u>Κατηγορίες αντικειμένων που εντοπίστηκαν</u>

<u>Προβολή της λίστας εντοπισμένων αντικειμένων</u>

<u>Προβολή της λίστας εξαιρέσεων</u>

<u>Τρόπος αποστολής δεδομένων σχετικά με παράθυρο εφαρμογής ή προγράμματος περιήγησης στην</u> <u>Kaspersky</u>

<u>Καταστροφέας αρχείων</u>

<u>Καθαρισμός μη χρησιμοποιούμενων δεδομένων</u>

<u>Πληροφορίες για τον καθαρισμό μη χρησιμοποιούμενων δεδομένων</u>

<u>Καθαρισμός μη χρησιμοποιούμενων δεδομένων</u>

Δημιουργία αντιγράφων ασφαλείας

<u>Σχετικά με τη δημιουργία αντιγράφων ασφαλείας</u>

<u>Πώς να δημιουργήσετε μια εργασία δημιουργίας αντιγράφων ασφαλείας</u>

<u>Βήμα 1. Επιλογή αρχείων</u>

<u>Βήμα 2. Επιλογή φακέλων για δημιουργία αντιγράφων ασφαλείας</u>

Βήμα 3. Επιλογή τύπων αρχείων για δημιουργία αντιγράφων ασφαλείας

<u>Βήμα 4. Επιλογή χώρου αποθήκευσης αντιγράφων ασφαλείας</u>

<u>Βήμα 5. Δημιουργία χρονοδιαγράμματος δημιουργίας αντιγράφων ασφαλείας</u>

<u>Βήμα 6. Ρύθμιση κωδικού πρόσβασης για την προστασία των αντιγράφων ασφαλείας</u>

<u>Βήμα 7. Ρυθμίσεις χώρου αποθήκευσης εκδόσεων αρχείων</u>

Βήμα 8. Εισαγωγή ονόματα εργασίας δημιουργίας αντιγράφων ασφαλείας

<u> Βήμα 9. Ολοκλήρωση Οδηγού</u>

Πώς να ξεκινήσετε μια εργασία δημιουργίας αντιγράφων ασφαλείας

Επαναφορά δεδομένων από αντίγραφο ασφαλείας

Επαναφορά δεδομένων από τον χώρο αποθήκευσης FTP

Επαναφορά δεδομένων από αντίγραφο ασφαλείας με χρήση του Kaspersky Restore Utility

<u>Σχετικά με τον online χώρο αποθήκευσης</u>

<u>Πώς να ενεργοποιήσετε τον online χώρο αποθήκευσης</u>

<u>Αποθήκευση δεδομένων σε θαλάμους δεδομένων</u>

Σχετικά με τον θάλαμο δεδομένων

<u>Πώς να μετακινήσετε αρχεία στο θάλαμο δεδομένων</u>

Πώς να αποκτήσετε πρόσβαση στα αρχεία που είναι αποθηκευμένα σε θάλαμο δεδομένων

Τρόπος δέσμευσης πόρων του λειτουργικού συστήματος για παιχνίδια υπολογιστή

<u>Πώς να βελτιστοποιήσετε το φορτίο στο λειτουργικό σύστημα λόγω της εκτέλεσης εργασιών του</u> <u>Kaspersky Total Security</u>

Τρόπος κατάργησης ιχνών δραστηριότητας στον υπολογιστή

<u>Τρόπος παύσης και συνέχισης της προστασίας του υπολογιστή</u>

Τρόπος επαναφοράς των προεπιλεγμένων ρυθμίσεων της εφαρμογής

Τρόπος προβολής της αναφοράς λειτουργίας της εφαρμογής

Τρόπος εφαρμογής των ρυθμίσεων εφαρμογών σε άλλο υπολογιστή

<u>Συμμετοχή στο Kaspersky Security Network</u>

<u>Πώς να ενεργοποιήσετε ή να απενεργοποιήσετε τη συμμετοχή στο Kaspersky Security Network</u>

<u>Πώς να ελέγξετε τη σύνδεση με το Kaspersky Security Network</u>

<u>Προστασία με χρήση λειτουργίας αναπαράστασης υλικού</u>

<u>Σχετικά με την προστασία κατά τη χρήση εικονικοποίησης υλικού</u>

Πώς να ενεργοποιήσετε την προστασία με χρήση εικονικοποίησης υλικού

<u>Προστασία χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface (AMSI)</u>

<u>Σχετικά με την προστασία χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface</u>

<u>Πώς να ενεργοποιήσετε την προστασία χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface</u>

<u>Πώς να εξαιρέσετε μια δέσμη ενεργειών από τη σάρωση χρησιμοποιώντας τη λειτουργία</u> <u>Antimalware Scan Interface</u>

<u>Χρήση της εφαρμογής από τη γραμμή εντολών</u>

<u>Αξιολόγηση του Kaspersky Total Security</u>

<u>Επικοινωνία με την Τεχνική υποστήριξη</u>

<u>Τρόπος λήψης τεχνικής υποστήριξης</u>

<u>Τεχνική υποστήριξη μέσω τηλεφώνου</u>

<u>Τεχνική υποστήριξη μέσω του My Kaspersky</u>

<u>Συλλογή πληροφοριών για τεχνική υποστήριξη</u>

Σχετικά με τα περιεχόμενα και την αποθήκευση των αρχείων δεδομένων υπηρεσίας

<u>Πώς να ενεργοποιήσετε την ιχνηλάτηση</u>

<u>Περιορισμοί και προειδοποιήσεις</u>

<u>Άλλες πηγές ενημέρωσης σχετικά με την εφαρμογή</u>

<u>Γλωσσάριο</u>

<u>Hypervisor</u>

Kaspersky Security Network (KSN)

<u>Phishing</u>

<u>Rootkit</u>

<u>Spam (ανεπιθύμητη αλληλογραφία)</u>

<u>Άγνωστος ιός</u>

<u>Αντικείμενα εκκίνησης</u>

<u>Αξιόπιστη διεργασία</u>

<u>Αποκλεισμός αντικειμένου</u>

Βάσεις δεδομένων προστασίας από ιούς

<u>Βάση δεδομένων κακόβουλων διευθύνσεων ιστού</u>

<u>Βάση δεδομένων των διευθύνσεων ιστού phishing</u>

<u>Δέσμη ενεργειών</u>

Δημιουργία αντιγράφων ασφαλείας

<u>Διακομιστές ενημέρωσης της Kaspersky</u>

<u>Διάρκεια ισχύος της άδειας χρήσης</u>

<u>Ενεργοποίηση της εφαρμογής</u>

<u>Ενημέρωση</u>

<u>Επίπεδο απειλών</u>

<u>Επίπεδο ασφαλείας</u>

<u>Εργασία</u>

<u>Θάλαμος δεδομένων</u>

<u>Ιός</u>

<u>Ίχνη</u>

<u>Καραντίνα</u>

Καταγραφέας πληκτρολόγησης (keylogger)

<u>Κωδικός ενεργοποίησης</u>

<u>Μάσκα αρχείου</u>

<u>Μη συμβατή εφαρμογή</u>

Μολυσμένο αντικείμενο

<u>Μονάδες της εφαρμογής</u>

<u>Ομάδα αξιοπιστίας</u>

Πακέτο ενημέρωσης

<u>Πιθανό μήνυμα spam</u>

Πιθανώς μολυσμένο αντικείμενο

Πρόγραμμα εκμετάλλευσης

<u>Πρόγραμμα ευρετικής ανάλυσης</u>

<u>Προστατευμένο πρόγραμμα περιήγησης</u>

<u>Πρωτόκολλο</u>

<u>Ρυθμίσεις εργασιών</u>

<u>Σάρωση κυκλοφορίας δικτύου</u>

<u>Στοιχεία προστασίας</u>

<u>Συμπιεσμένο αρχείο</u>

<u>Τεχνολογία iChecker</u>

<u>Τομέας εκκίνησης δίσκων</u>

<u>Τρωτό σημείο</u>

<u>Ψευδές θετικό</u>

<u>Ψηφιακή υπογραφή</u>

<u>Πληροφορίες σχετικά με κώδικα τρίτων</u>

<u>Επισημάνσεις για τα σήματα κατατεθέντα</u>

<u>Δικαιώματα</u>

Συχνές ερωτήσεις



Πρώτα βήματα

<u>Πώς να εγκαταστήσετε μια νέα</u> <u>έκδοση της εφαρμογής πάνω σε</u> <u>μια υπάρχουσα</u>

<u>Πώς να διαμορφώσετε τις</u> <u>προτεινόμενες ρυθμίσεις της</u> <u>εφαρμογής κατά την εγκατάσταση</u>

<u>Πώς να ενεργοποιήσετε την</u> <u>εφαρμογή</u>

<u>Πώς να δημιουργήσετε</u> <u>λογαριασμό My Kaspersky</u>



Αναφορές και ενημερώσεις

<u>Τρόπος προβολής της</u> <u>αναφοράς λειτουργίας της</u> <u>εφαρμογής</u>

<u>Πώς να ξεκινήσετε την</u> <u>ενημέρωση των βάσεων</u> <u>δεδομένων και των</u> <u>λειτουργικών μονάδων της</u> <u>εφαρμογής</u> <u>Πώς να διαχειριστείτε την</u> <u>προστασία των συσκευών σας από</u> <u>απόσταση</u>



Προστασία υπολογιστή

<u>Τρόπος προβολής πληροφοριών</u> <u>σχετικά με την κατάσταση</u> <u>προστασίας του υπολογιστή</u>

<u>Πώς να κάνετε ανάκτηση του</u> <u>λειτουργικού συστήματος μετά</u> <u>από μόλυνση</u>

<u>Πώς να ξεκινήσετε μια πλήρη</u> <u>σάρωση του υπολογιστή για ιούς</u>

<u>Πώς να ξεκινήσετε μια γρήγορη</u> <u>σάρωση του υπολογιστή για ιούς</u>

<u>Πώς να εκτελέσετε μια σάρωση για</u> <u>τρωτά σημεία</u>

<u>Πώς να ρυθμίσετε τη σάρωση στις</u> <u>προστατευμένες τοποθεσίες web</u>



Προστασία αγορών και μεταφορών χρημάτων

<u>Πώς να προστατεύσετε τις online</u> <u>αγορές σας</u>

<u>Πώς να ρυθμίσετε τις παραμέτρους</u> <u>της λειτουργίας Ασφαλείς</u> <u>τραπεζικές συναλλαγές</u>

<u>Πώς να ρυθμίσετε τις παραμέτρους</u> <u>της λειτουργίας Ασφαλείς</u> <u>τραπεζικές συναλλαγές για έναν</u> <u>συγκεκριμένο δικτυακό τόπο</u>



Προστασία για παιδιά

<u>Πώς να προστατεύσετε τα παιδιά</u> <u>σας από απειλές στον</u> <u>κυβερνοχώρο</u>



Βελτιστοποίηση λειτουργικού συστήματος

<u>Πώς να καθαρίσετε τον</u> <u>υπολογιστή από σπάνια</u> <u>χρησιμοποιούμενες εφαρμογές</u> <u>και επεκτάσεις προγράμματος</u> <u>περιήγησης</u>

<u>Πώς να βελτιστοποιήσετε την</u> <u>εφαρμογή για παιχνίδια στον</u> <u>υπολογιστή</u>

<u>Τρόπος εφαρμογής των</u> <u>ρυθμίσεων εφαρμογών σε άλλο</u> <u>υπολογιστή</u>



Προστασία προσωπικών δεδομένων

<u>Πώς να αποτρέψετε τη συλλογή</u> <u>δεδομένων για εσάς από</u> <u>τοποθεσίες web</u>

<u>Πώς να εκκινήσετε το</u> <u>Kaspersky Password Manager</u> <u>Πώς να κάνετε λήψη και</u> <u>εγκατάσταση του Kaspersky Safe</u> <u>Kids και να προστατέψετε τα</u> <u>παιδιά σας</u>

Νέα στοιχεία

Η Kaspersky δημιούργησε μια ειδική έκδοση της εφαρμογής για κατοίκους της πολιτείας της Καλιφόρνια των ΗΠΑ. Εάν είστε κάτοικος της πολιτείας της Καλιφόρνια των ΗΠΑ. Εάν είστε κάτοικος της πολιτείας της καλιφόρνια των ΗΠΑ, πρέπει να κάνετε λήψη και εγκατάσταση <u>αυτής της έκδοσης της εφαρμογής</u> .

Οι ακόλουθες νέες δυνατότητες και βελτιώσεις εισάγονται στο Kaspersky Total Security:

- Στοιχείο Βελτιωμένη προστασία από ιούς στο Web:
 - Βελτιωμένα κείμενα ειδοποιήσεων που προειδοποιούν σχετικά με προσπάθειες επίσκεψης σε δικτυακούς τόπους phishing ή πιθανού phishing.
 - Όταν η σάρωση κυκλοφορίας δικτύου HTTPS είναι απενεργοποιημένη, η επέκταση Kaspersky Protection συνεχίζει να παρέχει προστασία.
- Βελτιωμένη αλληλεπίδραση μεταξύ του χρήστη και της Τεχνικής Υποστήριξης. Η εφαρμογή διαθέτει πλέον σύνδεση για συνομιλία με την Τεχνική Υποστήριξη (δεν διατίθεται σε ορισμένες εκδόσεις της εφαρμογής).
- Βελτιωμένη ειδοποίηση σχετικά με την πληκτρολόγηση κωδικού ενεργοποίησης ο οποίος χρησιμοποιείται ήδη.
- Επιδιορθώθηκε ένα πρόβλημα ύπαρξης τρωτών σημείων που εμφανιζόταν συνήθως κατά τη δημιουργία αρχείων του προγράμματος περιήγησης Mozilla Firefox.
- Το εικονίδιο του προγράμματος εγκατάστασης ενημερώθηκε σύμφωνα με το νέο στυλ της εμπορικής επωνυμίας.
- Βελτιωμένο παράθυρο λήξης άδειας χρήσης.
- Υπάρχει πλέον δυνατότητα μετάβασης στην έκδοση light του My Kaspersky απευθείας από την εφαρμογή.
- Υπάρχει πλέον δυνατότητα απόκρυψης του παραθύρου σάρωσης αφαιρούμενης μονάδας δίσκου.

- Προσθήκη υποστήριξης για το Microsoft Windows 10 21Η1.
- Επιδιορθώθηκε το πρόβλημα ύπαρξης τρωτών σημείων που αφορούσε την αυθαίρετη διαγραφή αρχείων κατά την αποθήκευση της αναφοράς λειτουργίας της εφαρμογής για την Τεχνική Υποστήριξη.
- Επιδιορθώθηκε το πρόβλημα ύπαρξης τρωτών σημείων που αφορούσε την αυθαίρετη διαγραφή αρχείων κατά τη διαγραφή δεδομένων υπηρεσίας και αναφορών λειτουργίας της εφαρμογής.

<u>Λειτουργίες που καταργήθηκαν στην τρέχουσα και στις προηγούμενες εκδόσεις της</u> <u>εφαρμογής</u> ?

Kaspersky Total Security 2021:

- Καταργήθηκε η δυνατότητα Application Advisor.
- Καταργήθηκε η δυνατότητα Προστασία Προγραμμάτων ΙΜ.
- Καταργήθηκε η Λειτουργία Αξιόπιστες εφαρμογές.
- Καταργήθηκε η δυνατότητα αναζήτησης τρωτών σημείων στο λειτουργικό σύστημα.
- Περιορισμένη υποστήριξη για το παλιό πρόγραμμα περιήγησης Microsoft Edge.
 Αυτό το πρόγραμμα περιήγησης δεν υποστηρίζει πλέον τις δυνατότητες Ασφαλής καταχώρηση δεδομένων και Προστατευμένο πρόγραμμα περιήγησης.
 Εξακολουθείτε να προστατεύεστε κατά τη σάρωση της κυκλοφορίας.
- Διακοπή υποστήριξης για την επέκταση Kaspersky Protection στο πρόγραμμα περιήγησης Internet Explorer.
- Καταργήθηκε η δυνατότητα αποθήκευσης αντιγράφων ασφαλείας σε διακομιστή FTP.

Kaspersky Total Security 2020:

Καταργήθηκε το στοιχείο Γονικός Έλεγχος. Το Kaspersky Safe Kids προσφέρεται ως αντικατάστασή του.

Kaspersky Total Security 2019:

 Το στοιχείο Διαχείριση εφαρμογών δεν παρέχει πλέον τη δυνατότητα Έλεγχος αλλαγών συστήματος για την παρακολούθηση των ρυθμίσεων του λειτουργικού συστήματος.

- Το στοιχείο Γονικός Έλεγχος δεν παρέχει πλέον έλεγχο της ανταλλαγής μηνυμάτων στα κοινωνικά δίκτυα.
- Οι ακόλουθες δυνατότητες έχουν καταργηθεί από το στοιχείο Πρόγραμμα Anti-Spam:
 - Ενοποίηση με το Microsoft Office Outlook και το Outlook Express.
 - Διαχείριση μιας προσαρμοσμένης βάσης δεδομένων spam.
 - Σάρωση μηνυμάτων που μεταδίδονται μέσω του πρωτοκόλλου Exchange MAPI.
 - Προσθήκη διεύθυνσης αποστολέα στη λίστα των επιτρεπόμενων διευθύνσεων κατά τη διάρκεια της Εκπαίδευσης Προγράμματος Anti-Spam.
 - Ενέργειες κατά την ανίχνευση μηνυμάτων spam: μετακίνηση, αντιγραφή, διαγραφή και παράβλεψη.

Εάν θέλετε να συνεχίσετε να χρησιμοποιείτε κάποιες από τις καταργημένες λειτουργίες, μπορείτε να <u>επιστρέψετε στην προηγούμενη έκδοση της εφαρμογής</u>.

Απαιτήσεις υλικού και λογισμικού

Γενικές απαιτήσεις

- 1500 MB ελεύθερος χώρος στον σκληρό δίσκο
- Επεξεργαστής που υποστηρίζει το σετ οδηγιών SSE2
- Πρόσβαση στο Διαδίκτυο (για εγκατάσταση και ενεργοποίηση της εφαρμογής, για χρήση του Kaspersky Security Network και για ενημέρωση των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής)
- Microsoft Windows Installer 4.5 ή νεότερη έκδοση
- Microsoft .NET Framework 4 ή νεότερη έκδοση
- Η προστασία πρόσβασης στην webcam παρέχεται μόνο για <u>συμβατά μοντέλα webcam</u> 🗷

Απαιτήσεις λειτουργικού συστήματος

Λειτουργικό σύστημα	CPU	RAM
Microsoft Windows 10 Home (εκδόσεις: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1)	1 GHz ή υψηλότερη	1 GB (για λειτουργικά συστήματα 32 bit) ή 2 GB (για λειτουργικά συστήματα 64 bit)
Microsoft Windows 10 Enterprise (εκδόσεις: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1)		
Microsoft Windows 10 Pro (εκδόσεις: 1507, 1511, 1607, 1703, 1709, 1803, 1809, 1903, 1909, 2004, 20H2, 21H1)		
Microsoft Windows 8.1 (Service Pack 0 ή μεταγενέστερη έκδοση, Windows 8.1 Update)	1 GHz ή υψηλότερη	1 GB (για λειτουργικά συστήματα 32 bit) ή 2 GB (για λειτουργικά συστήματα 64 bit)
Microsoft Windows 8.1 Pro (Service Pack 0 ή μεταγενέστερη έκδοση, Windows 8.1 Update)		
Microsoft Windows 8.1 Enterprise (Service Pack 0 ή μεταγενέστερη έκδοση, Windows 8.1 Update)		
Microsoft Windows 8 (Service Pack 0 ή μεταγενέστερη έκδοση)	1 GHz ή υψηλότερη	1 GB (για λειτουργικά συστήματα 32 bit) ή 2 GB (για λειτουργικά συστήματα 64 bit)
Microsoft Windows 8 Pro (Service Pack 0 ή μεταγενέστερη έκδοση)		
Microsoft Windows 8 Enterprise (Service Pack 0 ή μεταγενέστερη έκδοση)		
Microsoft Windows 7 Starter (Service Pack 1 ή μεταγενέστερη έκδοση)	1 GHz ή υψηλότερη	1 GB (για λειτουργικά συστήματα 32 bit) ή 2 GB (για λειτουργικά συστήματα 64 bit)
Microsoft Windows 7 Home Basic (Service Pack 1 ή μεταγενέστερη έκδοση)		
Microsoft Windows 7 Home Premium (Service Pack 1 ή μεταγενέστερη έκδοση)		
Microsoft Windows 7 Professional (Service Pack 1 ή μεταγενέστερη έκδοση)		

Microsoft Windows 7 Ultimate (Service Pack 1 ή μεταγενέστερη έκδοση)

Για τη λειτουργία των στοιχείων προστασίας Προστασία από ιούς στο Web, Πρόγραμμα Anti-Banner και Ασφαλείς τραπεζικές συναλλαγές, πρέπει να εκτελείται η υπηρεσία Μηχανισμός βασικού φιλτραρίσματος στο λειτουργικό σύστημα.

Υποστήριξη προγράμματος περιήγησης

Τα ακόλουθα προγράμματα περιήγησης υποστηρίζουν την εγκατάσταση της επέκτασης Kaspersky Protection:

- Microsoft Edge 77.x 88.x που βασίζεται στο Chromium,
- Mozilla Firefox εκδόσεις 52.x 84.x,
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x,
- Google Chrome εκδόσεις 48.x 88.x.

Τα ακόλουθα προγράμματα περιήγησης υποστηρίζουν Πληκτρολόγιο οθόνης και σάρωση κρυπτογραφημένων συνδέσεων:

- Microsoft Edge 77.x 88.x που βασίζεται στο Chromium,
- Mozilla Firefox εκδόσεις 52.x 84.x,
- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x,
- Google Chrome 48.x 88.x.

Τα ακόλουθα προγράμματα περιήγησης υποστηρίζουν τη λειτουργία Προστατευμένο πρόγραμμα περιήγησης:

- Microsoft Internet Explorer 8.0, 9.0, 10.0, 11.0,
- Microsoft Edge 77.x 88.x που βασίζεται στο Chromium,
- Mozilla Firefox εκδόσεις 52.x 84.x,

- Mozilla Firefox ESR 52.x, 60.x, 68.x, 78.x,
- Google Chrome 48.x 88.x,
- Yandex Browser 18.3.1 20.12.0 (με <u>περιορισμούς</u>).

Οι νεότερες εκδόσεις των προγραμμάτων περιήγησης μπορούν να υποστηριχθούν εάν το πρόγραμμα περιήγησης υποστηρίζει την αντίστοιχη τεχνολογία.

Το Kaspersky Total Security υποστηρίζει το Google Chrome και το Mozilla Firefox σε λειτουργικά συστήματα 32-bit και 64-bit.

Απαιτήσεις για tablet

- Microsoft Windows 8, Microsoft Windows 8.1, Microsoft Windows 10
- Επεξεργαστής Intel Celeron με ταχύτητα ρολογιού 1,66 GHz ή ταχύτερη
- 1000 MB ελεύθερη μνήμη RAM

Απαιτήσεις για netbook

- Επεξεργαστής Atom 1,60 GHz ή ταχύτερος
- 1024 MB ελεύθερη μνήμη RAM
- Οθόνη 10.1 ιντσών με ανάλυση οθόνης 1024x600
- Επεξεργαστής γραφικών Intel GMA 950 ή νεότερος

Οι απαιτήσεις του Kaspersky Password Manager είναι διαθέσιμες στα <u>αρχεία βοήθειας για</u> <u>αυτή την εφαρμογή</u>.

Συμβατότητα με άλλες εφαρμογές της Kaspersky

Το Kaspersky Total Security είναι συμβατό με τις εξής εφαρμογές της Kaspersky:

- Kaspersky Safe Kids 1.5
- Kaspersky Password Manager 9.2

- Kaspersky Software Updater 2.1
- Kaspersky Virus Removal Tool 2015, 2020
- Kaspersky VPN Secure Connection 4.0, 5.0, 5.1, 5.2, 5.3

Πώς να εγκαταστήσετε την εφαρμογή

Η εγκατάσταση του Kaspersky Total Security στον υπολογιστή σας γίνεται αλληλεπιδραστικά, με τη χρήση του Οδηγού εγκατάστασης και κατάργησης.

Ο Οδηγός αποτελείται από μια σειρά σελίδων (βήματα), στις οποίες μπορείτε να περιηγηθείτε με τα κουμπιά **Πίσω** και **Επόμενο**. Για να κλείσετε τον Οδηγό αφού ολοκληρωθεί, κάντε κλικ στο κουμπί **Ολοκληρώθηκε**. Για να διακόψετε τη δραστηριότητα του Οδηγού σε οποιοδήποτε βήμα της εγκατάστασης, απλώς κλείστε το παράθυρο του Οδηγού.

Ο αριθμός και η ακολουθία βημάτων στον Οδηγό εξαρτάται από την περιοχή όπου εγκαθιστάτε την εφαρμογή. Σε <u>ορισμένες περιοχές</u>, ο Οδηγός σάς ζητά να αποδεχτείτε πρόσθετες συμφωνίες σχετικά με τον τρόπο επεξεργασίας των προσωπικών σας δεδομένων και να επιβεβαιώσετε ότι είστε τουλάχιστον 16 ετών.

Αν η εφαρμογή θα χρησιμοποιηθεί για την προστασία περισσότερων από ενός υπολογιστές (ο μέγιστος επιτρεπόμενος αριθμός εξαρτάται από την Άδεια Χρήσης Τελικού Χρήστη που διαθέτετε), η διαδικασία εγκατάστασης θα είναι πανομοιότυπη για όλους τους υπολογιστές.

Για να εγκαταστήσετε το Kaspersky Total Security στον υπολογιστή σας,

Στο CD εγκατάστασης, εκτελέστε το αρχείο με την επέκταση .exe.

Στη συνέχεια, η εφαρμογή εγκαθίσταται χρησιμοποιώντας τον τυπικό Οδηγό εγκατάστασης και κατάργησης.

Σε ορισμένες περιοχές, το CD εγκατάστασης δεν περιλαμβάνει το πακέτο εγκατάστασης της εφαρμογής. Το CD εγκατάστασης περιέχει μόνο το αρχείο αυτόματης εκτέλεσης. Όταν εκτελείται αυτό το αρχείο, ανοίγει το παράθυρο λήψης της εφαρμογής.

<u>Πώς εγκαθιστάτε την εφαρμογή χρησιμοποιώντας το αρχείο autorun</u> ව

Για να εγκαταστήσετε το Kaspersky Total Security χρησιμοποιώντας το αρχείο αυτόματης εκτέλεσης:

Κάντε κλικ στο κουμπί Λήψη και Εγκατάσταση στο παράθυρο λήψης της εφαρμογής.

Κάνοντας κλικ στο κουμπί **Λήψη και Εγκατάσταση** στέλνετε πληροφορίες σχετικά με την έκδοση του λειτουργικού σας συστήματος στο Kaspersky.

2. Σε περίπτωση αποτυχίας της λήψης, κάντε κλικ στη σύνδεση Λήψη και εγκατάσταση χειροκίνητα από τον δικτυακό τόπο, η οποία θα σας μεταφέρει σε έναν δικτυακό τόπο από τον οποίο μπορείτε να πραγματοποιήσετε χειροκίνητη λήψη της εφαρμογής.

Στη συνέχεια, η εφαρμογή εγκαθίσταται χρησιμοποιώντας τον τυπικό Οδηγό εγκατάστασης και κατάργησης.

Για να εγκαταστήσετε το Kaspersky Total Security, μπορείτε επίσης να πραγματοποιήσετε λήψη του πακέτου εγκατάστασης το Διαδίκτυο. Σε αυτήν την περίπτωση, ο Οδηγός θα εμφανίσει επιπλέον βήματα εγκατάστασης για ορισμένες γλώσσες τοπικής προσαρμογής.

Μαζί με την εφαρμογή εγκαθίστανται και πρόσθετα για τα προγράμματα περιήγησης για να διασφαλιστεί η ασφαλής περιήγησή σας στο Διαδίκτυο.

Όταν εκτελέσετε εφαρμογές εγγραφής ή αναπαραγωγής ήχου και βίντεο για πρώτη φορά από την εγκατάσταση του Kaspersky Total Security, η εγγραφή ή αναπαραγωγή του ήχου και του βίντεο μπορεί να διακοπεί. Αυτό είναι απαραίτητο για την ενεργοποίηση της <u>λειτουργίας που ελέγχει την πρόσβαση από τις εφαρμογές στις</u> <u>συσκευές εγγραφής ήχου</u>. Η υπηρεσία συστήματος που ελέγχει το υλικό ήχου επανεκκινείται όταν το Kaspersky Total Security εκτελείται για πρώτη φορά. Το Kaspersky Total Security εγκαθίσταται μαζί με την εφαρμογή Kaspersky VPN Secure Connection με σκοπό τη δημιουργία ασφαλών συνδέσεων μέσω του Virtual Private Network (VPN: Εικονικό ιδιωτικό δίκτυο). Μπορείτε να καταργήσετε το Kaspersky VPN Secure Connection χωριστά από το Kaspersky Total Security. Εάν η χρήση του VPN απαγορεύεται στη χώρα σας, το Kaspersky VPN Secure Connection δεν θα εγκατασταθεί.

Έλεγχος για νεότερη έκδοση της εφαρμογής

Πριν από την εγκατάσταση, ο Οδηγός εγκατάστασης αναζητά στους διακομιστές ενημέρωσης της Kaspersky κάποια τυχόν νεότερη έκδοση του Kaspersky Total Security.

Εάν ο Οδηγός δεν εντοπίσει κάποια νεότερη έκδοση της εφαρμογής στους διακομιστές ενημέρωσης της Kaspersky, αρχίζει να εγκαθιστά την τρέχουσα έκδοση.

Αν ο Οδηγός εγκατάστασης εντοπίσει μια νεότερη έκδοση του Kaspersky Total Security στους διακομιστές ενημέρωσης της Kaspersky, σας ειδοποιεί για τη δυνατότητα λήψης και εγκατάστασης αυτής της έκδοσης στον υπολογιστή σας. Συνιστάται να εγκαταστήσετε τη νέα έκδοση της εφαρμογής, καθώς οι νεότερες εκδόσεις περιλαμβάνουν περισσότερες βελτιώσεις οι οποίες σας επιτρέπουν να διασφαλίσετε πιο αξιόπιστη προστασία του υπολογιστή σας. Εάν αρνηθείτε να εγκαταστήσετε τη νέα έκδοση, ο Οδηγός αρχίζει να εγκαθιστά την τρέχουσα έκδοση της εφαρμογής. Εάν συμφωνήσετε να εγκαταστήσετε τη νέα έκδοση της εφαρμογής, ο Οδηγός αντιγράφει στον υπολογιστή σας τα αρχεία από το πακέτο εγκατάστασης και αρχίζει να εγκαθιστά την τρέχουσα έκδοση.

Εκκίνηση της εγκατάστασης της εφαρμογής

Σε αυτό το βήμα, ο Οδηγός σάς προτείνει να εγκαταστήσετε την εφαρμογή.

Για να συνεχίσετε με την εγκατάσταση, κάντε κλικ στο κουμπί **Συνέχεια**.

Ανάλογα με τον τύπο της εγκατάστασης και τη γλώσσα τοπικής προσαρμογής, σε αυτό το βήμα ο Οδηγός σάς προτείνει να διαβάσετε την Άδεια Χρήσης Τελικού Χρήστη που θα ισχύει ανάμεσα σε εσάς και την Kaspersky και θα σας ρωτήσει αν θέλετε να συμμετάσχετε στο Kaspersky Security Network.

Ανασκόπηση της Άδειας Χρήσης Τελικού Χρήστη

Αυτό το βήμα του Οδηγού εμφανίζεται για ορισμένες γλώσσες τοπικής προσαρμογής κατά την εγκατάσταση του Kaspersky Total Security από ένα πακέτο εγκατάστασης που έχει ληφθεί μέσω διαδικτύου.

Σε αυτό το βήμα, ο Οδηγός σάς προτείνει να διαβάσετε τη συμφωνία παραχώρησης Άδειας Χρήσης Τελικού Χρήστη που θα ισχύει ανάμεσα σε εσάς και την Kaspersky.

Διαβάστε προσεκτικά την Άδεια Χρήσης Τελικού Χρήστη και, εάν συμφωνείτε με όλους τους όρους της, κάντε κλικ στο κουμπί **Αποδοχή**. Μετά από αυτό το βήμα, η εγκατάσταση της εφαρμογής στον υπολογιστή σας θα συνεχιστεί.

Εάν οι όροι της Άδειας Χρήσης Τελικού Χρήστη δεν γίνουν αποδεκτοί, δεν θα πραγματοποιηθεί η εγκατάσταση της εφαρμογής.

Σε <u>ορισμένες περιοχές</u>, πρέπει επίσης να αποδεχτείτε τους όρους της Πολιτικής απορρήτου για να συνεχίσετε την εγκατάσταση της εφαρμογής.

Δήλωση για το Kaspersky Security Network

Σε αυτό το βήμα, ο Οδηγός σάς δίνει τη δυνατότητα να συμμετάσχετε στο Kaspersky Security Network. Η συμμετοχή στο πρόγραμμα περιλαμβάνει την αποστολή πληροφοριών στην ΑΟ Kaspersky Lab σχετικά με απειλές που εντοπίστηκαν στον υπολογιστή σας, εφαρμογές που εκτελούνται, υπογεγραμμένες εφαρμογές που έχουν ληφθεί, καθώς και πληροφορίες σχετικά με το λειτουργικό σας σύστημα. Δεν γίνεται συλλογή, επεξεργασία ή αποθήκευση προσωπικών δεδομένων που λαμβάνονται από εσάς.

Διαβάστε τη Δήλωση για το Kaspersky Security Network. Εάν αποδέχεστε όλους τους όρους, κάντε κλικ στο κουμπί **Αποδοχή** στο παράθυρο του Οδηγού.

Εάν δεν θέλετε να συμμετάσχετε στο Kaspersky Security Network, κάντε κλικ στο κουμπί **Άρνηση**.

Αφού αποδεχθείτε ή απορρίψετε τη συμμετοχή στο Kaspersky Security Network, η εγκατάσταση της εφαρμογής θα συνεχιστεί.

Σε <u>ορισμένες εκδόσεις της εφαρμογής</u>, η Δήλωση για το Kaspersky Security Network περιλαμβάνει πληροφορίες σχετικά με την επεξεργασία προσωπικών δεδομένων.

Εγκατάσταση της εφαρμογής

Μερικές εκδόσεις του Kaspersky Total Security διανέμονται στο πλαίσιο συνδρομής και πριν την εγκατάσταση πρέπει να καταχωρηθεί κωδικός πρόσβασης που λαμβάνεται από τον πάροχο της υπηρεσίας.

Η εγκατάσταση της εφαρμογής ξεκινά αφού καταχωρήσετε τον κωδικό πρόσβασης.

Η εγκατάσταση της εφαρμογής μπορεί να διαρκέσει αρκετή ώρα. Περιμένετε να ολοκληρωθεί.

Μόλις ολοκληρωθεί η εγκατάσταση, ο Οδηγός εγκατάστασης θα προχωρήσει αυτόματα στο επόμενο βήμα.

Έλεγχοι κατά την εγκατάσταση της εφαρμογής

Το Kaspersky Total Security εκτελεί αρκετούς ελέγχους κατά την εγκατάσταση. Αυτοί οι έλεγχοι ενδέχεται να εντοπίσουν τα εξής προβλήματα:

- Μη συμμόρφωση του λειτουργικού συστήματος με τις απαιτήσεις λογισμικού. Κατά την εγκατάσταση, ο Οδηγός ελέγχει τα εξής:
 - Εάν το λειτουργικό σύστημα και το Service Pack πληρούν τις απαιτήσεις λογισμικού
 - Όλες οι απαιτούμενες εφαρμογές είναι διαθέσιμες
 - Ο ελεύθερος χώρος στον δίσκο επαρκεί για την εγκατάσταση
 - Ο χρήστης που εγκαθιστά την εφαρμογή διαθέτει προνόμια διαχειριστή

Εάν δεν πληρείται οποιαδήποτε από τις απαιτήσεις που παρατίθενται παραπάνω, θα εμφανιστεί στην οθόνη μια σχετική ειδοποίηση.

 Παρουσία μη συμβατών εφαρμογών στον υπολογιστή. Αν εντοπιστούν μη συμβατές εφαρμογές, θα εμφανιστούν σε μια λίστα στην οθόνη και θα σας ζητηθεί να τις καταργήσετε. Συνιστάται να καταργήσετε μη αυτόματα όλες τις εφαρμογές που δεν μπορεί να αφαιρέσει αυτόματα το Kaspersky Total Security. Κατά την κατάργηση μη συμβατών εφαρμογών, θα χρειαστεί να κάνετε επανεκκίνηση του λειτουργικού σας συστήματος. Έπειτα, η εγκατάσταση του Kaspersky Total Security συνεχίζεται αυτόματα.

Εγκατάσταση του Kaspersky Password Manager

Πριν από την ολοκλήρωση της εγκατάστασης, το Kaspersky Total Security σάς προτείνει επίσης να εγκαταστήσετε το <u>Kaspersky Password Manager για να προστατεύσετε τους</u> <u>κωδικούς πρόσβασής σας</u>. Η εγκατάσταση του Kaspersky Password Manager μπορεί να συνεχιστεί μετά το τέλος της εγκατάστασης του Kaspersky Total Security. Δεν υπάρχει ξεχωριστή ειδοποίηση σχετικά με την ολοκλήρωση της εγκατάστασης του Kaspersky Password Manager.

Συνιστώμενες ρυθμίσεις

Σε αυτό το βήμα μπορείτε να δείτε και να αλλάξετε τις ρυθμίσεις του Kaspersky Total Security, τις οποίες οι ειδικοί της Kaspersky σας συμβουλεύουν να ενεργοποιήσετε προτού ξεκινήσετε να χρησιμοποιείτε την εφαρμογή.

Για να αλλάξετε τις συνιστώμενες ρυθμίσεις:

- 1. Επιλέξτε ποιες ρυθμίσεις επιθυμείτε να ενεργοποιήσετε ή να απενεργοποιήσετε:
 - Εάν καταφορτώνετε και εγκαθιστάτε συχνά εφαρμογές από το Διαδίκτυο, αφήστε το πλαίσιο ελέγχου Ενεργοποίηση προστασίας από διαφημίσεις ώστε να γίνεται εγκατάσταση μόνο του επιθυμητού λογισμικού και να αποκλείονται οι πρόσθετες εγκαταστάσεις επιλεγμένο. Αυτό θα σας βοηθήσει να αποτρέψετε την εγκατάσταση μη απαραίτητων εφαρμογών.
 - Αφήστε επιλεγμένο το πλαίσιο ελέγχου Διαγραφή κακόβουλων εργαλείων, προγραμμάτων adware, λογισμικού αυτόματων κλήσεων και ύποπτων πακέτων εάν επιθυμείτε η εφαρμογή να διαγράψει αυτά τα αντικείμενα.
 - Εάν εγκαθιστάτε συχνά νέες εφαρμογές, αφήστε επιλεγμένο το πλαίσιο ελέγχου
 Εντοπισμός άλλου λογισμικού που μπορεί να χρησιμοποιηθεί από εγκληματίες
 για την καταστροφή του υπολογιστή σας ή των προσωπικών δεδομένων σας.
 Αυτό θα σας βοηθήσει να εντοπίσετε εφαρμογές που μπορεί να χρησιμοποιηθούν για
 την πρόκληση βλάβης στον υπολογιστή σας ή στα προσωπικά δεδομένα σας.
 - Για να μάθετε περισσότερα σχετικά με τις νέες και κύριες δυνατότητες της εφαρμογής, αφήστε το πλαίσιο ελέγχου Κάντε μια περιήγηση στις λειτουργίες της εφαρμογής επιλεγμένο.

Εάν δεν θέλετε να ενεργοποιήσετε τις συνιστώμενες ρυθμίσεις του Kaspersky, αποεπιλέξτε τα σχετικά πλαίσια.

2. Κάντε κλικ στο κουμπί **Εφαρμογή**.

Ολοκλήρωση εγκατάστασης

Σε αυτό το βήμα, ο Οδηγός σάς ενημερώνει για την ολοκλήρωση της εγκατάστασης της εφαρμογής.

Κάντε κλικ στο κουμπί **Ολοκληρώθηκε**.

Όλα τα απαραίτητα στοιχεία της εφαρμογής θα εκκινηθούν αυτόματα μόλις ολοκληρωθεί η εγκατάσταση.

Σε ορισμένες περιπτώσεις, μπορεί να χρειαστεί να επανεκκινήσετε το λειτουργικό σύστημα για να ολοκληρωθεί η εγκατάσταση.

Ενεργοποίηση της εφαρμογής

Ο Οδηγός ενεργοποίησης ξεκινά κατά την πρώτη εκκίνηση του Kaspersky Total Security.

Με τη διαδικασία της *ενεργοποίησης* καθίσταται δυνατή η χρήση μια πλήρως λειτουργικής έκδοσης της εφαρμογής για ένα καθορισμένο χρονικό διάστημα.

Εάν αποκτήσατε μια άδεια χρήσης για το Kaspersky Total Security και κάνατε λήψη της εφαρμογής από ηλεκτρονικό κατάστημα, η ενεργοποίηση της εφαρμογής μπορεί να γίνει αυτόματα κατά τη διάρκεια της εγκατάστασης.

Προσφέρονται οι εξής επιλογές για την ενεργοποίηση του Kaspersky Total Security:

 Ενεργοποίηση εφαρμογής. Κάντε αυτήν την επιλογή και εισαγάγετε τον κωδικό ενεργοποίησης. εάν έχετε αγοράσει άδεια χρήσης για την εφαρμογή.

Εάν καθορίσετε έναν κωδικό ενεργοποίησης για το Kaspersky Internet Security ή το Kaspersky Anti-Virus στο πεδίο εισαγωγής, η διαδικασία μετάβασης στο Kaspersky Internet Security ή το Kaspersky Anti-Virus ξεκινά μετά την ολοκλήρωση της ενεργοποίησης.

 Ενεργοποίηση δοκιμαστικής έκδοσης της εφαρμογής. Χρησιμοποιήστε αυτήν την επιλογή ενεργοποίησης, εάν θέλετε να εγκαταστήσετε τη δοκιμαστική έκδοση της εφαρμογής πριν αποφασίσετε να αγοράσετε μια άδεια χρήσης. Θα έχετε τη δυνατότητα να χρησιμοποιήσετε την εφαρμογή και όλες τις λειτουργίες της για μια σύντομη περίοδο αξιολόγησης. Όταν λήξει η δοκιμαστική άδεια χρήσης, η δοκιμαστική έκδοση δεν θα μπορεί να ενεργοποιηθεί ξανά.

Για την ενεργοποίηση της εφαρμογής, απαιτείται σύνδεση στο Διαδίκτυο.

Κατά την εγκατάσταση και την ενεργοποίηση της εφαρμογής, ενδέχεται να σας ζητηθεί να δημιουργήσετε έναν λογαριασμό My Kaspersky. Σας συνιστούμε να συνδέσετε την εφαρμογή στο My Kaspersky, ώστε να μπορείτε να αποθηκεύσετε τον κωδικό ενεργοποίησης για επακόλουθη ανάκτηση μετά την επανεγκατάσταση του λειτουργικού συστήματος, την εγκατάσταση προστασίας σε μια νέα συσκευή ή την επανεγκατάσταση της εφαρμογής.

Εγγραφή και σύνδεση στο My Kaspersky

Αυτό το βήμα δεν είναι διαθέσιμο σε όλες τις εκδόσεις του Kaspersky Total Security.

Οι εγγεγραμμένοι χρήστες στο <u>My Kaspersky</u> έχουν τη δυνατότητα να στέλνουν αιτήματα στην Τεχνική υποστήριξη και στο Εργαστήριο ιών, να διαχειρίζονται τους κωδικούς ενεργοποίησης με εύκολο τρόπο και να λαμβάνουν τις τελευταίες πληροφορίες σχετικά με νέες εφαρμογές και ειδικές προσφορές της Kaspersky.

- Εάν έχετε ήδη λογαριασμό My Kaspersky, ανοίγει το παράθυρο Σύνδεση στο My Kaspersky. Εισαγάγετε τα διαπιστευτήριά σας για να συνδέσετε την εφαρμογή στην πύλη My Kaspersky και κάντε κλικ στο κουμπί Σύνδεση.
- Εάν δεν έχετε ακόμα λογαριασμό My Kaspersky, ανοίγει το παράθυρο εγγραφής λογαριασμού My Kaspersky. <u>Συμπληρώστε τη φόρμα εγγραφής</u> και κάντε κλικ στο κουμπί Δημιουργία.

Σε <u>ορισμένες περιοχές</u>, η εφαρμογή σάς ζητά να διαβάσετε και να αποδεχτείτε τον κανονισμό σχετικά με την παροχή δεδομένων. Εάν αποδέχεστε τους όρους της δήλωσης, κάντε κλικ στο κουμπί **Αποδοχή και σύνδεση**.

Σε ορισμένες περιπτώσεις, η εγγραφή στο My Kaspersky αποτελεί προϋπόθεση για να ξεκινήσει η χρήση της εφαρμογής.

Ολοκλήρωση ενεργοποίησης

Ο Οδηγός σάς ενημερώνει ότι το Kaspersky Total Security έχει ενεργοποιηθεί επιτυχώς.

Κάντε κλικ στο κουμπί **Ολοκληρώθηκε** για έξοδο από τον Οδηγό.

Σφάλμα εγκατάστασης εφαρμογής σε Windows 7 και Windows Server 2008 R2

Το Kaspersky Total Security δεν μπορεί να εγκατασταθεί σε Microsoft Windows 7 και Microsoft Windows Server 2008 R2 αν δεν έχουν εγκατασταθεί οι ακόλουθες ενημερώσεις:

- 1. ΚΒ4490628 (ενημέρωση 12 Μαρτίου 2019);
- 2. ΚΒ4474419 (ενημέρωση από 23 Σεπτεμβρίου 2019).

Το σφάλμα εγκατάστασης προκύπτει ως αποτέλεσμα του ότι η Microsoft ενημέρωσε τον αλγόριθμο υπογραφής ενοτήτων και προγραμμάτων οδήγησης εφαρμογών τρίτων. Τώρα οι μονάδες και τα προγράμματα οδήγησης εφαρμογών τρίτων (συμπεριλαμβανομένης της Kaspersky) υπογράφονται χρησιμοποιώντας αλγόριθμο κλειδώματος SHA256. Χρειάζεται να εγκαταστήσετε τις ενημερώσεις για τα KB4490628K και KB4474419, προκειμένου οι ενότητες και τα προγράμματα οδήγησης του Kaspersky Total Security να μπορούν να υπογράφονται χρησιμοποιώντας τον αλγόριθμο κλειδώματος SHA256.

Χρησιμοποιήστε μία από τις ακόλουθες μεθόδους για να εγκαταστήσετε τις ενημερώσεις.

Ενημέρωση εγκατάστασης χρησιμοποιώντας το Windows Update

Εάν η αυτόματη εγκατάσταση ενημερώσεων είναι απενεργοποιημένη στον υπολογιστή σας:

Στο μενού Έναρξη, επιλέξτε Πίνακας Ελέγχου → Σύστημα και Ασφάλεια → Windows Update.

Ανοίγει το παράθυρο του Windows Update.

- 2. Στο αριστερό μενού του παραθύρου του **Windows Update**, επιλέξτε **Αλλαγή ρυθμίσεων**.
- 3. Στο μπλοκ **Σημαντικές ενημερώσεις** που ανοίγει, επιλέξτε **Αυτόματη εγκατάσταση** ενημερώσεων (συνιστάται).

Όλες οι απαραίτητες ενημερώσεις θα ληφθούν και θα εγκατασταθούν αυτόματα στον υπολογιστή σας.

Χειροκίνητη εγκατάσταση του Service Pack 1 εάν δεν είναι εγκατεστημένο

Εάν ο υπολογιστής σας λειτουργεί σε Windows 7 Service Pack 0 ή Windows Server 2008 R2 Service Pack 0, πρώτα θα πρέπει να εγκαταστήσετε το Service Pack 1 (KB976932).

Για την εγκατάσταση της ενημέρωσης του Service Pack 1:

- 1. Μεταβείτε στην επιλογή <u>Κατάλογος του Microsoft Update</u> 🗹 .
- 2. Επιλέξτε την έκδοση λειτουργικού συστήματος του υπολογιστή σας και κάντε κλικ στο κουμπί **Λήψη**.
- Κάντε λήψη της ενημέρωσης στον υπολογιστή σας κάνοντας κλικ στο σύνδεσμο στο ανοιχτό παράθυρο.
- 4. Εγκαταστήστε την ενημέρωση.

Χειροκίνητη εγκατάσταση του ΚΒ4490628

Για να εγκαταστήσετε χειροκίνητα το KB4490628:

- 1. Μεταβείτε στην επιλογή Κατάλογος του Microsoft Update 🗹 .
- 2. Επιλέξτε την έκδοση λειτουργικού συστήματος του υπολογιστή σας και κάντε κλικ στο κουμπί **Λήψη**.
- Κάντε λήψη της ενημέρωσης στον υπολογιστή σας κάνοντας κλικ στο σύνδεσμο στο ανοιχτό παράθυρο.
- 4. Εγκαταστήστε την ενημέρωση.

Χειροκίνητη εγκατάσταση του ΚΒ4474419

Για να εγκαταστήσετε χειροκίνητα το ΚΒ4474419:

- 1. Μεταβείτε στην επιλογή Κατάλογος του Microsoft Update 🗷 .
- 2. Επιλέξτε την έκδοση λειτουργικού συστήματος του υπολογιστή σας και κάντε κλικ στο κουμπί **Λήψη**.
- Κάντε λήψη της ενημέρωσης στον υπολογιστή σας κάνοντας κλικ στο σύνδεσμο στο ανοιχτό παράθυρο.

4. Εγκαταστήστε την ενημέρωση.

Μετά την εγκατάσταση ενημερώσεων, επανεκκινήστε τον υπολογιστή και εγκαταστήστε το Kaspersky Total Security εκ νέου.

Εγκατάσταση της εφαρμογής από τη γραμμή εντολών

Μπορείτε να εγκαταστήσετε το Kaspersky Total Security από τη γραμμή εντολών.

Ορισμένες εντολές μπορούν να εκτελεστούν μόνο από τον λογαριασμό διαχειριστή.

Σύνταξη γραμμής εντολών:

<διαδρομή προς το αρχείο του πακέτου εγκατάστασης> [παράμετροι]

Λεπτομερείς οδηγίες και λίστα με τις ρυθμίσεις εγκατάστασης παρέχονται στον <u>δικτυακό</u> <u>τόπο Τεχνικής υποστήριξης</u> .

Πρώτα βήματα

Για να υποστηρίζει πλήρως το Kaspersky Total Security τα προγράμματα περιήγησης, πρέπει να εγκατασταθεί η επέκταση Kaspersky Protection και να ενεργοποιηθεί σε όλα τα προγράμματα περιήγησης. Το Kaspersky Total Security χρησιμοποιεί την επέκταση Kaspersky Protection για να ενσωματώσει μια δέσμη ενεργειών στον δικτυακό τόπο που ανοίγει στο Προστατευμένο πρόγραμμα περιήγησης και στην κυκλοφορία. Η εφαρμογή χρησιμοποιεί τη συγκεκριμένη δέσμη ενεργειών για αλληλεπίδραση με την ιστοσελίδα και για τη μετάδοση δεδομένων σε τράπεζες, των οποίων οι δικτυακοί τόποι προστατεύονται από το στοιχείο Ασφαλείς τραπεζικές συναλλαγές. Η εφαρμογή προστατεύει τα δεδομένα που μεταδίδονται μέσω της δέσμης ενεργειών χρησιμοποιώντας ψηφιακή υπογραφή. Το Kaspersky Total Security μπορεί να ενσωματώσει τη δέσμη ενεργειών χωρίς χρήση της επέκτασης Kaspersky Protection.

Το Kaspersky Total Security υπογράφει τα δεδομένα που μεταδίδονται μέσω της δέσμης ενεργειών χρησιμοποιώντας τις εγκατεστημένες βάσεις δεδομένων προστασίας από ιούς και τα αιτήματα προς το Kaspersky Security Network. Η εφαρμογή αποστέλλει τα αιτήματα στο Kaspersky Security Network ανεξάρτητα από το εάν έχετε αποδεχτεί ή όχι τους όρους της Δήλωσης του Kaspersky Security Network. Εγκατάσταση της επέκτασης Kaspersky Protection σε Microsoft Edge που βασίζεται σε Chromium, Mozilla Firefox και Google Chrome.

Η επέκτασης Kaspersky Protection δεν εγκαθίσταται αυτόματα στα Microsoft Edge που βασίζεται σε Chromium, Mozilla Firefox και Google Chrome. Αν η επέκταση Kaspersky Protection δεν έχει εγκατασταθεί στο πρόγραμμα περιήγησής σας, η εφαρμογή σάς ζητά να μεταβείτε στη σελίδα λήψεων των επεκτάσεων και να εγκαταστήσετε χειροκίνητα την επέκταση Kaspersky Protection όταν ξεκινά το πρόγραμμα περιήγησης.

Υποστήριξη Yandex Browser

Όταν χρησιμοποιείτε το Yandex Browser, είναι ενεργοποιημένα τα ακόλουθα στοιχεία της εφαρμογής:

- Προστατευμένο πρόγραμμα περιήγησης
- Σύμβουλος URL
- Προστασία από ιούς στο Web
- Κατά του phishing

Τα στοιχεία Ιδιωτική περιήγηση και Πρόγραμμα Anti-Banner λειτουργούν, αλλά δεν είναι δυνατό να ρυθμιστούν οι παράμετροί τους στο Yandex Browser.

Υποστήριξη του Internet Explorer

Ξεκινώντας με το Kaspersky Total Security 2021, η επέκταση Kaspersky Protection δεν θα υποστηρίζει πλέον τον πρόγραμμα περιήγησης Internet Explorer. Εάν θέλετε να συνεχίσετε να χρησιμοποιείτε την επέκταση Kaspersky Protection στον Internet Explorer, μπορείτε να επιστρέψετε στην προηγούμενη έκδοση της εφαρμογής.

Πώς να ενημερώσετε την εφαρμογή

Η εφαρμογή ενημερώνεται αυτόματα εάν επιλέξετε τη λειτουργία εκτέλεσης **Αυτόματα** στο παράθυρο ρυθμίσεων ενημέρωσης (**Ενημέρωση βάσης δεδομένων** → **Χρονοδιάγραμμα** ενημέρωσης βάσεων δεδομένων).

Η εφαρμογή ενημερώνεται αυτόματα αν <u>εγκαταστήσετε μια νέα έκδοση της εφαρμογής</u> πάνω από την προηγούμενη.

Εάν έχετε μια ισχύουσα άδεια χρήσης για μια προηγούμενη έκδοση του Kaspersky Total Security, δεν χρειάζεται να ενεργοποιήσετε την εφαρμογή. Ο Οδηγός εγκατάστασης και κατάργησης εγκατάστασης θα ανακτήσει αυτόματα πληροφορίες σχετικά με την άδεια χρήσης για την προηγούμενη έκδοση του Kaspersky Total Security και θα τις εφαρμόσει κατά την εγκατάσταση του Kaspersky Total Security.

Κατά τη λήψη της ενημέρωσης, η εφαρμογή συγκρίνει τις προηγούμενες και τις νέες εκδόσεις στην Άδεια Χρήσης Τελικού Χρήστη, τη Δήλωση Kaspersky Security Network και τη Δήλωση αναφορικά με την επεξεργασία δεδομένων για σκοπούς μάρκετινγκ. Εάν οι συμφωνίες ή/και οι δηλώσεις διαφέρουν, η εφαρμογή σάς δίνει τη δυνατότητα να τις διαβάσετε και αποδεχτείτε πάλι.

Η εφαρμογή μπορεί να αναβαθμιστεί εάν είναι εγκατεστημένες στον υπολογιστή σας οι ακόλουθες εκδόσεις του Kaspersky Total Security:

- Kaspersky Total Security 2015
- Kaspersky Total Security 2016
- Kaspersky Total Security 2017
- Kaspersky Total Security 2018
- Kaspersky Total Security 2019
- Kaspersky Total Security 2020

Περιορισμοί στην αναβάθμιση μιας προηγούμενης έκδοσης της εφαρμογής

Οι αναβαθμίσεις προγενέστερων εκδόσεων δεν υποστηρίζονται.

Η αναβάθμιση από το Kaspersky Total Security έχει τους ακόλουθους περιορισμούς:

- Κατά την αναβάθμιση μιας προηγούμενης έκδοσης του Kaspersky Total Security, οι ακόλουθες ρυθμίσεις της εφαρμογής αντικαθίστανται με προεπιλεγμένες ρυθμίσεις:
 - Ρυθμίσεις εμφάνισης τους Kaspersky Total Security
 - Χρονοδιάγραμμα σάρωσης
 - Συμμετοχή στο Kaspersky Security Network
 - Επίπεδο προστασίας της Προστασίας αρχείων από ιούς

- Επίπεδο προστασίας της Προστασίας email από ιούς
- Ρυθμίσεις του Προγράμματος Anti-Banner
- Πηγές ενημέρωσης
- Λίστα αξιόπιστων διευθύνσεων web
- Ρυθμίσεις για τον Σύμβουλο URL
- Μετά από αναβάθμιση από προηγούμενη έκδοση, το Kaspersky Total Security ξεκινά αυτόματα ακόμη και αν η αυτόματη εκκίνηση της εφαρμογής έχει απενεργοποιηθεί στις αποθηκευμένες ρυθμίσεις. Κατά την επόμενη επανεκκίνηση του λειτουργικού συστήματος, το Kaspersky Total Security δεν θα ξεκινήσει αυτόματα εάν η αυτόματη εκκίνηση της εφαρμογής είναι απενεργοποιημένη στις αποθηκευμένες ρυθμίσεις.

Εγκατάσταση πάνω από άλλες εφαρμογές της Kaspersky

Εγκατάσταση νέας έκδοσης του Kaspersky Total Security πάνω από προηγούμενη έκδοση του Kaspersky Internet Security

Εάν εγκαταστήσετε μια νέα έκδοση του Kaspersky Total Security σε έναν υπολογιστή στον οποίο έχει ήδη εγκατασταθεί μια από τις προηγούμενες εκδόσεις του Kaspersky Internet Security με τρέχουσα άδεια, ο Οδηγός ενεργοποίησης σας προτρέπει να επιλέξετε μία από τις παρακάτω επιλογές:

- Συνέχιση χρήσης του Kaspersky Internet Security στα πλαίσια της τρέχουσας άδειας χρήσης. Σε αυτή την περίπτωση, θα ξεκινήσει ο Οδηγός μετάπτωσης. Όταν ολοκληρωθεί Οδηγός μετάβασης, η νέα έκδοση του Kaspersky Internet Security θα εγκατασταθεί στον υπολογιστή σας. Μπορείτε να χρησιμοποιήσετε το Kaspersky Internet Security μέχρι να λήξει η άδεια χρήσης για την προηγούμενη έκδοση του Kaspersky Internet Security.
- Συνέχεια με την εγκατάσταση της νέας έκδοσης του Kaspersky Total Security. Σε αυτή την περίπτωση, η εφαρμογή θα εγκατασταθεί και θα ενεργοποιηθεί σύμφωνα με το <u>τυπικό</u> <u>σενάριο</u>.

Εγκατάσταση του Kaspersky Total Security μέσω Kaspersky Security Cloud

Εάν πραγματοποιείτε εγκατάσταση του Kaspersky Total Security μέσω του Kaspersky Security Cloud, δεν θα μπορείτε να χρησιμοποιήσετε το Kaspersky Total Security μέσω της άδειας χρήσης για το Kaspersky Security Cloud. Μπορείτε να χρησιμοποιήσετε το Kaspersky Security Cloud μέσω αυτής της άδειας χρήσης σε μια άλλη συσκευή.

Οι ρυθμίσεις της εφαρμογής Kaspersky Security Cloud δεν αποθηκεύονται και δεν μπορούν να εφαρμοστούν στο Kaspersky Total Security.

Μετάβαση από το Kaspersky Total Security σε άλλες εφαρμογές της Kaspersky

Όταν λήξει η άδεια χρήσης του Kaspersky Total Security, η εφαρμογή σάς δίνει την δυνατότητα να αγοράσετε μια άδεια χρήσης του Kaspersky Security Cloud.

To Kaspersky Security Cloud είναι μια υπηρεσία ασφάλειας υπολογιστών που υπερβαίνει τη συνηθισμένη προστασία από ιούς και άλλες απειλές για υπολογιστές. Η εφαρμογή προσφέρει εξατομικευμένες προτάσεις και σενάρια προσαρμοσμένης προστασίας που είναι διαμορφωμένα γύρω από εσάς και την οικογένειά σας.

Το Kaspersky Security Cloud προσαρμόζεται με ευελιξία στις ανάγκες σας και προσφέρει πρόσθετες δυνατότητες, όπως:

- Έλεγχο αδύναμων ρυθμίσεων στο λειτουργικό σύστημα
- Έλεγχο συσκευών στο δίκτυό σας Wi-Fi
- Ειδήσεις σχετικά με την ασφάλεια

Η συνδρομή στο Kaspersky Security Cloud σάς επιτρέπει να χρησιμοποιείτε ελεύθερα το Kaspersky Safe Kids για την προστασία των παιδιών σας και το Kaspersky Password Manager για την προστασία των κωδικών πρόσβασης.

Η μετάβαση στο Kaspersky Security Cloud δεν είναι διαθέσιμη σε όλες τις περιοχές.

Μετάβαση στο Kaspersky Free όταν έχει λήξει η άδεια χρήσης του Kaspersky Total Security

Όταν λήξει η άδεια χρήσης του Kaspersky Total Security, μπορείτε να αγοράσετε μια νέα άδεια χρήσης και να συνεχίσετε να χρησιμοποιείτε όλες τις δυνατότητες της εφαρμογής. Η εφαρμογή ενδέχεται επίσης να σας ζητήσει να μεταβείτε στο Kaspersky Free για να διατηρήσετε τη βασική προστασία του υπολογιστή σας.

Αν δεν χρησιμοποιήσατε θαλάμους δεδομένων και αντίγραφα ασφαλείας όταν η άδεια χρήση σας ήταν ενεργή, η μετάβαση στο Kaspersky Free μπορεί να πραγματοποιηθεί αυτόματα. Μετά τη μετάβαση, η εφαρμογή σάς ειδοποιεί σχετικά με αυτό και ζητά να ανανεώσετε την άδεια χρήσης ή να συνεχίσετε να χρησιμοποιείτε τη δωρεάν έκδοση για προστασία.

Αν χρησιμοποιήσατε θαλάμους ή/και αντίγραφα ασφαλείας όταν η άδεια χρήσης σας ήταν ενεργή, η εφαρμογή σάς ειδοποιεί ότι η πρόσβαση σε αυτά τα στοιχεία περιορίζεται λόγω λήξης της άδειας χρήσης.

Για να ανανεώσετε την άδεια χρήσης ή να μεταβείτε στο Kaspersky Free, πραγματοποιήστε μία από τις εξής ενέργειες:

 Αν θέλετε να ανανεώσετε την άδεια χρήσης και να συνεχίσετε να χρησιμοποιείτε όλες τις δυνατότητες του Kaspersky Total Security, κάντε κλικ στο κουμπί Ανανέωση άδειας χρήσης.

Κάνοντας κλικ σε αυτό το κουμπί μεταβαίνετε στο κατάστημα.

• Αν δεν θέλετε να ανανεώσετε την άδεια χρήσης, κάντε κλικ στο κουμπί Όχι τώρα.

Αν κάνετε κλικ σε αυτό το κουμπί, η εφαρμογή θα ελέγξει αν υπάρχουν άλλες διαθέσιμες άδειες χρήσης. Αν η εφαρμογή δεν εντοπίσει άλλες άδειες χρήσης, μπορεί να σας ζητηθεί να μεταβείτε στο Kaspersky Free.

Έναρξη μετεγκατάστασης στο Kaspersky Free

Στο βήμα αυτό, ο Οδηγός μετεγκατάστασης σας προσφέρει τη δυνατότητα να μεταβείτε στο Kaspersky Free και να διατηρήσετε τη βασική προστασία του υπολογιστή σας.

Για να μεταβείτε στο Kaspersky Free, κάντε κλικ στο κουμπί **Μετάβαση στο Kaspersky Free**.

Επιβεβαίωση της μετεγκατάστασης στο Kaspersky Free

Στο βήμα αυτό, ο Οδηγός μετεγκατάστασης σας προσφέρει τη δυνατότητα να επιβεβαιώσετε ή να αρνηθείτε τη μετάβαση στο Kaspersky Free. Αν χρησιμοποιήσατε θαλάμους ή/και αντίγραφα ασφαλείας όταν η άδεια χρήσης σας ήταν ενεργή, η εφαρμογή σάς ειδοποιεί ότι η πρόσβαση σε αυτά τα στοιχεία θα περιοριστεί μετά τη μετάβαση στο Kaspersky Free. Για να διατηρήσετε την πρόσβαση στα αρχεία που είναι αποθηκευμένα στους θαλάμους δεδομένων σας, μετακινήστε τα σε άλλη θέση προτού συνεχίσετε τη μετάβαση στο Kaspersky Free. Για να επαναφέρετε τα δεδομένα σας από τα αντίγραφα ασφαλείας σας, μπορείτε να χρησιμοποιήσετε το Kaspersky Restore Utility.

Πραγματοποιήστε μία από τις εξής ενέργειες:

- Για να επιβεβαιώσετε τη μετάβαση, κάντε κλικ στο κουμπί Μετάβαση.
 Ο Οδηγός μετεγκατάστασης προχωρά στο επόμενο βήμα.
- Για να αρνηθείτε τη μετάβαση, κάντε κλικ στο κουμπί Άκυρο.
 Κλείνει ο Οδηγός μετεγκατάστασης.

Αναζήτηση για μη συμβατό λογισμικό

Σε αυτό το βήμα, ο Οδηγός μετεγκατάστασης ελέγχει εάν στον υπολογιστή σας υπάρχουν εγκατεστημένες εφαρμογές μη συμβατές με το Kaspersky Free. Εάν δεν βρεθούν τέτοιες εφαρμογές, ο Οδηγός μετεγκατάστασης θα προχωρήσει αυτόματα στο επόμενο βήμα. Αν κλείσετε το παράθυρο του Οδηγού μετεγκατάστασης σε αυτό το βήμα, η αναζήτηση για μη συμβατό λογισμικό θα συνεχιστεί στο παρασκήνιο.

Εάν βρεθούν μη συμβατές εφαρμογές, ο Οδηγός μετεγκατάστασης τις εμφανίζει σε μια λίστα στο παράθυρο και σάς ειδοποιεί να τις απεγκαταστήσετε.

Μετά από την απεγκατάσταση των μη συμβατών εφαρμογών, ο Οδηγός μετεγκατάστασης προχωρά στο επόμενο βήμα.

Ολοκλήρωση μετεγκατάστασης στο Kaspersky Free

Στο βήμα αυτό, ο Οδηγός μετεγκατάστασης σας ενημερώνει ότι η μετάβαση στο Kaspersky Free έχει ολοκληρωθεί.

Για να ξεκινήσετε το Kaspersky Free, κάντε κλικ στο κουμπί **Εκτέλεση**.

Μετάβαση στο Kaspersky Free κατά την απεγκατάσταση της δοκιμαστικής έκδοσης του Kaspersky Total Security

Κατά την απεγκατάσταση της δοκιμαστικής έκδοσης του Kaspersky Total Security, μπορείτε να μεταβείτε στο Kaspersky Free για να διατηρήσετε τη βασική προστασία. Όταν καταργείτε τη δοκιμαστική έκδοση του Kaspersky Total Security, η εφαρμογή σάς δίνει την δυνατότητα να αγοράσετε μια άδεια χρήσης ώστε να συνεχίσετε να χρησιμοποιείτε όλη τη λειτουργικότητα της εφαρμογής.

Για να ανανεώσετε την άδεια χρήσης ή να μεταβείτε στο Kaspersky Free, πραγματοποιήστε μία από τις εξής ενέργειες:

- Για να αγοράσετε μια άδεια χρήσης, κάντε κλικ στο κουμπί Ανανέωση άδειας χρήσης.
 Κάνοντας κλικ σε αυτό το κουμπί μεταβαίνετε στο κατάστημα.
- Για να ξεκινήσετε τη μετάβαση στο Kaspersky Free, κάντε κλικ στο κουμπί Όχι, ευχαριστώ.

Κάνοντας κλικ σε αυτό το κουμπί, ξεκινά ο Οδηγός μετεγκατάστασης στο Kaspersky Free.

Αν χρησιμοποιήσατε θαλάμους δεδομένων και αντίγραφα ασφαλείας στη δοκιμαστική έκδοση, θα έχετε περιορισμένη πρόσβαση σε αυτά μετά τη μετάβαση στο Kaspersky Free. Για να διατηρήσετε πλήρη πρόσβαση στους θαλάμους δεδομένων και τα αντίγραφα ασφαλείας σας, αγοράστε μια άδεια χρήσης.

Έναρξη μετεγκατάστασης στο Kaspersky Free

Στο βήμα αυτό, ο Οδηγός μετεγκατάστασης σας προσφέρει τη δυνατότητα να μεταβείτε στο Kaspersky Free και να διατηρήσετε τη βασική προστασία του υπολογιστή σας.

Για να μεταβείτε στο Kaspersky Free, κάντε κλικ στο κουμπί **Μετάβαση στο Kaspersky Free**.

Επιβεβαίωση της μετεγκατάστασης στο Kaspersky Free

Στο βήμα αυτό, ο Οδηγός μετεγκατάστασης σας προσφέρει τη δυνατότητα να επιβεβαιώσετε ή να αρνηθείτε τη μετάβαση στο Kaspersky Free.

Πραγματοποιήστε μία από τις εξής ενέργειες:

- Για να επιβεβαιώσετε τη μετάβαση, κάντε κλικ στο κουμπί Μετάβαση.
 Ο Οδηγός μετεγκατάστασης προχωρά στο επόμενο βήμα.
- Για να αρνηθείτε τη μετάβαση στο Kaspersky Free, κάντε κλικ στο κουμπί Άκυρο.
 Κλείνει ο Οδηγός μετεγκατάστασης.

Αναζήτηση για μη συμβατό λογισμικό

Σε αυτό το βήμα, ο Οδηγός μετεγκατάστασης ελέγχει εάν στον υπολογιστή σας υπάρχουν εγκατεστημένες εφαρμογές μη συμβατές με το Kaspersky Free. Εάν δεν βρεθούν τέτοιες εφαρμογές, ο Οδηγός μετεγκατάστασης θα προχωρήσει αυτόματα στο επόμενο βήμα. Αν κλείσετε το παράθυρο του Οδηγού μετεγκατάστασης σε αυτό το βήμα, η αναζήτηση για μη συμβατό λογισμικό θα συνεχιστεί στο παρασκήνιο.

Εάν βρεθούν μη συμβατές εφαρμογές, ο Οδηγός μετεγκατάστασης τις εμφανίζει σε μια λίστα στο παράθυρο και σάς ειδοποιεί να τις απεγκαταστήσετε.

Μετά από την απεγκατάσταση των μη συμβατών εφαρμογών, ο Οδηγός μετεγκατάστασης προχωρά στο επόμενο βήμα.

Ολοκλήρωση μετεγκατάστασης στο Kaspersky Free

Στο βήμα αυτό, ο Οδηγός μετεγκατάστασης σας ενημερώνει ότι η μετάβαση στο Kaspersky Free έχει ολοκληρωθεί.

Για να ξεκινήσετε το Kaspersky Free, κάντε κλικ στο κουμπί **Εκτέλεση**.

Πώς να καταργήσετε την εγκατάσταση της εφαρμογής

Μετά την κατάργηση του Kaspersky Total Security, ο υπολογιστής και τα προσωπικά σας δεδομένα δεν θα προστατεύονται.

Το Kaspersky Total Security καταργείται χρησιμοποιώντας τον Οδηγό εγκατάστασης και κατάργησης.

<u>Πώς απεγκαθιστάτε την εφαρμογή σε Windows 7</u> ?

Για εκκίνηση του Οδηγού σε υπολογιστή με λειτουργικό σύστημα Microsoft Windows 7 ή προηγούμενες εκδόσεις,

στο μενού **Έναρξη**, επιλέξτε **Όλα τα προγράμματα** → **Kaspersky Total Security** → **Κατάργηση του Kaspersky Total Security**.

<u>Πώς απεγκαθιστάτε την εφαρμογή σε Windows 8 ή νεότερη έκδοση </u>

Για να εκκινήσετε τον Οδηγό σε υπολογιστή με λειτουργικό σύστημα Microsoft Windows 8 ή μεταγενέστερο λειτουργικό σύστημα:

- 1. Στην οθόνη έναρξης, κάντε κλικ στο πλακίδιο Kaspersky Total Security για να εμφανιστεί η γραμμή εργαλείων.
- 2. Κάντε κλικ στο κουμπί **Κατάργηση** στη γραμμή εργαλείων.
- 3. Στο παράθυρο που θα ανοίξει, επιλέξτε το Kaspersky Total Security στη λίστα.
- 4. Κάντε κλικ στο κουμπί **Κατάργηση** που βρίσκεται στο πάνω μέρος του παραθύρου.

Εισαγωγή κωδικού πρόσβασης για την κατάργηση της εφαρμογής

Για να καταργήσετε το Kaspersky Total Security, πρέπει να εισαγάγετε τον κωδικό πρόσβασης για τις ρυθμίσεις της εφαρμογής. Εάν δεν μπορείτε να καθορίσετε τον κωδικό πρόσβασης για οποιοδήποτε λόγο, η κατάργηση της εφαρμογής δεν επιτρέπεται.

Αυτό το βήμα εμφανίζεται μόνο αν έχει οριστεί κωδικός πρόσβασης για την κατάργηση της εφαρμογής.

Αποθήκευση του κωδικού ενεργοποίησης

Βεβαιωθείτε ότι κωδικός ενεργοποίησης που διαθέτετε για το Kaspersky Total Security είναι αποθηκευμένος στο <u>My Kaspersky</u>. Αν εγκαταστήσετε το Kaspersky Total Security σε άλλον υπολογιστή, θα χρειαστείτε τον κωδικό ενεργοποίησης.

Εάν το Kaspersky Total Security δεν είναι συνδεδεμένο στο My Kaspersky, ο Οδηγός σας ζητά να συνδεθείτε στο My Kaspersky και, στη συνέχεια, αποθηκεύει τον κωδικό ενεργοποίησης στο My Kaspersky.

Αποθήκευση δεδομένων για μελλοντική χρήση

Σε αυτό το βήμα, μπορείτε να καθορίσετε ποια από τα δεδομένα που χρησιμοποιεί η εφαρμογή θέλετε να διατηρηθούν ώστε να χρησιμοποιηθούν ξανά κατά την επόμενη εγκατάσταση της εφαρμογής (για παράδειγμα, όταν πρόκειται να εγκατασταθεί μια νεότερη έκδοση της εφαρμογής).

Μπορείτε να αποθηκεύσετε τα ακόλουθα δεδομένα:

- Τα Στοιχεία άδειας χρήσης είναι ένα σύνολο δεδομένων που καταργούν την ανάγκη ενεργοποίησης της εφαρμογής σε περίπτωση μελλοντικής εγκατάστασης, καθώς σας επιτρέπουν να τη χρησιμοποιήσετε με την τρέχουσα άδεια χρήσης, εκτός εάν η άδεια λήξει πριν ξεκινήσετε την εγκατάσταση.
- Αρχεία καραντίνας είναι τα αρχεία που έχουν ελεγχθεί από την εφαρμογή και έχουν μετακινηθεί στην Καραντίνα.

Αφού καταργηθεί το Kaspersky Total Security από τον υπολογιστή, τα αρχεία καραντίνας καθίστανται μη διαθέσιμα. Για να διαχειριστείτε αυτά τα αρχεία, πρέπει να είναι εγκατεστημένο το Kaspersky Total Security.

 Ρυθμίσεις λειτουργίας της εφαρμογής είναι οι τιμές των ρυθμίσεων της εφαρμογής που επιλέχθηκαν κατά τη διαμόρφωση.

Μπορείτε επίσης να εξάγετε τις ρυθμίσεις προστασίας από τη γραμμή εντολών, χρησιμοποιώντας την ακόλουθη εντολή: avp.com EXPORT <file_name>.

- Δεδομένα iChecker είναι αρχεία που περιέχουν πληροφορίες σχετικά με αντικείμενα που έχουν ήδη σαρωθεί με την τεχνολογία iChecker ?.
- Οι Βάσεις δεδομένων προγράμματος Anti-Spam είναι βάσεις δεδομένων με δείγματα μηνυμάτων spam που έχει προσθέσει ο χρήστης.
- Ο όρος Κρυπτογράφηση δεδομένων αναφέρεται σε αρχεία που είναι τοποθετημένα σε θαλάμους δεδομένων για αποθήκευση.

Επιβεβαίωση κατάργησης της εφαρμογής

Επειδή η κατάργηση της εφαρμογής αποτελεί απειλή για την ασφάλεια του υπολογιστή και των προσωπικών δεδομένων σας, θα σας ζητηθεί να επιβεβαιώσετε την πρόθεσή σας να καταργήσετε την εφαρμογή. Για να γίνει αυτό, κάντε κλικ στο κουμπί **Κατάργηση**.

Ολοκλήρωση κατάργησης

Σε αυτό το βήμα, ο Οδηγός καταργεί την εφαρμογή από τον υπολογιστή σας. Περιμένετε μέχρι να ολοκληρωθεί η κατάργηση.
Αφού καταργήσετε το Kaspersky Total Security, μπορείτε να προσδιορίσετε το λόγο για τον οποίο αποφασίσατε να καταργήσετε την εφαρμογή αφήνοντας ένα σχόλιο στο δικτυακό τόπο της Kaspersky. Για να το κάνετε αυτό, πρέπει να μεταβείτε στον δικτυακό τόπο της Kaspersky κάνοντας κλικ στο κουμπί **Συμπλήρωση της φόρμας**.

Αυτή η λειτουργία ενδέχεται να μην είναι διαθέσιμη σε ορισμένες περιοχές.

Κατά την κατάργηση της εφαρμογής, θα πρέπει να επανεκκινήσετε το λειτουργικό σύστημά σας. Εάν ακυρώσετε την άμεση επανεκκίνηση, η ολοκλήρωση της διαδικασίας κατάργησης θα αναβληθεί μέχρι να γίνει επανεκκίνηση του λειτουργικού συστήματος ή μέχρι να απενεργοποιηθεί και να ενεργοποιηθεί ξανά ο υπολογιστής.

Εκχώρηση άδειας χρήσης της εφαρμογής

Η ενότητα αυτή καλύπτει τις βασικές πτυχές της άδειας χρήσης της εφαρμογής.

Πληροφορίες για την Άδεια Χρήσης Τελικού Χρήστη

Η *Άδεια Χρήσης Τελικού Χρήστη* αποτελεί μια δεσμευτική συμφωνία ανάμεσα σε εσάς και την AO Kaspersky Lab, στην οποία προσδιορίζονται οι όροι με τους οποίους μπορείτε να χρησιμοποιείτε την εφαρμογή.

Διαβάστε τους όρους της Άδειας Χρήσης προσεκτικά προτού αρχίσετε να χρησιμοποιείτε την εφαρμογή.

Κατά την εγκατάσταση της εφαρμογής, αποδέχεστε τους όρους της Άδειας Χρήσης επιβεβαιώνοντας ότι συμφωνείτε με την Άδεια Χρήσης. Αν δεν αποδέχεστε τους όρους της Άδειας Χρήσης, πρέπει να ματαιώσετε την εγκατάσταση της εφαρμογής και να μην χρησιμοποιήσετε την εφαρμογή.

Πληροφορίες για την άδεια χρήσης

Η *άδεια* χρήσης αντιπροσωπεύει ένα δικαίωμα περιορισμένου χρόνου για χρήση της εφαρμογής, το οποίο σας παρέχεται σύμφωνα με τους όρους της Άδειας χρήσης τελικού χρήστη. Η άδεια χρήσης συνδέεται με το μοναδικό κωδικό που έχετε λάβει για την ενεργοποίηση του αντιγράφου σας του Kaspersky Total Security.

Η άδεια χρήσης σας παρέχει το δικαίωμα χρήσης των εξής υπηρεσιών:

Το δικαίωμα χρήσης της εφαρμογής σε μία ή περισσότερες συσκευές

Ο αριθμός των συσκευών στις οποίες μπορείτε να χρησιμοποιήσετε την εφαρμογή καθορίζεται στην Άδεια Χρήσης Τελικού Χρήστη.

- Βοήθεια από την Τεχνική Υποστήριξη της Kaspersky
- Άλλες υπηρεσίες διαθέσιμες από την Kaspersky ή τους συνεργάτες της κατά την περίοδο ισχύος της άδειας χρήσης

Για να χρησιμοποιήσετε την εφαρμογή, θα πρέπει να αγοράσετε μια άδεια χρήσης της εφαρμογής.

Η άδεια χρήσης έχει περιορισμένη διάρκεια. Η λήξη της άδειας χρήσης μπορεί να ακολουθείται από μια περίοδο χάριτος, κατά τη διάρκεια της οποίας μπορείτε να χρησιμοποιήσετε όλες τις δυνατότητες της εφαρμογής χωρίς περιορισμούς.

Εάν δεν <u>ανανεώσετε την άδεια χρήσης σας</u>, η εφαρμογή σας θα μεταβεί στην <u>κατάσταση</u> <u>περιορισμένης λειτουργικότητας</u> όταν λήξει η περίοδος χάριτος. Στην κατάσταση περιορισμένης λειτουργικότητας δεν είναι διαθέσιμες όλες οι δυνατότητες της εφαρμογής. Η διάρκεια της κατάστασης περιορισμένης λειτουργικότητας εξαρτάται από την περιοχή και τους όρους της άδειάς σας. Όταν λήξει και η κατάσταση περιορισμένης λειτουργικότητας, όλες οι δυνατότητες της εφαρμογής θα απενεργοποιηθούν. Θα βρείτε πληροφορίες σχετικά με την περίοδο χάριτος και την κατάσταση περιορισμένης λειτουργικότητας στο παράθυρο **Εκχώρηση άδειας χρήσης**, το οποίο ανοίγει κάνοντας κλικ στη σύνδεση **Άδεια χρήσης** στο κάτω μέρος του κύριου παραθύρου.

Συνιστάται να ανανεώσετε την άδεια χρήσης πριν από τη λήξη της, ώστε να εξασφαλίσετε τη μέγιστη προστασία του υπολογιστή σας από κάθε απειλή κατά της ασφάλειάς του.

Πριν αγοράσετε άδεια χρήσης, μπορείτε να χρησιμοποιήσετε μια δωρεάν δοκιμαστική έκδοση του Kaspersky Total Security. Η δοκιμαστική έκδοση του Kaspersky Total Security παραμένει λειτουργική κατά τη διάρκεια μιας σύντομης περιόδου αξιολόγησης. Μετά τη λήξη της περιόδου αξιολόγησης, θα απενεργοποιηθούν όλες οι λειτουργίες του Kaspersky Total Security. Για να συνεχίσετε τη χρήση της εφαρμογής, πρέπει να αγοράσετε μια άδεια χρήσης.

Εάν δεν επιθυμείτε να ανανεώσετε την προστασία του υπολογιστή σας, μπορείτε να καταργήσετε το Kaspersky Total Security.

Πληροφορίες για την κατάσταση περιορισμένης λειτουργικότητας

Ο παρακάτω πίνακας παραθέτει τις δυνατότητες του Kaspersky Total Security που είναι ή δεν είναι διαθέσιμες όταν η εφαρμογή βρίσκεται σε κατάσταση περιορισμένης λειτουργικότητας. Εάν η τιμή στη στήλη κατάστασης περιορισμένης λειτουργικότητας είναι "ναι", αυτό σημαίνει ότι η αντίστοιχη δυνατότητα είναι διαθέσιμη στη λειτουργία περιορισμένης λειτουργικότητας. Εάν η τιμή στη στήλη κατάστασης περιορισμένης λειτουργικότητας είναι "όχι", η αντίστοιχη δυνατότητα δεν είναι διαθέσιμη. Επιπλέον πληροφορίες είναι διαθέσιμες στη στήλη Περιορισμοί.

Λειτουργίες του Kaspersky Total Security στην κατάσταση περιορισμένης λειτουργικότητας

Λειτουργικότητα	Περιορισμοί	Κατάσταση περιορισμένης λειτουργικότητας
Προστασία αρχείων από ιούς		ναι
Σάρωση για ιούς	Η σάρωση μπορεί να εκκινηθεί χειροκίνητα. Η προγραμματισμένη σάρωση και οι ρυθμίσεις σάρωσης δεν είναι διαθέσιμες.	ναι
Σάρωση για τρωτά σημεία		όχι
Να ενημερώσετε τις βάσεις δεδομένων και τις λειτουργικές μονάδες της εφαρμογής	Οι ρυθμίσεις δεν είναι διαθέσιμες.	ναι
Προστασία ενάντια σε προγράμματα adware και spyware		ναι
Προστασία από ιούς στο Web	Λειτουργεί με περιορισμούς.	ναι
Προστασία email από ιούς	Λειτουργεί με περιορισμούς.	ναι
Ευρετική ανάλυση	Λειτουργεί με περιορισμούς.	ναι
Προστασία κατά των rootkit		όχι
Αποτροπή εκμετάλλευσης		ναι

Παρακολούθηση συστημάτων		ναι
Προστασία κατά του phishing		ναι
Έλεγχος αξιοπιστίας αρχείων στο Kaspersky Security Network	Λειτουργεί με περιορισμούς.	ναι
Σύμβουλος URL		όχι
Ασφαλής καταχώρηση δεδομένων		όχι
Δίσκος διάσωσης	Μπορεί να πραγματοποιηθεί λήψη μέσω του περιβάλλοντος εργασίας της εφαρμογής.	ναι
Προστασία με κωδικό πρόσβασης των ρυθμίσεων της εφαρμογής	Λειτουργεί με περιορισμούς.	ναι
Απόδοση	Οι ρυθμίσεις απόδοσης της εφαρμογής μπορούν να διαμορφωθούν.	ναι
Κατάσταση παιχνιδιών	Λειτουργεί με περιορισμούς.	ναι
Απειλές και Εξαιρέσεις	Λειτουργεί με περιορισμούς.	ναι
Αυτοάμυνα	Λειτουργεί με περιορισμούς.	ναι
Καραντίνα	Λειτουργεί με περιορισμούς.	ναι
Ειδοποιήσεις	Μπορείτε να διαμορφώσετε μόνο τη ρύθμιση που ελέγχει την εμφάνιση διαφημίσεων της Kaspersky.	ναι
Διαμόρφωση της εμφάνισης της εφαρμογής	Λειτουργεί με περιορισμούς.	ναι
My Kaspersky		ναι
Αντιμετώπιση προβλημάτων των		όχι

Microsoft Windows

Έλεγχος εφαρμογών		όχι
Τείχος προστασίας		όχι
Αποκλεισμός επιθέσεων δικτύου		ναι
Πρόγραμμα Anti-Spam		όχι
Πρόγραμμα Anti-Banner		όχι
Ασφαλείς τραπεζικές συναλλαγές		όχι
Ασφαλής αναζήτηση		όχι
Ιδιωτική περιήγηση		όχι
Εκκαθάριση ιδιωτικού απορρήτου		όχι
Γονικός έλεγχος		όχι
Προστασία της Webcam		όχι
Ειδοποίηση σχετικά με τη σύνδεση σε μη ασφαλές δίκτυο Wi-Fi		όχι
Παρακολούθηση δικτύου		όχι
Διαχείριση εφαρμογών		όχι
Kaspersky Password Manager		όχι
Καθαρισμός μη χρησιμοποιούμενων δεδομένων		όχι
Καταστροφέας αρχείων		όχι
Κρυπτογράφηση δεδομένων	Είναι διαθέσιμα μόνο τα δεδομένα από θαλάμους δεδομένων που έχουν δημιουργηθεί προηγουμένως.	όχι
Δημιουργία αντιγράφων	Είναι διαθέσιμη μόνο η ανάκτηση	όχι

ασφαλείας	δεδομένων από αντίγραφα ασφαλείας που έχουν δημιουργηθεί προηγουμένως.	
My Kaspersky	Μόνο προβολή και διαχείριση των κωδικών ενεργοποίησης.	ναι
Εκκαθάριση λογισμικού υπολογιστή		όχι
Ρυθμίσεις παραμέτρων προγράμματος περιήγησης		όχι
Kaspersky VPN		όχι

Πληροφορίες για τον κωδικό ενεργοποίησης

Ο *Κωδικός ενεργοποίησης* είναι ένας κωδικός που λαμβάνετε μόλις αγοράσετε μια άδεια χρήσης για το Kaspersky Total Security. Αυτός ο κωδικός απαιτείται για την ενεργοποίηση της εφαρμογής.

Ο κωδικός ενεργοποίησης είναι μια μοναδική ακολουθία ψηφίων και λατινικών χαρακτήρων, με τη μορφή xxxxx-xxxxx-xxxxx.

Ανάλογα με τον τρόπο αγοράς της εφαρμογής, μπορείτε να αποκτήσετε τον κωδικό ενεργοποίησης με έναν από τους παρακάτω τρόπους:

- Όταν αγοράζετε τη συσκευασμένη έκδοση του Kaspersky Total Security, ο κωδικός ενεργοποίησης βρίσκεται στο εγχειρίδιο χρήσης ή στη συσκευασία λιανικής που περιέχει το CD για την εγκατάσταση.
- Όταν αγοράζετε το Kaspersky Total Security από ηλεκτρονικό κατάστημα, ο κωδικός ενεργοποίησης αποστέλλεται στη διεύθυνση που καθορίσατε κατά την παραγγελία.

Η διάρκεια ισχύος της άδειας χρήσης ξεκινά την αντίστροφη μέτρηση από την ημερομηνία που θα ενεργοποιήσετε την εφαρμογή. Εάν αγοράσατε μια άδεια χρήσης για χρήση του Kaspersky Total Security σε διάφορες συσκευές, η διάρκεια ισχύος της άδειας χρήσης ξεκινά από τη στιγμή της πρώτης εφαρμογής του κωδικού ενεργοποίησης. Σας συνιστούμε να δημιουργήσετε έναν λογαριασμό My Kaspersky, έτσι ώστε να μην χάσετε τον κωδικό ενεργοποίησης κατά την επανεγκατάσταση του λειτουργικού σας συστήματος, να εγκαταστήσετε την εφαρμογή σε μια νέα συσκευή ή να εγκαταστήσετε ξανά την εφαρμογή στην τρέχουσα συσκευή σας. Μπορείτε να δημιουργήσετε έναν λογαριασμό My Kaspersky κατά την <u>εγκατάσταση και την ενεργοποίηση της εφαρμογής</u>. Εάν δεν δημιουργήσατε λογαριασμό My Kaspersky κατά την εγκατάσταση και την ενεργοποίηση της εφαρμογής, μπορείτε επίσης να <u>δημιουργήσετε έναν λογαριασμό στην εγκατεστημένη εφαρμογή</u>.

Εάν διαγράψετε κατά λάθος ή χάσετε τον κωδικό ενεργοποίησης, μπορείτε να <u>δοκιμάσετε να</u> <u>τον επαναφέρετε</u>.

Πώς να επαναφέρετε τους κωδικούς ενεργοποίησης

Εάν χάσατε έναν κωδικό ενεργοποίησης που σας είχε δοθεί στο παρελθόν, μπορείτε να τον επαναφέρετε με τις παρακάτω μεθόδους:

- Εάν έχετε λογαριασμό My Kaspersky, μπορείτε να βρείτε τους κωδικούς ενεργοποίησής σας στην ενότητα Άδειες χρήσης της τοποθεσίας web <u>My Kaspersky</u> ^I.
- Εάν δεν έχετε λογαριασμό My Kaspersky, αλλά η εφαρμογή είναι εγκατεστημένη και ενεργοποιημένη σε μία από τις συσκευές σας, δημιουργήστε έναν <u>λογαριασμό My</u> <u>Kaspersky</u> σε αυτήν τη συσκευή και χρησιμοποιήστε τον για να συνδεθείτε στο My Kaspersky. Η εφαρμογή θα μεταδώσει πληροφορίες σχετικά με την άδεια χρήσης σας στον λογαριασμό. Ο κωδικός ενεργοποίησης θα εμφανίζεται στην ενότητα **Άδειες** χρήσης της τοποθεσία web My Kaspersky.
- Εάν δεν διαθέτετε ούτε λογαριασμό My Kaspersky ούτε έχετε ενεργοποιήσει την εφαρμογή σε κάποια από τις συσκευές σας, Επικοινωνήστε με την Τεχνική Υποστήριξη.

Μπορείτε να διαβάσετε περισσότερα σχετικά με τον <u>τρόπο επαναφοράς των κωδικών</u> ενεργοποίησης χρησιμοποιώντας το My Kaspersky 🖬.

Πληροφορίες για τη συνδρομή

Η *συνδρομή στο Kaspersky Total Security* προβλέπει τη χρήση της εφαρμογής στα πλαίσια των επιλεγμένων ρυθμίσεων (ημερομηνία λήξης και αριθμός προστατευμένων συσκευών). Μπορείτε να αποκτήσετε μια συνδρομή για το Kaspersky Total Security από ένα φορέα παροχής υπηρεσιών (για παράδειγμα, από τον παροχέα υπηρεσιών Διαδικτύου). Μπορείτε να διακόψετε ή να συνεχίσετε τη συνδρομή να επιλέξετε να ανανεώνεται αυτόματα ή να την ακυρώσετε. Μπορείτε να διαχειριστείτε τη συνδρομή σας μέσω της σελίδας του προσωπικού λογαριασμού σας στο δικτυακό τόπο του φορέα παροχής υπηρεσιών. Οι προμηθευτές μπορούν να προσφέρουν δύο τύπους συνδρομών για το Kaspersky Total Security: συνδρομές για ενημερώσεις και συνδρομές για ενημέρωση και προστασία.

Η συνδρομή μπορεί να είναι περιορισμένη (για παράδειγμα, ένα έτος) ή απεριόριστη (χωρίς ημερομηνία λήξης). Για να συνεχίσετε να χρησιμοποιείτε το Kaspersky Total Security, μετά τη λήξη της περιορισμένης συνδρομής, πρέπει να ανανεώσετε τη συνδρομή σας. Οι απεριόριστες συνδρομές ανανεώνονται αυτόματα, αρκεί να έχει προπληρωθεί εγκαίρως το αντίτιμό τους στον φορέα παροχής υπηρεσιών.

Όταν λήγει μια περιορισμένη συνδρομή, θα έχετε στη διάθεσή σας μια περίοδο χάριτος για να την ανανεώσετε. Κατά τη διάρκεια αυτής της περιόδου, δεν θα γίνουν αλλαγές στη λειτουργικότητα της εφαρμογής.

Αν η συνδρομή δεν ανανεωθεί πριν από τη λήξη της περιόδου χάριτος, το Kaspersky Total Security θα πάψει να ενημερώνει τις βάσεις δεδομένων εφαρμογών (αν έχετε συνδρομή για ενημερώσεις), θα πάψει να αλληλεπιδρά με το Kaspersky Security Network και επίσης θα πάψει να προστατεύει τον υπολογιστή και να εκτελεί εργασίες σάρωσης (αν έχετε συνδρομή για ενημερώσεις και προστασία).

Για να χρησιμοποιήσετε το Kaspersky Total Security στο πλαίσιο της συνδρομής, πρέπει να χρησιμοποιήσετε τον κωδικό ενεργοποίησης που λάβατε από το φορέα παροχής υπηρεσιών. Σε ορισμένες περιπτώσεις, ένας κωδικός ενεργοποίησης μπορεί να ληφθεί και να εφαρμοστεί αυτόματα. Όταν χρησιμοποιείτε την εφαρμογή στο πλαίσιο συνδρομής, δεν μπορείτε να χρησιμοποιήσετε άλλον κωδικό ενεργοποίησης για να ανανεώσετε την άδεια χρήσης σας. Μπορείτε να χρησιμοποιήσετε έναν άλλον κωδικό ενεργοποίησης μόνο όταν λήξει η συνδρομή σας.

Εάν το Kaspersky Total Security είναι ήδη σε χρήση στο πλαίσιο μιας τρέχουσας άδειας χρήσης όταν κάνετε εγγραφή της συνδρομής σας, όταν ολοκληρώσετε την εγγραφή σας, το Kaspersky Total Security θα χρησιμοποιείται πλέον στο πλαίσιο της συνδρομής. Ο κωδικός ενεργοποίησης που έχετε χρησιμοποιήσει για την ενεργοποίηση της εφαρμογής μπορεί να εφαρμοστεί σε άλλον υπολογιστή.

Για ακύρωση της συνδρομής σας, επικοινωνήστε με τον φορέα παροχής υπηρεσιών από τον οποίο αγοράσατε το Kaspersky Total Security.

Ανάλογα με τον πάροχο της συνδρομής, το σύνολο των επιλογών διαχείρισης εγγραφής ενδέχεται να διαφέρει. Επιπλέον, δεν μπορείτε να λάβετε περίοδο χάριτος κατά την οποία μπορείτε να ανανεώσετε τη συνδρομή σας.

Πώς να αποκτήσετε μια άδεια χρήσης

Μπορείτε να αγοράσετε μια άδεια χρήσης ή να ανανεώσετε μια ήδη υπάρχουσα. Αγοράζοντας μια άδεια χρήσης, θα λάβετε έναν κωδικό ενεργοποίησης τον οποίο πρέπει να εφαρμόσετε για να <u>ενεργοποιήσετε την εφαρμογή</u>.

Για να αποκτήσετε μια άδεια χρήσης:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Ανοίξτε το παράθυρο **Εκχώρηση άδειας χρήσης** με έναν από τους εξής τρόπους:
 - Κάνοντας κλικ στη σύνδεση Η άδεια χρήσης λείπει στο κάτω μέρος του κεντρικού παραθύρου εάν η εφαρμογή δεν έχει ενεργοποιηθεί.
 - Κάνοντας κλικ στη σύνδεση Άδεια χρήσης: Ν ημέρες απομένουν στο κάτω μέρος του κεντρικού παραθύρου εάν η εφαρμογή έχει ενεργοποιηθεί.
- 3. Στο παράθυρο που ανοίγει, κάντε κλικ στο κουμπί **Αγορά άδειας χρήσης**.

Ανοίγει ο δικτυακός τόπος του Kaspersky eStore ή μιας συνεργαζόμενης εταιρείας, από όπου μπορείτε να αγοράσετε την άδεια χρήσης.

Πώς να ενεργοποιήσετε την εφαρμογή

Για να χρησιμοποιήσετε τις δυνατότητες και τις πρόσθετες υπηρεσίες της εφαρμογής, πρέπει να την ενεργοποιήσετε.

Εάν δεν ενεργοποιήσατε την εφαρμογή κατά την εγκατάσταση, μπορείτε να το κάνετε αργότερα. Θα λάβετε υπενθύμιση για την ανάγκη ενεργοποίησης της εφαρμογής μέσω μηνυμάτων του Kaspersky Total Security που εμφανίζονται στην περιοχή ειδοποιήσεων της γραμμής εργασιών.

Για να ενεργοποιήσετε το Kaspersky Total Security:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Μεταβείτε στο παράθυρο του κωδικού ενεργοποίησης χρησιμοποιώντας μία από τις ακόλουθες μεθόδους**:**
 - Κάντε κλικ στη σύνδεση <κατάσταση άδειας χρήσης> που βρίσκεται στο κάτω μέρος του κύριου παραθύρου εφαρμογής, ανοίξτε το παράθυρο Εκχώρηση άδειας χρήσης και κάντε κλικ στο κουμπί Εισαγωγή κωδικού.

- Κάντε κλικ στη σύνδεση Η άδεια χρήσης λείπει που βρίσκεται στο κάτω μέρος του κύριου παραθύρου εφαρμογής, ανοίξτε το παράθυρο Ενεργοποίηση και κάντε κλικ στο κουμπί Εισαγωγή κωδικού.
- Στο κάτω μέρος του κύριου παραθύρου, κάντε κλικ στη σύνδεση **Εισαγωγή κωδικού**.
- 3. Στο παράθυρο **Ενεργοποίηση**, εκτελέστε τις ακόλουθες ενέργειες:
 - <u>Εάν έχετε κωδικό ενεργοποίησης</u> ?
 - a. Εισαγάγετε τον κωδικό ενεργοποίησης στο πεδίο καταχώρησης και κάντε κλικ στο κουμπί **Ενεργοποίηση**.

Αποστέλλεται αίτημα ενεργοποίησης της εφαρμογής.

b. Κάντε κλικ στο κουμπί **Ολοκληρώθηκε** στο παράθυρο **Ενεργοποίηση** για να ολοκληρώσετε τη διαδικασία εγγραφής.

Εάν δεν έχετε κωδικό ενεργοποίησης ?

- Κάντε κλικ στη σύνδεση Πού μπορώ να βρω έναν κωδικό ενεργοποίησης;, μεταβείτε στην τοποθεσία web της Γνωσιακής βάσης για να διαβάσετε σχετικά με τον τρόπο με τον οποίο μπορείτε να βρείτε τον κωδικό ενεργοποίησης σε περίπτωση που τον ξεχάσετε ή τον χάσετε.
- Κάντε κλικ στο κουμπί Αγορά άδειας χρήσης και μεταβείτε στο κατάστημα για να αγοράσετε την άδεια χρήσης της εφαρμογής.
- Κάντε κλικ στη σύνδεση Ενεργοποίηση δοκιμαστικής έκδοσης της εφαρμογής για να ενεργοποιήσετε τη δοκιμαστική έκδοση της εφαρμογής.

Πώς να ανανεώσετε μια άδεια χρήσης

Μπορείτε να ανανεώσετε την άδεια χρήσης. Για να γίνει αυτό, μπορείτε να ορίσετε ένα νέο κωδικό ενεργοποίησης, χωρίς να περιμένετε να λήξει η τρέχουσα άδεια χρήσης. Όταν λήξει η τρέχουσα άδεια χρήσης, το Kaspersky Total Security ενεργοποιείται αυτόματα χρησιμοποιώντας τον πρόσθετο κωδικό ενεργοποίησης.

Για να ορίσετε πρόσθετο κωδικό ενεργοποίησης για την αυτόματη ανανέωση της άδειας χρήσης:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Στο κάτω μέρος του κεντρικού παραθύρου, κάντε κλικ στη σύνδεση Άδεια χρήσης: Ν ημέρες απομένουν για να ανοίξετε το παράθυρο Εκχώρηση άδειας χρήσης.
- Στο παράθυρο που θα εμφανιστεί, στην ενότητα Νέος κωδικός ενεργοποίησης, κάντε κλικ στο κουμπί Εισαγωγή κωδικού.
- 4. Εισαγάγετε τον κωδικό ενεργοποίησης στα αντίστοιχα πεδία και κάντε κλικ στο κουμπί **Προσθήκη**.

Στη συνέχεια, το Kaspersky Total Security στέλνει τα δεδομένα στον διακομιστή ενεργοποίησης της Kaspersky για επαλήθευση. Μετά τη λήξη της άδειας χρήσης, ο διακομιστής ενεργοποίησης επανελέγχει τα δεδομένα κατά την πρώτη προσπάθεια ενεργοποίησης της εφαρμογής με τον νέο κωδικό ενεργοποίησης.

5. Κάντε κλικ στο κουμπί **Ολοκληρώθηκε**.

Ο νέος κωδικός ενεργοποίησης θα εμφανιστεί στο παράθυρο Εκχώρηση άδειας χρήσης.

Η εφαρμογή θα ενεργοποιηθεί αυτόματα με το νέο κωδικό ενεργοποίησης όταν λήξει η άδεια χρήσης. Μπορείτε επίσης να ενεργοποιήσετε χειροκίνητα την εφαρμογή με το νέο κωδικό ενεργοποίησης, κάνοντας κλικ στο κουμπί **Ενεργοποίηση τώρα**. Το κουμπί αυτό είναι διαθέσιμο εάν η εφαρμογή δεν έχει ενεργοποιηθεί αυτόματα. Το κουμπί αυτό δεν είναι διαθέσιμο πριν τη λήξη της άδειας χρήσης.

Εάν ο νέος κωδικός ενεργοποίησης έχει χρησιμοποιηθεί ήδη σε αυτόν ή άλλον υπολογιστή, η ημερομηνία ενεργοποίησης για την ανανέωση της άδειας χρήσης θα είναι η ημερομηνία πρώτης ενεργοποίησης της εφαρμογής με τον συγκεκριμένο κωδικό.

Όταν ανανεώνετε την τρέχουσα άδεια χρήσης, ο κωδικός ενεργοποίησης δεν αλλάζει. Η άδεια χρήσης θα ανανεωθεί αυτόματα στην εφαρμογή μετά την αγορά. Δεν χρειάζεται να εισαγάγετε ξανά τον κωδικό ενεργοποίησης στην εφαρμογή.

Μπορεί να χρειαστούν έως και 24 ώρες μετά την αγορά πριν εμφανιστεί η σωστή κατάσταση της άδειας χρήσης.

Παροχή δεδομένων

Αυτή η ενότητα περιέχει πληροφορίες σχετικά με τα καθορισμένα δεδομένα που παρέχετε στη Kaspersky. Η υποενότητα <u>Αποθήκευση δεδομένων στην αναφορά λειτουργίας της</u> <u>εφαρμογής</u> περιέχει δεδομένα που αποθηκεύονται τοπικά στον υπολογιστή σας και δεν αποστέλλονται στην Kaspersky.

Παροχή δεδομένων υπό τους όρους της Άδειας Χρήσης Τελικού Χρήστη

Αυτή η ενότητα περιέχει πληροφορίες σχετικά με τα καθορισμένα δεδομένα που παρέχονται στην Kaspersky εάν έχετε εγκαταστήσει την έκδοση της εφαρμογής που δεν προορίζεται για χρήση στην Ευρωπαϊκή Ένωση, τη Μεγάλη Βρετανία, τη Βραζιλία ή από κατοίκους της πολιτείας της Καλιφόρνια.

Συμφωνείτε να υποβάλετε αυτόματα τις ακόλουθες πληροφορίες στην ΑΟ Kaspersky Lab μέσω του εγκατεστημένου λογισμικού (εφεξής "το Λογισμικό"), του οποίου τα δικαιώματα ανήκουν στην ΑΟ Kaspersky Lab (εφεξής "Kaspersky" ή "ο Δικαιούχος"), για σκοπούς βελτίωσης της ποιότητας της προστασίας πραγματικού χρόνου, για δημιουργία των πλέον κατάλληλων ενημερωτικών και διαφημιστικών προσφορών, για βελτίωση της λειτουργίας του λογισμικού και έγκαιρο εντοπισμό και διόρθωση των σφαλμάτων που σχετίζονται με τον μηχανισμό για την εγκατάσταση, κατάργηση και ενημέρωση του λογισμικού και για καταμέτρηση του αριθμού των χρηστών:

 Πληροφορίες σχετικά με το εγκατεστημένο Λογισμικό του Κατόχου δικαιωμάτων: πλήρης έκδοση του Λογισμικού, αναγνωριστικό ενημέρωσης Λογισμικού, τύπος του εγκατεστημένου Λογισμικού, Αναγνωριστικό εγκατάστασης Λογισμικού (PCID), ημερομηνία και ώρα εγκατάστασης του Λογισμικού, αναγνωριστικό Λογισμικού που προέρχεται από την άδεια χρήσης, αναγνωριστικό του Λογισμικού με άδεια χρήσης, τοπική προσαρμογή Λογισμικού, σημαία που υποδεικνύει αν είναι ενεργοποιημένο η συμμετοχή στο KSN, αναγνωριστικό αλλαγής εταιρικής επωνυμίας Λογισμικού, κατάσταση εγκατάστασης/απεγκατάστασης Λογισμικού, κωδικός σφάλματος εγκατάστασης, αναγνωριστικό Λογισμικού, αναγνωριστικό αλλαγής εταιρικής επωνυμίας του Λογισμικού, τύπος εγκατάστασης (νέα εγκατάσταση, ενημέρωση), τύποι λογισμικού τρίτου μέρους που προτάθηκαν για εγκατάσταση κατά την εγκατάσταση του Λογισμικού, τύποι λογισμικού τρίτου μέρους που επιλέχθηκαν για εγκατάσταση κατά την εγκατάσταση του Λογισμικού, τύποι λογισμικού τρίτου μέρους που εγκαταστάθηκαν κατά την εγκατάσταση του Λογισμικού, αναγνωριστικό χρήστη του δικτυακού τόπου του Κατόχου Δικαιωμάτων, διάρκεια εγκατάστασης του Λογισμικού σε δευτερόλεπτα, σημαία που υποδεικνύει εάν η εγκατάσταση ματαιώθηκε από τον χρήστη, αναγνωριστικό Λογισμικού, κωδικός του συνεργάτη οργανισμού που σχετίζεται με την αλλαγή της εταιρικής επωνυμίας του Λογισμικού, πληροφορίες σχετικά με στοιχείο του περιβάλλοντος εργασίας από το οποίο ο χρήστης αποφάσισε να αγοράσει το Λογισμικό, τύπος ιστορίας χρήστη, πλήρες όνομα του συνεργάτη οργανισμού μέσω του οποίου υποβλήθηκε η παραγγελία άδειας χρήσης Λογισμικού,

- Άλλες πληροφορίες: πρωτόκολλο που χρησιμοποιείται για την ανταλλαγή δεδομένων με το KSN, καθυστέρηση στην αποστολή των στατιστικών στοιχείων, αναγνωριστικό της καμπάνιας μάρκετινγκ, έκδοση πρωτοκόλλου αλληλεπίδρασης μεταξύ του Λογισμικού και των μηνυμάτων μάρκετινγκ, αναγνωριστικό σελίδας, τύπος καταχώρησης Δικτυακής Πύλης, αναγνωριστικό του ελέγχου στο περιβάλλον εργασίας χρήστη, αναγνωριστικό ενέργειας του χρήστη, email χρήστη που καταχωρήθηκε κατά τη δημιουργία παραγγελίας στο περιβάλλον εργασίας του λογισμικού, τύπος του αιτήματος, μέγεθος περιεχομένου του αιτήματος, αναγνωριστικό πρωτοκόλλου, τύπος συμπίεσης δεδομένων, αναγνωριστικό της επιλογής του χρήστη στην καμπάνια μάρκετινγκ, επιλογή χρήστη στην καμπάνια μάρκετινγκ, τύπος της περιοχής στην οποία παρουσιάστηκε το συμβάν, λίστα αναγνωριστικού του περιεχομένου που έχει διαβάσει ο χρήστης,
- Πληροφορίες σχετικά με το περιβάλλον Χρήστη: κατάσταση ενεργοποίησης Διαφύλαξης συσκευής (Windows), αναγνωριστικό συσκευής, εξωτερική διεύθυνση IP, μοναδικό αναγνωριστικό συσκευής, τύπος λειτουργικού συστήματος (διακομιστής, σταθμός εργασίας, ελεγκτής τομέα), έκδοση λειτουργικού συστήματος, αριθμός κατασκευής λειτουργικού συστήματος, αριθμός ενημέρωσης λειτουργικού συστήματος, ειδική έκδοση λειτουργικού συστήματος σχετικά με την έκδοση λειτουργικού συστήματος, ειδική έκδοση λειτουργικού συστήματος, εκτεταμένες πληροφορίες σχετικά με την έκδοση λειτουργικού συστήματος, τύπος πλατφόρμας υλικού, επιπρόσθετες πληροφορίες σχετικά με λειτουργίες του λειτουργικού συστήματος, οικογένεια λειτουργικού συστήματος, τύπος πλατφόρμας υλικού, επιπρόσθετες πληροφορίες σχετικά με λειτουργίες του λειτουργικού συστήματος, τύπος προγράματος, τύπος προγράματος, τύπος προγογιστής, του λειτουργικού συστήματος, αριθμός ενημέρωσης λειτουργικού συστήματος, οικογένεια δειτουργικού συστήματος, τύπος πλατφόρμας υλικού, επιπρόσθετες πληροφορίες σχετικά με του λειτουργίες του λειτουργικού συστήματος, τύπος προγράμας του χρήστη, ημερομηνία και ώρα στη συσκευή του χρήστη,
- Πληροφορίες σχετικά με ένα αντικείμενο που υποβάλλεται σε επεξεργασία: άθροισμα ελέγχου (MD5) του αντικειμένου που υποβάλλεται σε επεξεργασία, άθροισμα ελέγχου (SHA256) του αντικειμένου που υποβάλλεται σε επεξεργασία, άθροισμα ελέγχου τμημάτων του αντικειμένου που σαρώνεται για τον ταχύ εντοπισμό κακόβουλου λογισμικού ή του νόμιμου λογισμικού που μπορούν να χρησιμοποιηθούν για την πρόκληση βλάβης στον υπολογιστή ή στα δεδομένα του χρήστη, δημόσιο κλειδί του πιστοποιητικού, αποτύπωμα ψηφιακού πιστοποιητικού του αντικειμένου που υποβάλλεται σε σάρωση και του αλγορίθμου κλειδώματος, όνομα του εντοπισμένου κακόβουλου λογισμικού ή του νόμιμου λογισμικού που μπορεί να χρησιμοποιηθεί για την πρόκληση βλάβης στη συσκευή ή στα δεδομένα του χρήστη, χρονική σήμανση της εγγραφής που ενεργοποιήθηκε στις βάσεις δεδομένων προστασίας από ιούς του Λογισμικού, αναγνωριστικό της εγγραφής που ενεργοποιήθηκε στις βάσεις δεδομένων προστασίας από ιούς του Λογισμικού, τύπος της εγγραφής που ενεργοποιήθηκε στις βάσεις δεδομένων προστασίας από ιούς του Λογισμικού, μέγεθος του αντικειμένου που υποβάλλεται σε επεξεργασία, όνομα του αντικειμένου που υποβάλλεται σε επεξεργασία, διαδρομή του αντικειμένου που υποβάλλεται σε επεξεργασία, κωδικός καταλόγου, αναγνωριστικό της ευπάθειας που εντοπίστηκε στις ρυθμίσεις λογισμικού, τύπος αθροίσματος ελέγχου του αντικειμένου που υποβάλλεται σε επεξεργασία,

- Πληροφορίες σχετικά με την πρόσβαση σε υπηρεσία web: διεύθυνση web που υποβάλλεται σε επεξεργασία, αριθμός θύρας, διεύθυνση web της προέλευσης του αιτήματος υπηρεσίας web (αναφορά), διεύθυνση IPv4 της υπηρεσίας web στην οποία πραγματοποιήθηκε πρόσβαση, τύπος πιστοποιητικού,
- Πληροφορίες σχετικά με την άδεια χρήσης και άλλες συμφωνίες: τύπος της νομικής συμφωνίας που έγινε αποδεκτή από τον χρήστη κατά τη χρήση του Λογισμικού, έκδοση της νομικής συμφωνίας που έγινε αποδεκτή από τον χρήστη κατά τη χρήση του Λογισμικού, σημαία που υποδεικνύει αν ο χρήστης έχει αποδεχθεί τους όρους της νομικής συμφωνίας κατά τη χρήση του Λογισμικού, ημερομηνία και ώρα αποδοχής των όρων της Συμφωνίας από τον χρήστη κατά τη χρήση του Λογισμικού, ημερομηνία ενεργοποίησης Λογισμικού, σειριακός αριθμός του κλειδιού άδειας χρήσης του Λογισμικού, αναγνωριστικό άδειας χρήσης Λογισμικού, αναγνωριστικό του μοντέλου πληροφοριών που χρησιμοποιείται για την παροχή της άδειας χρήσης του Λογισμικού, τύπος της άδειας χρήσης του Λογισμικού που χρησιμοποιείται, διάρκεια ισχύος της άδειας χρήσης του Λογισμικού, αριθμός ημερών έως τη λήξη της άδειας χρήσης του Λογισμικού, πλήρες όνομα του συνεργάτη οργανισμού μέσω του οποίου υποβλήθηκε η παραγγελία άδειας χρήσης του Λογισμικού, πληροφορίες σχετικά με τη δοκιμαστική έκδοση Λογισμικού, τρέχουσα κατάσταση του κλειδιού άδειας χρήσης του Λογισμικού, αριθμός παραγγελίας μέσω της οποίας αγοράστηκε η άδεια χρήσης του Λογισμικού, αναγνωριστικό στοιχείου της λίστας τιμών μέσω του οποίου αγοράστηκε η άδεια χρήσης του Λογισμικού, αριθμός παραγγελίας της αγοράς άδειας χρήσης του Λογισμικού από τον συνεργάτη, αναγνωριστικό της χώρας του συνεργάτη που πούλησε την άδεια χρήσης του Λογισμικού, δεδομένα σχετικά με την άδεια χρήσης για την αναγνώριση μιας ομάδας χρηστών της εταιρείας που αγόρασε την άδεια χρήσης μέσω του σχολίου στις ιδιότητες της άδειας χρήσης, Ημερομηνία και ώρα λήξης της άδειας χρήσης Λογισμικού, τρέχουσα κατάσταση συνδρομής του Λογισμικού, αιτία της τρέχουσας/μεταβαλλόμενης κατάστασης της συνδρομής του Λογισμικού, τύπος συνδρομής του Λογισμικού, ημερομηνία και ώρα λήξης της συνδρομής του Λογισμικού, δεδομένα άδειας χρήσης για αναγνώριση ομάδας χρηστών που βασίζεται σε επιπρόσθετες ρυθμίσεις της άδειας χρήσης συνδρομής, δεδομένα άδειας χρήσης του Λογισμικού για αναγνώριση ομάδας χρηστών που βασίζεται σε επιπρόσθετες ρυθμίσεις της άδειας χρήσης συνδρομής, δεδομένα άδειας χρήσης για αναγνώριση ομάδας χρηστών που βασίζεται σε επιπρόσθετες ρυθμίσεις της άδειας χρήσης συνδρομής, αριθμός ημερών από την ενεργοποίηση του Λογισμικού, αριθμός ημερών από τη λήξη του κλειδιού άδειας χρήσης του Λογισμικού, πληροφορίες σχετικά με σφάλμα ενεργοποίησης Λογισμικού, κατηγορία σφάλματος ενεργοποίησης του Λογισμικού, κωδικός σφάλματος ενεργοποίησης του Λογισμικού, αγορασμένοι κωδικοί ενεργοποίησης, ρύθμιση αναγνωριστικών του Λογισμικού που μπορούν να ενεργοποιηθούν στη συσκευή του χρήστη, κωδικός ενεργοποίησης Λογισμικού, κωδικός ενεργοποίησης Λογισμικού που βρίσκεται σε χρήση αυτήν τη στιγμή, Κεφαλίδα άδειας χρήσης Λογισμικού, αναγνωριστικό τοπικού κέντρου ενεργοποίησης, Ημερομηνία και ώρα δημιουργίας του κλειδιού άδειας χρήσης του Λογισμικού, τύπος της άδειας χρήσης που χρησιμοποιήθηκε για την ενεργοποίηση του Λογισμικού, αναγνωριστικό του στοιχείου λιανικής Λογισμικού (SKU),

- Πληροφορίες σχετικά με την αλληλεπίδραση με Δικτυακή Πύλη: αναγνωριστικό λογαριασμού Δικτυακής Πύλης, σελίδα τοποθεσίας web Δικτυακής Πύλης στην οποία ανακατευθύνει το Λογισμικό, χώρα και περιοχή της υπηρεσίας web της Kaspersky Lab από την οποία πραγματοποιήθηκε λήψη της δοκιμαστικής έκδοσης του Λογισμικού, χρόνος της τελευταίας αλλαγής κατάστασης, έκδοση του χρησιμοποιούμενου πρωτοκόλλου για τον έλεγχο των ρυθμίσεων Λογισμικού από τη Δικτυακή Πύλη, κατάσταση προστασίας συσκευής, κατάσταση χρήσης στοιχείων προστασίας, κατάσταση εργασιών σάρωσης, κατάσταση της εργασίας ενημέρωσης των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής, λίστα προβλημάτων ασφάλειας, περιεχόμενα των συστάσεων για την ενότητα της λίστας προβλημάτων, κατάσταση της άδειας χρήσης που χρησιμοποιείται από το Λογισμικό, τρόπος λειτουργίας του Λογισμικού, πληροφορίες σχετικά με την ενημέρωση βάσεων δεδομένων και λειτουργικών μονάδων της εφαρμογής, λίστα προβλημάτων ασφάλειας που έχουν αγνοηθεί, αναγνωριστικό χρήστη που εκδόθηκε μετά από επιτυχημένη επαλήθευση ταυτότητας σε Δικτυακή Πύλη, κωδικός πρόσβασης μίας χρήσης για αυτόματη σύνδεση του Λογισμικού που λήφθηκε από τον λογαριασμό της Δικτυακής Πύλης, κωδικός πρόσβασης μίας χρήσης για εγγραφή συσκευής σε Δικτυακή Πύλη, όνομα υπολογιστή στο δίκτυο (όνομα τομέα), τύπος της συσκευής που συνδέθηκε σε Δικτυακή Πύλη, αιτία αποσύνδεσης από Δικτυακή Πύλη, τύπος διακριτικού, δεδομένα για τη λήψη ενός διακριτικού ελέγχου ταυτότητας για την περίοδο λειτουργίας,
- Πληροφορίες σχετικά με την ενημέρωση τοπικών βάσεων δεδομένων: αναγνωριστικό της έναρξης ενημέρωσης Λογισμικού.

Πρόσθετες πληροφορίες

- Πληροφορίες σχετικά με το υλικολογισμικό που είναι εγκατεστημένο στον υπολογιστή, συμπεριλαμβανομένων των πληροφοριών για τον κατασκευαστή, το μοντέλο και τη χωρητικότητα του σκληρού δίσκου (HDD), το μέγεθος της φυσικής και εικονικής μνήμης, τον κατασκευαστή της μνήμης RAM, τον κατασκευαστή της μητρικής πλακέτας, τον κατασκευαστή και το όνομα της εφαρμογής BIOS, τον κατασκευαστή και το μοντέλο της κάρτας γραφικών και το μέγεθος της μνήμης RAM για βίντεο, τον κατασκευαστή και το του προσαρμογέα δικτύου, την ταχύτητα μετάδοσης δεδομένων του, τον κατασκευαστή και το όνομα της οθόνης, το αναγνωριστικό της εγκατάστασης λογισμικού και το μοναδικό αναγνωριστικό του υπολογιστή.
- Πληροφορίες σχετικά με τις συσκευές USB που είναι συνδεδεμένες στον υπολογιστή: την κατηγορία / το μοντέλο της συσκευής USB, τον κατασκευαστή και το όνομα της συσκευής, την ημερομηνία της πιο πρόσφατης σύνδεσης της συσκευής στον υπολογιστή.
- Πληροφορίες σχετικά με συσκευές που υποστηρίζουν το πρωτόκολλο UPnP,
 συμπεριλαμβανομένου του ονόματος του κατασκευαστή και του ονόματος της συσκευής,
 καθώς και της ημερομηνίας της πιο πρόσφατης σύνδεσης.

- Πληροφορίες σχετικά με τη φόρτωση του συστήματος, συμπεριλαμβανομένης της ελεύθερης μνήμης και της μνήμης που χρησιμοποιείται και του μεγέθους του ελεύθερου χώρου στο δίσκο.
- Πληροφορίες σχετικά με όλες τις εγκατεστημένες εφαρμογές, συμπεριλαμβανομένου του ονόματος και της έκδοσης της εγκατεστημένης εφαρμογής, των εκδόσεων των εγκατεστημένων ενημερώσεων, το όνομα του εκδότη, την ημερομηνία της εγκατάστασης και την πλήρη διαδρομή προς τον φάκελο εγκατάστασης στον υπολογιστή, τη ρύθμιση παραμέτρων (ρυθμίσεις) της εφαρμογής (συμπεριλαμβανομένων των προγραμμάτων περιήγησης).
- Πληροφορίες σχετικά με τις εκδόσεις του λειτουργικού συστήματος (ΛΣ) και των service pack που είναι εγκατεστημένα στον υπολογιστή, το όνομα του υπολογιστή στο δίκτυο (τοπικό όνομα και όνομα τομέα), τοπικές ρυθμίσεις του λειτουργικού συστήματος (πληροφοριών για τη ζώνη ώρας, των προεπιλεγμένων μορφών πληκτρολογίου, της γλώσσας περιβάλλοντος εργασίας), ρυθμίσεις UAC, ρυθμίσεις τείχους προστασίας δικτύου του λειτουργικού συστήματος και του δείκτη δραστηριοτήτων του, ρυθμίσεις γονικού ελέγχου του λειτουργικού συστήματος και λογαριασμός χρήστη.
- Όνομα και τοποθεσία οποιουδήποτε αρχείου στον υπολογιστή.
- Συγκεντρωτικές πληροφορίες σχετικά με τη δραστηριότητα του χρήστη στον υπολογιστή, η διάρκεια αλληλεπίδρασης του χρήστη με τον υπολογιστή, η περίοδος συγκέντρωσης πληροφοριών, ο συνολικός αριθμός συμβάντων κατά τη διάρκεια αυτής της περιόδου, συγκεντρωτικές πληροφορίες σχετικά με τις διεργασίες που εκκινήθηκαν από τον χρήστη στο σύστημα, το όνομα της διεργασίας, ο συνολικός αριθμός των φορών που εκτελέστηκε η διεργασία, η συνολική διάρκεια λειτουργίας της, το άθροισμα ελέγχου (checksum) (CRC64) του ονόματος του λογαριασμού από τον οποίο εκκινήθηκε η διεργασία, η πλήρης διαδρομή στο αρχείο της διεργασίας, πληροφορίες σχετικά με το λογισμικό με το οποίο συσχετίζεται η διεργασία (όνομα, περιγραφή, κατασκευαστής και έκδοση), ο συνολικός αριθμός των φορών που προβλήθηκε το παράθυρο του λογισμικού, η συνολική διάρκεια προβολής του, στατιστικές παράμετροι για το όνομα του παραθύρου, το όνομα.
- Πληροφορίες σχετικά με επισκέψεις σε τοποθεσίες web, η διεύθυνση της τοποθεσίας web, τμήματα τομέα των διευθύνσεων web που ο Χρήστης εισήγαγε στη γραμμή διεύθυνσης του προγράμματος περιήγησης ή που ο Χρήστης άνοιξε από συστήματα αναζήτησης.

Η βασική λειτουργικότητα του Λογισμικού όπως περιγράφεται στο Εγχειρίδιο Χρήστη αφορά την προστασία του Τελικού Χρήστη από γνωστές απειλές ασφάλειας των πληροφοριών. Για διασφαλίζεται ότι αυτές οι βασικές λειτουργικές δυνατότητες παρέχονται στο λογισμικό που χρησιμοποιείτε, ο Κάτοχος δικαιωμάτων πρέπει να λάβει και να επεξεργαστεί τις ακόλουθες πληροφορίες:

- Πληροφορίες σχετικά με το στοιχείο Πρόγραμμα Anti-Spam: ευρετικά καθορισμένη διεύθυνση IP του αποστολέα με βάση τις κεφαλίδες που λαμβάνονται και τις κεφαλίδες περιόδου λειτουργίας SMTP, η πιο πιθανή διεύθυνση IP του αποστολέα ανεπιθύμητων μηνυμάτων, άθροισμα ελέγχου του επεξεργασμένου αντικειμένου (MD5), αθροίσματα ελέγχου συνημμένων, καθορισμένες κατηγορίες κειμένου ενός μηνύματος email, διευθύνσεις web που εντοπίστηκαν στο επεξεργασμένο μήνυμα email, μεταδεδομένα και τμήματα του επεξεργασμένου μηνύματος email που θα ελεγχθούν στις υπηρεσίες του Κατόχου δικαιωμάτων.
- Πληροφορίες σχετικά με το περιβάλλον Χρήστη: όνομα δικτύου Wi-Fi, άθροισμα ελέγχου (MD5 με salt) της διεύθυνσης MAC του σημείου πρόσβασης, άθροισμα ελέγχου (SHA256 με salt) της διεύθυνσης MAC του σημείου πρόσβασης, τύπος ελέγχου ταυτότητας δικτύου Wi-Fi, τύπος κρυπτογράφησης δικτύου Wi-Fi, αναγνωριστικό δικτύου Wi-Fi με βάση τη διεύθυνση MAC του σημείου πρόσβασης, αναγνωριστικό δικτύου Wi-Fi με βάση το όνομα δικτύου Wi-Fi, αναγνωριστικό δικτύου Wi-Fi με βάση το όνομα δικτύου Wi-Fi και τη διεύθυνση MAC του σημείου πρόσβασης, ισχύς σήματος Wi-Fi, λίστα των διαθέσιμων δικτύων Wi-Fi και των ρυθμίσεών τους, ρυθμίσεις DHCP (αθροίσματα ελέγχου τοπικής διεύθυνσης IP της πύλης, DHCP IP, DNS1 IP, DNS2 IP και μάσκα υποδικτύου), ρυθμίσεις DHCP (αθροίσματα ελέγχου τοπικής IPv6 πύλης, DHCP IPv6, DNS1 IPv6, DNS2 IPv6, μάσκα υποδικτύου), URL της υπηρεσίας που χρησιμοποιείται για πρόσβαση στο διαδίκτυο.

Η Kaspersky Lab προστατεύει τις πληροφορίες που λαμβάνει όπως προβλέπεται από τον νόμο και σύμφωνα με τους ισχύοντες κανόνες της Kaspersky. Τα δεδομένα μεταδίδονται μέσω κρυπτογραφημένων καναλιών.

Προκειμένου να βελτιώσουμε την κατανόηση της ασφάλειας σχετικά με νέες απειλές και τις πηγές τους και για να βελτιώσουμε το επίπεδο προστασίας της ασφάλειάς Σας και τη λειτουργία του προϊόντος, ο Κάτοχος δικαιωμάτων, με τη συγκατάθεσή σας που έχει επιβεβαιωθεί ρητά στη Δήλωση Συλλογής δεδομένων, δικαιούται ρητά να λαμβάνει τέτοιες πληροφορίες. Μπορείτε να απενεργοποιήσετε την υπηρεσία Kaspersky Security Network κατά την εγκατάσταση. Επίσης, μπορείτε να ενεργοποιήσετε και απενεργοποιήσετε την υπηρεσία του Δικτύου Ασφαλείας της Kaspersky σε οποιαδήποτε στιγμή από τη σελίδα επιλογών του Λογισμικού.

Αποδέχεστε και συμφωνείτε περαιτέρω ότι οποιεσδήποτε πληροφορίες που συλλέγονται από τον Κάτοχο Δικαιωμάτων μπορούν να χρησιμοποιηθούν για την παρακολούθηση και δημοσίευση αναφορών σχετικά με τάσεις κινδύνων ασφάλειας κατά την αποκλειστική διακριτική ευχέρεια του Κατόχου Δικαιωμάτων. Εάν δεν θέλετε οι πληροφορίες που συλλέγονται από το λογισμικό να αποστέλλονται στον Κάτοχο δικαιωμάτων, δεν πρέπει να ενεργοποιήσετε ή/και θα πρέπει να απενεργοποιήσετε την υπηρεσία Kaspersky Security Network.

Παροχή δεδομένων υπό τους όρους της Άδειας Χρήσης Τελικού Χρήστη εντός της επικράτειας της Ευρωπαϊκής Ένωσης, του Ηνωμένου Βασιλείου Μεγάλης Βρετανίας ή από κατοίκους της πολιτείας της Καλιφόρνια

Αυτή η ενότητα περιέχει πληροφορίες σχετικά με τα καθορισμένα δεδομένα που παρέχονται στην Kaspersky εάν έχετε εγκαταστήσει την έκδοση της εφαρμογής που προορίζεται για χρήση στην Ευρωπαϊκή Ένωση, τη Μεγάλη Βρετανία, τη Βραζιλία ή από κατοίκους της πολιτείας της Καλιφόρνια. **Οι πληροφορίες που αναφέρονται σε αυτήν την ενότητα δεν περιέχουν προσωπικά δεδομένα του Χρήστη και είναι απαραίτητες για τη λειτουργία του Λογισμικού του Δικαιούχου, εκτός εάν ρητώς ορίζεται διαφορετικά**.

Συμφωνείτε να παρέχετε στην Kaspersky, αυτόματα κατά τη χρήση του λογισμικού, τα ακόλουθα δεδομένα για βελτίωση της ποιότητας της προστασίας σε πραγματικό χρόνο, για βελτίωση της λειτουργίας του λογισμικού και έγκαιρο εντοπισμό και διόρθωση των σφαλμάτων που σχετίζονται με τον μηχανισμό για την εγκατάσταση, κατάργηση και ενημέρωση του λογισμικού και για καταμέτρηση του αριθμού των χρηστών:

- Πληροφορίες σχετικά με το εγκατεστημένο λογισμικό του Κατόχου δικαιωμάτων: πλήρης έκδοση του λογισμικού, αναγνωριστικό ενημέρωσης λογισμικού, τύπος του εγκατεστημένου λογισμικού, κατάσταση εγκατάστασης/απεγκατάστασης του λογισμικού, κωδικός σφάλματος εγκατάστασης, αναγνωριστικό λογισμικού, αναγνωριστικό αλλαγής εταιρικής επωνυμίας του λογισμικού, τοπική προσαρμογή λογισμικού, κωδικός αλλαγής εταιρικής επωνυμίας του λογισμικού, τύπος λειτουργικού συστήματος (διακομιστής, σταθμός εργασίας, ελεγκτής τομέα), τύπος εγκατάστασης (νέα εγκατάσταση, αναβάθμιση), διάρκεια εγκατάστασης του λογισμικού σε δευτερόλεπτα, ένδειξη διακοπής εγκατάστασης από τον χρήστη.
- Άλλες πληροφορίες: πρωτόκολλο που χρησιμοποιείται για τη μετάδοση δεδομένων στο KSN.
- Πληροφορίες σχετικά με το περιβάλλον χρήστη: ένδειξη ότι το στοιχείο Device Guard (Windows) είναι ενεργοποιημένο, οικογένεια λειτουργικού συστήματος, έκδοση λειτουργικού συστήματος, αριθμός δομής λειτουργικού συστήματος, αριθμός ενημέρωσης λειτουργικού συστήματος, ειδική έκδοση λειτουργικού συστήματος, εκτεταμένες πληροφορίες σχετικά με την έκδοση λειτουργικού συστήματος, τύπος πλατφόρμας υλικού, πρόσθετες πληροφορίες για τις δυνατότητες του λειτουργικού συστήματος, τύπος συσκευής (φορητός υπολογιστής, επιτραπέζιος υπολογιστής, tablet).

- Πληροφορίες σχετικά με το επεξεργασμένο αντικείμενο: δημόσιο κλειδί του πιστοποιητικού, αποτύπωμα ψηφιακού πιστοποιητικού του σαρωμένου αντικειμένου και αλγόριθμος κλειδώματος, όνομα του εντοπισμένου κακόβουλου λογισμικού ή της νόμιμης εφαρμογής που μπορεί να χρησιμοποιηθεί για την πρόκληση βλάβης στη συσκευή ή στα δεδομένα του χρήστη, χρονική σήμανση της εγγραφής που ενεργοποιήθηκε στις βάσεις δεδομένων προστασίας από ιούς του λογισμικού, αναγνωριστικό της εγγραφής που ενεργοποιήθηκε στις βάσεις της εγγραφής που ενεργοποιήθηκε στις βάσεις δεδομένων προστασίας από ιούς του λογισμικού, τύπος της εγγραφής που ενεργοποιήθηκε στις βάσεις δεδομένων που ενεργοποιήθηκε στις βάσεις δεδομένου και αναγνωριστικό της εγγραφής του ενεργοποιήθηκε στις βάσεις δεδομένων προστασίας από ιούς του λογισμικού, τύπος της εγγραφής που ενεργοποιήθηκε στις βάσεις βασεις δεδομένων προστασίας από ιούς του λογισμικού, τύπος της εγγραφής που ενεργοποιήθηκε στις βάσεις βασεις δεδομένων προστασίας από ιούς του λογισμικού.
- Πληροφορίες σχετικά με αιτήματα υπηρεσίας web: επεξεργασμένη διεύθυνση web, διεύθυνση IP (IPv4) της υπηρεσίας web που ζητήθηκε, τύπος πιστοποιητικού.
- Πληροφορίες σχετικά με την άδεια χρήσης και άλλες συμφωνίες: Αναγνωριστικό λιανικής πώλησης λογισμικού, τύπος χρησιμοποιούμενης άδειας χρήσης λογισμικού, διάρκεια ισχύος της άδειας χρήσης λογισμικού, αριθμός ημερών που απομένουν έως τη λήξη της άδειας χρήσης λογισμικού, πλήρες όνομα του οργανισμού συνεργάτη που έλαβε την παραγγελία για την άδεια χρήσης λογισμικού.

Για να βελτιωθεί η ποιότητα προστασίας του Χρήστη που πραγματοποιεί συναλλαγές πληρωμής στο Διαδίκτυο, συμφωνείτε να παρέχετε αυτόματα στη χρηματοοικονομική τοποθεσία web τις πληροφορίες σχετικά με το όνομα και την έκδοση του Λογισμικού και τη ρύθμιση προσαρμογής του Λογισμικού, το αναγνωριστικό (ID) της προσθήκης του Λογισμικού στο πρόγραμμα περιήγησης που χρησιμοποιείται για την πρόσβαση στη χρηματοοικονομική τοποθεσία web και το αναγνωριστικό (ID) που δείχνει εάν χρησιμοποιήθηκε ένα ασφαλές ή κοινό πρόγραμμα περιήγησης.

Οι πληροφορίες που λαμβάνονται προστατεύονται από τον Δικαιούχο κατά τον τρόπο που προβλέπεται από τη νομοθεσία και είναι απαραίτητες για τη λειτουργία του Λογισμικού που τίθεται σε διαθεσιμότητα για χρήση υπό τους όρους της άδειας χρήσης.

Η Kaspersky μπορεί να χρησιμοποιήσει τα στατιστικά δεδομένα που αποκτήθηκαν με βάση τις πληροφορίες που λαμβάνει, για να παρακολουθεί τις τάσεις απειλών ως προς την ασφάλεια του υπολογιστή και για να δημοσιεύει αναφορές σχετικά με αυτές.

Παροχή δεδομένων στο Kaspersky Security Network

Το πεδίο εφαρμογής των δεδομένων που μεταβιβάζονται στο Kaspersky Security Network περιγράφεται στη Δήλωση για το Kaspersky Security Network.

Για να δείτε τη Δήλωση για το Kaspersky Security Network:

1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.

- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Στο παράθυρο **Ρυθμίσεις**, επιλέξτε την ενότητα **Προστασία**.
- 4. Στην ενότητα **Προστασία**, επιλέξτε το στοιχείο Kaspersky Security Network. Ανοίγει το παράθυρο **Kaspersky Security Network**.
- 5. Κάντε κλικ στη σύνδεση **Δήλωση για το Kaspersky Security Network** για να ανοίξετε το κείμενο της Δήλωσης του Kaspersky Security Network.

Αποθήκευση δεδομένων στην αναφορά λειτουργίας της εφαρμογής

Τα αρχεία αναφορών μπορεί να περιέχουν προσωπικά δεδομένα που λαμβάνονται κατά τη διάρκεια της λειτουργίας των στοιχείων προστασίας, όπως η Προστασία αρχείων από ιούς, η Προστασία email από ιούς, η Προστασία από ιούς στο Web, το Πρόγραμμα Anti-Spam και ο Γονικός έλεγχος.

Τα αρχεία αναφορών μπορεί να περιέχουν τα εξής προσωπικά δεδομένα:

- Διεύθυνση IP της συσκευής του χρήστη
- Ιστορικό περιήγησης στο διαδίκτυο
- Αποκλεισμένες συνδέσεις
- Εκδόσεις του προγράμματος περιήγησης και του λειτουργικού συστήματος
- Ονομασίες των cookie και άλλων αρχείων, καθώς και διαδρομές προς αυτά
- Διεύθυνση ηλεκτρονικού ταχυδρομείου, αποστολέας, θέμα μηνύματος, κείμενο μηνύματος, ονόματα χρήστη και λίστα επαφών

Τα αρχεία αναφορών αποθηκεύονται τοπικά στον υπολογιστή σας και δεν μεταδίδονται στην Kaspersky. Διαδρομή προς τα αρχεία αναφορών: %allusersprofile%\Kaspersky Lab\AVP21.0\Report\Database.

Οι αναφορές αποθηκεύονται στα παρακάτω αρχεία:

reports.db

- reports.db-wal
- reports.db-shm (δεν περιέχει προσωπικά δεδομένα)

Τα αρχεία αναφορών προστατεύονται από τη μη εξουσιοδοτημένη πρόσβαση εάν έχει ενεργοποιηθεί η αυτοάμυνα στο Kaspersky Total Security. Εάν η αυτοάμυνα είναι απενεργοποιημένη, τα αρχεία αναφορών δεν προστατεύονται.

Αποθήκευση δεδομένων για Τεχνική υποστήριξη

Η εφαρμογή επεξεργάζεται και αποθηκεύει τα ακόλουθα προσωπικά δεδομένα για περαιτέρω ανάλυση από την Τεχνική υποστήριξη:

- Τα δεδομένα εμφανίζονται στο περιβάλλον χρήστη της εφαρμογής:
 - Διεύθυνση email που χρησιμοποιείται για τη σύνδεση στο My Kaspersky
 - Διευθύνσεις δικτυακών τόπων που προστέθηκαν στις εξαιρέσεις (εμφανίζονται στα στοιχεία Προστασία από ιούς στο Web, Πρόγραμμα Anti-Banner, Ιδιωτική περιήγηση και Δίκτυο. καθώς και στο παράθυρο Αναφορές)
 - Δεδομένα άδειας χρήσης

Αυτά τα δεδομένα αποθηκεύονται τοπικά σε μη τροποποιημένη μορφή και είναι δυνατή η προβολή τους από οποιονδήποτε λογαριασμό χρήστη στον υπολογιστή.

- Δεδομένα σχετικά με τη μνήμη συστήματος των διεργασιών Kaspersky Total Security κατά τη στιγμή της δημιουργίας αποτύπωσης μνήμης.
- Δεδομένα που συλλέγονται όταν είναι ενεργοποιημένα τα ίχνη.

Τα δεδομένα αποθηκεύονται τοπικά σε τροποποιημένη μορφή και είναι δυνατή η προβολή τους από οποιονδήποτε λογαριασμό χρήστη στον υπολογιστή. Αυτά τα δεδομένα μεταδίδονται στην Kaspersky μόνο με τη συγκατάθεσή σας κατά την επικοινωνία με την Τεχνική υποστήριξη. Για να μάθετε περισσότερα σχετικά με τα δεδομένα, κάντε κλικ στη σύνδεση **Κανονισμού σχετικά με την παροχή δεδομένων** στο παράθυρο **Εργαλεία υποστήριξης**.

Σχετικά με τη χρήση της εφαρμογής στην Ευρωπαϊκή Ένωση, το Ηνωμένο Βασίλειο, τις ΗΠΑ, τη Βραζιλία ή από κατοίκους της πολιτείας της Καλιφόρνια Οι εκδόσεις της εφαρμογής που διανέμουν η Kaspersky και οι συνεργάτες μας στην Ευρωπαϊκή Ένωση, το Ηνωμένο Βασίλειο, τη Βραζιλία (καθώς και οι εκδόσεις που χρησιμοποιούνται από κατοίκους της πολιτείας της Καλιφόρνια) πληρούν τις απαιτήσεις των κανονισμών που διέπουν τη συλλογή και την επεξεργασία προσωπικών δεδομένων που έχουν δημιουργηθεί σε αυτές τις περιοχές.

Για την εγκατάσταση της εφαρμογής, πρέπει να αποδεχτείτε την Άδεια Χρήσης Τελικού Χρήστη και τους όρους της Πολιτικής απορρήτου.

Επιπλέον, ο Οδηγός εγκατάστασης και κατάργησης σας ζητά να δηλώσετε την αποδοχή εκ μέρους σας των παρακάτω συμφωνιών σχετικά με τον τρόπο επεξεργασίας των προσωπικών σας δεδομένων:

- Δήλωση για το Kaspersky Security Network. Αυτή η δήλωση επιτρέπει στους ειδικούς της Kaspersky να λάβουν άμεσα πληροφορίες σχετικά με απειλές που εντοπίζονται στον υπολογιστή σας, με εφαρμογές που εκτελούνται και υπογεγραμμένες εφαρμογές που έχουν ληφθεί, καθώς και πληροφορίες σχετικά με το λειτουργικό σύστημα για τη βελτίωση της προστασίας σας.
- Δήλωση αναφορικά με την επεξεργασία δεδομένων για σκοπούς μάρκετινγκ. Αυτή η δήλωση μας επιτρέπει να δημιουργήσουμε προσφορές με αξία για εσάς.
- Δήλωση σχετικά με την επεξεργασία δεδομένων κατά τη χρήση του Προγράμματος Anti-Spam. Αυτή η δήλωση επιτρέπει στους ειδικούς της Kaspersky να λαμβάνουν δεδομένα προκειμένου να βελτιώνουν το Πρόγραμμα Anti-Spam.

Μπορείτε να αποδεχτείτε ή να απορρίψετε τη Δήλωση Kaspersky Security Network και τη Δήλωση αναφορικά με την επεξεργασία δεδομένων για σκοπούς μάρκετινγκ σε οποιαδήποτε στιγμή από το παράθυρο **Ρυθμίσεις** → **Προστασία** → **Kaspersky Security Network**.

Γιατί χρειάζεται το My Kaspersky

To My Kaspersky είναι μια τοποθεσία web της Kaspersky που έχει σχεδιαστεί για κεντρική αποθήκευση και διαχείριση πληροφοριών των εφαρμογών Kaspersky που χρησιμοποιείτε.

Στο My Kaspersky, μπορείτε να κάνετε τα εξής:

- Να προβάλετε πληροφορίες σχετικά με τις άδειες χρήσης και τις ημερομηνίες λήξης τους
- Να διαχειρίζεστε <u>απομακρυσμένα</u> την προστασία του υπολογιστή
- Να αποθηκεύετε και να συγχρονίζετε με ασφάλεια τους κωδικούς πρόσβασης και άλλες προσωπικές πληροφορίες, εφόσον χρησιμοποιείτε το <u>Kaspersky Password Manager</u>

- Προστατέψτε τα παιδιά σας από κινδύνους του Διαδικτύου και εφαρμογών αν χρησιμοποιείτε το <u>Kaspersky Safe Kids</u>
- Να κάνετε λήψη των εφαρμογών που αγοράζετε
- Να επικοινωνήσετε με την Τεχνική υποστήριξη
- Να μάθετε πληροφορίες σχετικά με νέες εφαρμογές και ειδικές προσφορές από την Kaspersky

Για να αποκτήσετε πρόσβαση στις δυνατότητες του My Kaspersky, χρειάζεστε έναν <u>λογαριασμό</u>.

Λεπτομερείς πληροφορίες σχετικά με τη χρήση του My Kaspersky διατίθενται στη <u>Βοήθεια</u> <u>για το My Kaspersky</u> .

Πληροφορίες για τον λογαριασμό My Kaspersky

Απαιτείται *λογαριασμός My Kaspersky* για είσοδο στην <u>τοποθεσία web My Kaspersky</u> , καθώς και για τη χρήση του δικτυακού τόπου και ορισμένων εφαρμογών της Kaspersky.

Εάν δεν έχετε ακόμα λογαριασμό, μπορείτε να δημιουργήσετε έναν στην τοποθεσία web My Kaspersky ή από τις εφαρμογές που είναι συμβατές με την τοποθεσία web. Μπορείτε επίσης να χρησιμοποιήσετε λογαριασμούς που χρησιμοποιούνται με άλλους πόρους της Kaspersky για να εισέλθετε στην τοποθεσία web.

Κατά τη δημιουργία του λογαριασμού, πρέπει να καθορίσετε μια έγκυρη διεύθυνση email και έναν κωδικό πρόσβασης. Ο κωδικός πρόσβασης πρέπει να περιέχει τουλάχιστον 8 χαρακτήρες, έναν αριθμό, ένα κεφαλαίο γράμμα και ένα πεζό λατινικό γράμμα. Τα κενά διαστήματα δεν επιτρέπονται.

Εάν ο κωδικός πρόσβασης είναι πολύ αδύναμος ή συνηθισμένος, ο λογαριασμός δεν θα δημιουργηθεί.

Μόλις δημιουργηθεί ο λογαριασμός, θα λάβετε ένα μήνυμα email που θα περιέχει μια σύνδεση για την ενεργοποίηση του λογαριασμού σας.

Παρακαλούμε ενεργοποιήστε το λογαριασμό σας χρησιμοποιώντας τη σύνδεση στο email.

Πώς να δημιουργήσετε λογαριασμό My Kaspersky

Για να δημιουργήσετε ένα λογαριασμό My Kaspersky:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **My Kaspersky**.
- Στο παράθυρο My Kaspersky, κάντε κλικ στο κουμπί Σύνδεση.
 Ανοίγει το παράθυρο Σύνδεση στο My Kaspersky.
- 4. Εισαγάγετε τη διεύθυνση email σας στο πεδίο **Εισαγάγετε διεύθυνση email** και κάντε κλικ στο κουμπί δίπλα στο πεδίο εισαγωγής.
- 5. Εάν η εφαρμογή δεν εντοπίσει αυτόματα την περιοχή σας, θα σας ζητηθεί να επιλέξετε μία. Οι εφαρμογές που μπορείτε να εγκαταστήσετε και οι διαθέσιμες μέθοδοι πληρωμών που μπορείτε να χρησιμοποιήσετε εξαρτώνται από την περιοχή που έχετε επιλέξει. Εισαγάγετε την περιοχή σας και κάντε κλικ στην Επιβεβαίωση.
- 6. Εισαγάγετε τον κωδικό πρόσβασής σας στο πεδίο **Κωδικός πρόσβασης** και κάντε κλικ στο κουμπί δίπλα στο πεδίο εισαγωγής.

Ο κωδικός πρόσβασης πρέπει να περιέχει τουλάχιστον 8 χαρακτήρες οι οποίοι πρέπει να περιλαμβάνουν έναν αριθμό, ένα κεφαλαίο γράμμα και ένα πεζό γράμμα.

7. Επιλέξτε το πλαίσιο ελέγχου Συμφωνώ να παρέχω στην Kaspersky τη διεύθυνση email μου για τη λήψη εξατομικευμένων προσφορών μάρκετινγκ εάν επιθυμείτε να λαμβάνετε ειδοποιήσεις της Kaspersky στο γραμματοκιβώτιό σας.

Σε <u>ορισμένες εκδόσεις της εφαρμογής</u>, αυτό το πλαίσιο ελέγχου ονομάζεται Επιβεβαιώνω ότι επιτρέπω στην ΑΟ Kaspersky Lab να χρησιμοποιεί την προσωπική μου διεύθυνση email και το ονοματεπώνυμό μου για να επικοινωνεί μαζί μου μέσω email για εξατομικευμένες ειδικές προσφορές, κριτικές, έρευνες, υπενθυμίσεις ολοκλήρωσης παραγγελιών, σχετικά νέα και εκδηλώσεις ή Επιβεβαιώνω ότι επιτρέπω στην ΑΟ Kaspersky Lab να χρησιμοποιεί την προσωπική μου διεύθυνση email για να επικοινωνεί μαζί μου μέσω email για εξατομικευμένες ειδικές προσφορές, κριτικές, έρευνες, υπενθυμίσεις ολοκλήρωσης παραγγελιών, σχετικά νέα και εκδηλώσεις.

- 8. Εισαγάγετε το όνομά σας στο πεδίο **Το όνομά σας**.
- 9. Εισαγάγετε το επώνυμό σας στο πεδίο **Το επώνυμό σας**.
- 10. Κάντε κλικ στο κουμπί **Δημιουργία**.

Θα σταλεί ένα μήνυμα στη διεύθυνση email σας και θα περιέχει ένα σύνδεσμο στον οποίο πρέπει να κάνετε κλικ για να ενεργοποιήσετε το λογαριασμό My Kaspersky.

11. Κάντε κλικ στη σύνδεση για να ενεργοποιήσετε το λογαριασμό σας στην πύλη My Kaspersky.

Η διάταξη του πεδίου κατά τη δημιουργία ενός λογαριασμού σχεδιάζεται από ειδικούς της Kaspersky και ενδέχεται να αλλάξει.

Σχετικά με την απομακρυσμένη διαχείριση της προστασίας του υπολογιστή

Εάν ο υπολογιστής σας διαθέτει το Kaspersky Total Security εγκατεστημένο και είναι συνδεδεμένος στο My Kaspersky, μπορείτε να διαχειριστείτε την προστασία του από απόσταση.

Για να διαχειριστείτε την προστασία του υπολογιστή από απόσταση, συνδεθείτε στο Μy Kaspersky με τον <u>λογαριασμό</u> σας και μεταβείτε στην ενότητα **Συσκευές**.

Στην ενότητα **Συσκευές**, μπορείτε να κάνετε τα εξής:

- Να δείτε τη λίστα με τα προβλήματα ασφάλειας του υπολογιστή και να τα διορθώσετε από απόσταση
- Να σαρώσετε τον υπολογιστή για ιούς και άλλες απειλές
- Να ενημερώσετε τις βάσεις δεδομένων και τις λειτουργικές μονάδες της εφαρμογής
- Ρύθμιση παραμέτρων στοιχείων του Kaspersky Total Security

Εάν ξεκινήσετε μια σάρωση του υπολογιστή από το My Kaspersky, το Kaspersky Total Security επεξεργάζεται αυτόματα τα αντικείμενα που εντοπίζονται χωρίς να απαιτείται κάποια ενέργεια από εσάς. Μόλις εντοπίζεται ένας ιός ή άλλη απειλή, το Kaspersky Total Security επιχειρεί να εκτελέσει απολύμανση χωρίς επανεκκίνηση του υπολογιστή. Εάν η απολύμανση χωρίς επανεκκίνηση του υπολογιστή. Εάν η απολύμανση χωρίς επανεκκίνηση του υπολογιστή στο Μy Kaspersky, το σποίο σας ενημερώνει ότι ο υπολογιστής πρέπει να επανεκκινηθεί για να πραγματοποιηθεί η απολύμανση.

Εάν η λίστα εντοπισμένων αντικειμένων στο My Kaspersky περιλαμβάνει περισσότερα από 10 στοιχεία, αυτά ομαδοποιούνται. Σε αυτή την περίπτωση, τα εντοπισμένα αντικείμενα μπορούν να υποβληθούν σε επεξεργασία μέσω του My Kaspersky μόνο από κοινού, χωρίς τη δυνατότητα εξέτασης κάθε αντικειμένου ξεχωριστά. Για να δείτε τα αντικείμενα ξεχωριστά σε αυτή την περίπτωση, σας συνιστούμε να χρησιμοποιήσετε το περιβάλλον εργασίας της εφαρμογής που είναι εγκατεστημένη στον υπολογιστή.

Πώς να υλοποιήσετε την απομακρυσμένη διαχείριση της προστασίας του υπολογιστή

Για να υλοποιήσετε την απομακρυσμένη διαχείριση της προστασίας υπολογιστή, πρέπει να συνδέσετε τη συσκευή σας στο My Kaspersky. Εάν είχατε εισαγάγει παλιότερα τα διαπιστευτήριά σας σε άλλη εφαρμογή της Kaspersky στον ίδιο υπολογιστή, το Kaspersky Security Cloud θα συνδεθεί αυτόματα στο My Kaspersky. Εάν η εφαρμογή δεν καταφέρει να συνδέσει αυτόματα τη συσκευή σας στο My Kaspersky, πρέπει να συνδεθείτε χειροκίνητα.

Για να συνδέσετε μια συσκευή στο My Kaspersky:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **My Kaspersky**.
- 3. Κάντε κλικ στο κουμπί **Σύνδεση**.

Σε <u>ορισμένες περιοχές</u>, η εφαρμογή σάς ζητά να διαβάσετε και να αποδεχτείτε τον κανονισμό σχετικά με την παροχή δεδομένων. Εάν αποδέχεστε τους όρους της δήλωσης, κάντε κλικ στο κουμπί **Αποδοχή και σύνδεση**.

- Στο παράθυρο Σύνδεση στο My Kaspersky, εισάγετε τα διαπιστευτήρια για να συνδέσετε την εφαρμογή με το My Kaspersky και κάντε κλικ στο κουμπί Σύνδεση.
- Εάν δεν έχετε ακόμα λογαριασμό My Kaspersky:
 - a. Κάντε κλικ στο κουμπί **Δημιουργία λογαριασμού** και <u>εγγραφείτε στο My</u> <u>Kaspersky</u>.
 - b. Κάντε κλικ στο κουμπί **Δημιουργία**.

Η εφαρμογή θα συνδέσει τη συσκευή σας στο My Kaspersky.

Για να υλοποιήσετε την απομακρυσμένη διαχείριση της προστασίας του υπολογιστή:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **My Kaspersky**.
- 3. Στο παράθυρο **My Kaspersky**, κάντε κλικ στο κουμπί **Μετάβαση σε My Kaspersky**.

Το παράθυρο του My Kaspersky ανοίγει στο προεπιλεγμένο πρόγραμμα περιήγησης.

Η σύνδεση στο My Kaspersky μπορεί να αποτύχει λόγω δυσλειτουργίας του My Kaspersky. Εάν συμβεί αυτό, το Kaspersky Total Security εμφανίζει μια ειδοποίηση σχετικά με τα προβλήματα που παρουσιάστηκαν στο My Kaspersky και βρίσκονται σε διαδικασία επίλυσης από το προσωπικό της Kaspersky. Εάν δεν μπορείτε να συνδεθείτε στο My Kaspersky λόγω κάποιας δυσλειτουργίας του My Kaspersky, προσπαθήστε ξανά αργότερα.

Πώς να ρυθμίσετε τη διεπαφή της εφαρμογής

Αυτή η ενότητα περιέχει πληροφορίες σχετικά με τον τρόπο ρύθμισης των παραμέτρων της διεπαφής του Kaspersky Total Security.

Πώς να αλλάξετε το εικονίδιο της εφαρμογής

Για να αλλάξετε το εικονίδιο της εφαρμογής:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🥶 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Διεπαφή**.
- 4. Στον αποκλεισμό **Εικονίδιο εφαρμογής**, ορίστε μία από τις ακόλουθες επιλογές:
 - Τυπικό εικονίδιο. Όταν ενεργοποιηθεί αυτή η επιλογή, η επιφάνεια εργασίας και η περιοχή ειδοποιήσεων θα εμφανίσουν το τυπικό εικονίδιο της εφαρμογής.
 - Midori Kuma. Όταν ενεργοποιηθεί αυτή η επιλογή, η επιφάνεια εργασίας και η περιοχή ειδοποιήσεων θα εμφανίσουν το εικονίδιο που περιέχει μια εικόνα με το αρκουδάκι-μασκότ που είναι γνωστό ως Midori Kuma.

Η δυνατότητα αλλαγής του θέματος σχεδίασης της εφαρμογής δεν είναι διαθέσιμη σε όλες τις περιοχές.

Για να αλλάξετε το θέμα σχεδίασης της εφαρμογής:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🥶 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Διεπαφή**.
- 4. Στον αποκλεισμό **Θέμα σχεδίασης**, επιλέξτε το πλαίσιο ελέγχου **Χρήση προσαρμοσμένου θέματος σχεδίασης**.
- 5. Κάντε κλικ στο στοιχείο **Επιλογή** και εισαγάγετε τη διαδρομή προς το αρχείο ΖΙΡ ή τον φάκελο που περιέχει τα αρχεία με το προσαρμοσμένο θέμα σχεδίασης.

Αφού προσθέσετε ένα προσαρμοσμένο θέμα σχεδίασης, θα εφαρμοστεί μετά την επανεκκίνηση της εφαρμογής.

Σχετικά με τις ειδοποιήσεις της εφαρμογής

Οι ειδοποιήσεις που εμφανίζονται στην περιοχή ειδοποιήσεων της γραμμής εργασιών σάς ενημερώνουν για συμβάντα που παρουσιάζονται κατά τη λειτουργία της εφαρμογής και απαιτούν την προσοχή σας. Ανάλογα με το πόσο κρίσιμο είναι το εκάστοτε συμβάν, ενδέχεται να λάβετε τους ακόλουθους τύπους ειδοποιήσεων:

- Οι Κρίσιμες ειδοποιήσεις σας ενημερώνουν σχετικά με συμβάντα κρίσιμης σημασίας για την ασφάλεια του υπολογιστή, όπως ο εντοπισμός κακόβουλου αντικειμένου ή επικίνδυνης δραστηριότητας στο λειτουργικό σύστημα. Τα παράθυρα που χρησιμοποιούνται για τις κρίσιμες ειδοποιήσεις και τα αναδυόμενα μηνύματα έχουν κόκκινο χρώμα.
- Οι Σημαντικές ειδοποιήσεις σας ενημερώνουν σχετικά με συμβάντα που είναι δυνητικά σημαντικά για την ασφάλεια του υπολογιστή, όπως ο εντοπισμός ενός πιθανώς μολυσμένου αντικειμένου ή μιας ύποπτης δραστηριότητας στο λειτουργικό σύστημα. Τα

παράθυρα που χρησιμοποιούνται για τις σημαντικές ειδοποιήσεις και τα αναδυόμενα μηνύματα έχουν κίτρινο χρώμα.

 Οι Ενημερωτικές ειδοποιήσεις σας ενημερώνουν σχετικά με συμβάντα που δεν έχουν κρίσιμη σημασία για την ασφάλεια του υπολογιστή. Τα παράθυρα που χρησιμοποιούνται για τις ενημερωτικές ειδοποιήσεις και τα αναδυόμενα μηνύματα έχουν πράσινο χρώμα.

Εάν μια ειδοποίηση εμφανιστεί στην οθόνη, θα πρέπει να κάνετε μία από τις επιλογές που προτείνονται στην ειδοποίηση. Η βέλτιστη επιλογή είναι εκείνη που συνιστάται ως προεπιλογή από τους ειδικούς της Kaspersky.

Οι ειδοποιήσεις μπορούν να κλείσουν αυτόματα με την επανεκκίνηση του υπολογιστή, με το κλείσιμο του Kaspersky Total Security ή με την ενεργοποίηση της λειτουργίας Αναμονής σύνδεσης στα Windows 8. Οι ειδοποιήσεις του Ελέγχου εφαρμογών κλείνουν αυτόματα μετά από 500 δευτερόλεπτα. Οι ειδοποιήσεις σχετικά με την εκκίνηση των εφαρμογών κλείνουν μετά από 1 ώρα. Όταν μια ειδοποίηση κλείνει αυτόματα, το Kaspersky Total Security εκτελεί την προεπιλεγμένη συνιστώμενη ενέργεια.

Οι ειδοποιήσεις δεν εμφανίζονται κατά τη διάρκεια της πρώτης ώρας λειτουργίας της εφαρμογής, αν έχετε αγοράσει υπολογιστή με προεγκατεστημένο το Kaspersky Total Security (διανομή OEM). Η εφαρμογή επεξεργάζεται τα αντικείμενα που έχουν εντοπιστεί σύμφωνα με τις προτεινόμενες ενέργειες. Τα αποτελέσματα αυτής της επεξεργασίας αποθηκεύονται σε μια αναφορά.

Πώς να ρυθμίσετε τις παραμέτρους ειδοποιήσεων της εφαρμογής

Κάντε κλικ στις παρακάτω συνδέσεις για να μάθετε πώς να ρυθμίζετε τις παραμέτρων των ειδοποιήσεων εφαρμογών.

<u>Πώς να ρυθμίσετε τις παραμέτρους της παράδοσης των ειδοποιήσεων 💿</u>

Για να δημιουργήσετε κανόνες ειδοποίησης:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Διεπαφή**.

- 4. Στον αποκλεισμό **Ειδοποιήσεις**, κάντε κλικ στη σύνδεση **Ρυθμίσεις ειδοποιήσεων** για να προχωρήσετε στο παράθυρο ρυθμίσεων ειδοποιήσεων.
- 5. Επιλέξτε το στοιχείο στη λίστα στα αριστερά.
- 6. Το δεξί μέρος του παραθύρου εμφανίζει μια λίστα συμβάντων που ενδέχεται να προκύψουν κατά τη λειτουργία αυτού του στοιχείου.
- Επιλέξτε ένα συμβάν από τη λίστα και ενεργοποιήστε τα ακόλουθα πλαίσια ελέγχου:
 - Αποθήκευση σε τοπική αναφορά. Όταν προκύπτει το συμβάν, οι πληροφορίες σχετικά με αυτό το συμβάν θα εγγράφονται σε μια αναφορά, η οποία αποθηκεύεται στον τοπικό υπολογιστή.
 - Ειδοποίηση στην οθόνη. Όταν προκύπτει το συμβάν, θα εμφανίζεται μια αναδυόμενη ειδοποίηση πάνω από το εικονίδιο της εφαρμογής στην περιοχή ειδοποιήσεων της γραμμής εργασιών.

Μπορείτε να χρησιμοποιήσετε την αναπτυσσόμενη λίστα στην κάτω αριστερή γωνία για να υποδείξετε ποιες ειδοποιήσεις θέλετε να αποθηκεύσετε στην τοπική αναφορά:

- Από προεπιλογή. Όταν ενεργοποιείται αυτή η επιλογή, η αναφορά που δημιουργείται θα αποθηκεύει τα συμβάντα που έχουν επιλέξει οι ειδικοί της Kaspersky.
- Χειροκίνητα. Αυτή η επιλογή επιλέγεται αυτόματα εάν ρυθμίσετε τις παραμέτρους της δυνατότητας έτσι ώστε να γίνεται χειροκίνητη αποθήκευση συμβάντων σε μια αναφορά.
- Κρίσιμο. Όταν ενεργοποιείται αυτή η επιλογή, η αναφορά που δημιουργείται θα αποθηκεύει Κρίσιμα συμβάντα (όπως Συμβάντα δυσλειτουργίας εφαρμογής για το στοιχείο Έλεγχος συστήματος και το στοιχείο Έλεγχος εφαρμογών).
- Σημαντικό. Όταν ενεργοποιείται αυτή η επιλογή, η αναφορά που δημιουργείται θα αποθηκεύει Κρίσιμα συμβάντα (όπως Συμβάντα δυσλειτουργίας εφαρμογής για το στοιχείο Έλεγχος συστήματος και το στοιχείο Έλεγχος εφαρμογών) και Προειδοποιήσεις.
- Πληροφοριακό. Όταν ενεργοποιείται αυτή η επιλογή, η αναφορά που δημιουργείται θα αποθηκεύει όλα τα συμβάντα.

<u>Πώς να ρυθμίσετε τις παραμέτρους της παράδοσης των ειδοποιήσεων που περιέχουν</u> ειδήσεις και ειδικές προσφορές από την Kaspersky 😨

Εάν θέλετε να μείνετε ενημερωμένοι για τις τελευταίες ειδήσεις της ασφάλειας στον κυβερνοχώρο και να λαμβάνετε ειδικές προσφορές από την Kaspersky:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Μεταβείτε στην ενότητα **Διεπαφή**.
- 4. Στον αποκλεισμό Ειδοποιήσεις ειδήσεων, επιλέξτε το πλαίσιο ελέγχου Λήψη ενημερωτικών μηνυμάτων και διαφημίσεων από την Kaspersky, εάν θέλετε να λαμβάνετε ειδοποιήσεις για τις ειδήσεις σχετικά με την ασφάλεια του υπολογιστή.
- 5. Στον αποκλεισμό **Προωθητικό υλικό**:
 - Επιλέξτε το πλαίσιο ελέγχου Εμφάνιση πληροφοριών για ειδικές προσφορές, εάν θέλετε να λαμβάνετε τις καλύτερες προσφορές όταν επισκέπτεστε τοποθεσίες web της Kaspersky.
 - Επιλέξτε το πλαίσιο ελέγχου Λήψη ενημερωτικών μηνυμάτων και διαφημίσεων μετά τη λήξη της τρέχουσας άδειας χρήσης, εάν θέλετε να λαμβάνετε ειδοποιήσεις σχετικά με τις ειδήσεις για την ασφάλεια από την Kaspersky μετά τη λήξη της άδειας χρήσης ή της συνδρομής σας.

<u>Πώς να ενεργοποιήσετε τις ηχητικές ειδοποιήσεις </u>

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 😳 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Διεπαφή**.
- 4. Στον αποκλεισμό **Ειδοποιήσεις**, επιλέξτε το πλαίσιο ελέγχου **Ενεργοποίηση ηχητικών ειδοποιήσεων**.

Για να αλλάξετε το προεπιλεγμένο ηχητικό σήμα σε "ήχο γουρουνιού", πληκτρολογήστε **IDKFA** στο παράθυρο **Σχετικά με**.

Τα ηχητικά σήματα ειδοποιήσεων δεν αναπαράγονται στα Microsoft Windows 10.

Πώς να αλλάξετε το εικονίδιο της εφαρμογής στην περιοχή ειδοποιήσεων ανάλογα με την κατάσταση της εφαρμογής

Για να αλλάξετε το εικονίδιο της εφαρμογής στην περιοχή ειδοποιήσεων ανάλογα με την κατάσταση της εφαρμογής:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Διεπαφή**.
- 4. Στο πλαίσιο **Προβολή της κατάστασης εφαρμογής στην περιοχή ειδοποιήσεων**, επιλέξτε μια κατάσταση και επιλέξτε ένα πλαίσιο ελέγχου.

Όταν η εφαρμογή μεταβεί σε κατάσταση που αντιστοιχεί στην επιλεγμένη κατάσταση, το εικονίδιο της εφαρμογής στην περιοχή ειδοποιήσεων θα αλλάξει.

Τρόπος προστασία της πρόσβασης στις λειτουργίες διαχείρισης του Kaspersky Total Security με χρήση κωδικού πρόσβασης

Ο ίδιος υπολογιστής μπορεί να χρησιμοποιείται από πολλούς χρήστες, διαφορετικού επιπέδου εμπειρίας και εξοικείωσης με τους υπολογιστές. Η απεριόριστη πρόσβαση διαφορετικών χρηστών στο Kaspersky Total Security και τις ρυθμίσεις του ενδέχεται να μειώσει το επίπεδο ασφάλειας του υπολογιστή.

Για να περιορίσετε την πρόσβαση στην εφαρμογή, μπορείτε να ορίσετε έναν κωδικό πρόσβασης διαχειριστή για τον λογαριασμό KLAdmin. Αυτός ο χρήστης έχει απεριόριστα δικαιώματα για τη διαχείριση και την τροποποίηση των ρυθμίσεων του Kaspersky Total Security και για την εκχώρηση δικαιωμάτων πρόσβασης σε άλλους χρήστες. Αφού δημιουργήσετε έναν κωδικό πρόσβασης για το KLAdmin, μπορείτε να εκχωρήσετε δικαιώματα πρόσβασης σε διάφορους χρήστες ή ομάδες χρηστών.

Για να δημιουργήσετε έναν κωδικό πρόσβασης διαχειριστή KLAdmin για το Kaspersky Total Security:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Διεπαφή**.
- 4. Μετακινήστε τον **Προστασία με χρήση κωδικού πρόσβασης** στη θέση **Ενεργό**.
- 5. Στο ανοιχτό παράθυρο, συμπληρώστε τα πεδία **Όνομα χρήστη** (συνιστάται το KLAdmin), **Εισαγωγή κωδικού πρόσβασης** και **Επιβεβαίωση κωδικού πρόσβασης**.

Συμβουλές δημιουργίας ισχυρού κωδικού πρόσβασης:

- Ο κωδικός πρόσβασης πρέπει να περιέχει από οκτώ έως 128 χαρακτήρες.
- Ο κωδικός πρόσβασης περιέχει τουλάχιστον έναν αριθμό.
- Ο κωδικός πρόσβασης περιέχει πεζά και κεφαλαία γράμματα.
- Ο κωδικός πρόσβασης πρέπει να περιέχει τουλάχιστον έναν ειδικό χαρακτήρα (για παράδειγμα: ! @ # \$ % ^ & *).
- 6. Κάντε κλικ στο **ΟΚ**.

Εάν ξεχάσετε τον κωδικό πρόσβασης, δεν είναι δυνατό να τον ανακτήσετε. Σε περίπτωση που ξεχάσετε τον κωδικό πρόσβασης, επικοινωνήστε με την τεχνική υποστήριξη για να ανακτήσετε την πρόσβαση στις ρυθμίσεις του Kaspersky Total Security.

Ο χρήστης KLAdmin μπορεί να εκχωρήσει δικαιώματα στους παρακάτω χρήστες και ομάδες χρηστών:

- Ομάδα χρηστών Όλοι. Αυτή η ομάδα περιλαμβάνει όλους τους χρήστες του λειτουργικού συστήματος. Αν εκχωρήσετε σε αυτή την ομάδα δικαίωμα να εκτελεί μια συγκεκριμένη ενέργεια, οι χρήστες της ομάδας θα επιτρέπεται πάντα να εκτελέσουν αυτή την ενέργεια, ακόμα και αν ένας συγκεκριμένος χρήστης ή μια συγκεκριμένη ομάδα χρηστών που ανήκει στην ομάδα χρηστών Όλοι δεν έχει μεμονωμένο δικαίωμα να εκτελέσει την ενέργεια. Από προεπιλογή, τα μέλη της ομάδας Όλοι δεν επιτρέπεται να εκτερίπεται να εκτελούν
- <χρήστης συστήματος>. Από προεπιλογή, ο επιλεγμένος χρήστης δεν επιτρέπεται να εκτελεί οποιεσδήποτε ενέργειες. Αυτό σημαίνει ότι, όταν προσπαθήσετε να εκτελέσετε μια απαγορευμένη ενέργεια, θα σας ζητηθεί να πληκτρολογήσετε τον κωδικό πρόσβασης του λογαριασμού KLAdmin.

<u>Πώς να προσθέσετε έναν χρήστη ή μια ομάδα χρηστών</u> 😨

 Στην ενότητα Διεπαφή, στον αποκλεισμό Προστασία με χρήση κωδικού πρόσβασης, κάντε κλικ στο κουμπί Προσθήκη.

Ανοίγει το παράθυρο Προσθέστε δικαιώματα για έναν χρήστη ή μια ομάδα.

- 2. Κάντε κλικ στη σύνδεση **Επιλογή χρήστη** για να ανοίξετε το παράθυρο για την επιλογή χρήστη ή ομάδας χρηστών του λειτουργικού συστήματος.
- Στο πεδίο εισαγωγής ονόματος αντικειμένου, καθορίστε το όνομα του χρήστη ή της ομάδας χρηστών (όπως Διαχειριστής).
- 4. Κάντε κλικ στο **ΟΚ**.
- 5. Στο παράθυρο **Προσθέστε δικαιώματα για έναν χρήστη ή μια ομάδα**, στον αποκλεισμό **Δικαιώματα**, <u>επιλέξτε τα πλαίσια ελέγχου δίπλα στις ενέργειες που</u> θέλετε να επιτρέψετε για αυτόν τον συγκεκριμένο χρήστη ή ομάδα χρηστών.

Πώς να επεξεργαστείτε δικαιώματα για έναν χρήστη ή ομάδα χρηστών 💿

Στην ενότητα **Διεπαφή**, στον αποκλεισμό **Προστασία με χρήση κωδικού πρόσβασης**, επιλέξτε τον χρήστη ή την ομάδα χρηστών στη λίστα και κάντε κλικ στο κουμπί **Επεξεργασία**.

Πώς να επιτρέψετε μια ενέργεια για έναν μεμονωμένο χρήστη ή ομάδα χρηστών ව

- 1. Πηγαίνετε στο παράθυρο **Προσθέστε δικαιώματα για έναν χρήστη ή μια ομάδα** για την ομάδα Όλοι και καταργήστε την επιλογή που επιτρέπει αυτή την ενέργεια, αν είναι ενεργοποιημένη.
- Πηγαίνετε στο παράθυρο Προσθέστε δικαιώματα για έναν χρήστη ή μια ομάδα για τον επιλεγμένο χρήστη και επιλέξτε το πλαίσιο ελέγχου για να επιτρέψετε αυτή την ενέργεια.

Πώς να απαγορεύσετε μια ενέργεια για έναν μεμονωμένο χρήστη ή ομάδα χρηστών 🕑

- Πηγαίνετε στο παράθυρο Προσθέστε δικαιώματα για έναν χρήστη ή μια ομάδα για την ομάδα Όλοι και καταργήστε την επιλογή που επιτρέπει αυτή την ενέργεια, αν είναι ενεργοποιημένη.
- Πηγαίνετε στο παράθυρο Προσθέστε δικαιώματα για έναν χρήστη ή μια ομάδα για τον επιλεγμένο χρήστη και καταργήστε την επιλογή που επιτρέπει αυτή την ενέργεια.

Όταν προσπαθήσετε να εκτελέσετε οποιαδήποτε ενέργεια από τη λίστα του παραθύρου **Προσθέστε δικαιώματα για έναν χρήστη ή μια ομάδα**, το πρόγραμμα θα σας ζητήσει να πληκτρολογήσετε κωδικό πρόσβασης. Στο παράθυρο κωδικού πρόσβασης, πληκτρολογήστε το όνομα χρήστη και τον κωδικό πρόσβασης για τον τρέχοντα λογαριασμό χρήστη. Η ενέργεια θα εκτελεστεί αν ο καθορισμένος λογαριασμός έχει δικαίωμα να εκτελέσει αυτή την ενέργεια. Στο παράθυρο κωδικού πρόσβασης, μπορείτε να καθορίσετε το χρονικό διάστημα κατά το οποίο ο χρήστης δεν χρειάζεται να πληκτρολογήσει ξανά τον κωδικό πρόσβασης.

Πώς να επιταχύνετε την απόδοση του υπολογιστή

Μετά από παρατεταμένη χρήση ενός υπολογιστή, το λειτουργικό σύστημα ενδέχεται να επιβραδυνθεί. Αυτή η επιβράδυνση προκαλείται από μεγάλο αριθμό περιττών αρχείων και σφαλμάτων μητρώου των Windows που συσσωρεύονται κατά τη λειτουργία.

Το λειτουργικό σύστημα μπορεί επίσης να επιβραδυνθεί από εγκατεστημένες εφαρμογές που χρησιμοποιούνται σπάνια. Πολλές από αυτές τις εφαρμογές μπορεί να εκτελούνται μόλις φορτωθεί το λειτουργικό σύστημα και μπορούν να επιβραδύνουν σημαντικά τον υπολογιστή. Ίσως να μην γνωρίζετε καν ότι μια συγκεκριμένη εφαρμογή εκτελείται στο παρασκήνιο χρησιμοποιώντας πόρους υπολογιστή. Για να επιταχύνετε την απόδοση του υπολογιστή:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί Επιτάχυνση PC.
- 3. Στο ανοιχτό παράθυρο Επιτάχυνση PC:
 - Στον αποκλεισμό Επιτάχυνση επιδόσεων υπολογιστή, κάντε κλικ στο κουμπί
 Έναρξη (ή Προβολή, εάν η αναζήτηση είχε ήδη εκτελεστεί).

Η εφαρμογή εκτελεί αναζήτηση και δημιουργεί μια αναφορά με τα ακόλουθα περιεχόμενα:

- Μη χρησιμοποιούμενα αρχεία συστήματος. Κάντε κλικ στο μπλοκ για να δείτε μια λεπτομερή αναφορά για τα αρχεία του λειτουργικού συστήματος που δεν χρησιμοποιούνται. Κάντε κλικ στο κουμπί Εκκαθάριση για να διαγράψετε αυτά τα αρχεία.
- Σφάλματα μητρώου των Windows. Κάντε κλικ στο μπλοκ για να δείτε μια λεπτομερή αναφορά σχετικά με τα σφάλματα μητρώου των Windows που μπορείτε να διαγράψετε χωρίς να διακινδυνεύσετε ζημιά στο λειτουργικό σύστημα. Κάντε κλικ στο κουμπί Επιδιόρθωση για να επιδιορθώσετε τα σφάλματα που εντοπίστηκαν.
- Κάντε κλικ στην ενότητα Επιτάχυνση εκκίνησης για να δείτε μια αναφορά που δείχνει ποιες εφαρμογές αυτόματης εκτέλεσης επιβραδύνουν τον υπολογιστή.
 Μετακινήστε τον διακόπτη Αυτόματη εκτέλεση δίπλα στην εφαρμογή σε Ανενεργό και κάντε κλικ στο κουμπί Ολοκληρώθηκε.
- Κάντε κλικ στην επιλογή Αποδέσμευση χώρου για να απελευθερώσετε χώρο στον σκληρό δίσκο. Στο ανοιχτό παράθυρο, αναζητήστε περιττά αρχεία.
 - Διπλότυπα αρχεία. Κάντε κλικ στο κουμπί Εύρεση για να ξεκινήσετε την αναζήτηση διπλότυπων αρχείων. Μπορείτε να καθορίσετε την περιοχή αναζήτησης στην αναπτυσσόμενη λίστα. Στο παράθυρο αποτελεσμάτων αναζήτησης, επιλέξτε τα αρχεία και κάντε κλικ στο κουμπί Διαγραφή.
 - Μεγάλα αρχεία. Κάντε κλικ στο κουμπί Εύρεση για να ξεκινήσετε την αναζήτηση μεγάλων αρχείων. Μπορείτε να καθορίσετε την περιοχή αναζήτησης στην αναπτυσσόμενη λίστα. Στο παράθυρο αποτελεσμάτων αναζήτησης, επιλέξτε τα αρχεία και κάντε κλικ στο κουμπί Διαγραφή.
Η αναζήτηση μεγάλων αρχείων δεν λειτουργεί για αρχεία που έχουν δύο ή περισσότερες παραπομπές συνδέσεων υλικού στο λειτουργικό σύστημα.

 Εφαρμογές εκτός χρήσης. Κάντε κλικ στο κουμπί Εύρεση. Η αναφορά αποτελεσμάτων αναζήτησης περιλαμβάνει μια λίστα εφαρμογών που δεν έχουν χρησιμοποιηθεί για περισσότερο από τρεις μήνες. Επιλέξτε μια εφαρμογή και κάντε κλικ στο κουμπί Κατάργηση.

Για να στείλετε σχόλια σχετικά με την απόδοση της λειτουργίας Επιτάχυνση ΡC:

Στο παράθυρο **Επιτάχυνση PC**, κάντε κλικ στο κουμπί **Αποστολή σχολίων** και συμπληρώστε τη φόρμα σχολίων.

Τα σχόλιά σας είναι απαραίτητα στους ειδικούς της Kaspersky για να αξιολογήσουν την ποιότητα της λειτουργίας Επιτάχυνση PC.

Η δυνατότητα Επιτάχυνση υπολογιστή είναι διαθέσιμη σε λειτουργία δοκιμής μέχρι τις 30 Απριλίου 2021.

Αυτή η λειτουργικότητα δεν είναι διαθέσιμη σε όλες τις περιοχές.

Αξιολόγηση της κατάστασης προστασίας του υπολογιστή και επίλυση ζητημάτων ασφάλειας

Τυχόν προβλήματα με την προστασία του υπολογιστή υποδεικνύονται με μια ένδειξη στο επάνω μέρος του κύριου παραθύρου της εφαρμογής. Το πράσινο χρώμα σημαίνει ότι ο υπολογιστής σας προστατεύεται. Το κίτρινο χρώμα υποδεικνύει ότι υπάρχουν προβλήματα με την προστασία του υπολογιστή και το κόκκινο σημαίνει ότι υπάρχουν σοβαροί κίνδυνοι για την ασφάλεια του υπολογιστή σας. Συνιστάται να διορθώνετε τα προβλήματα και τις απειλές ασφάλειας αμέσως.

Μπορείτε να ανοίξετε το παράθυρο **Κέντρο ειδοποιήσεων** κάνοντας κλικ στην ένδειξη στο κύριο παράθυρο της εφαρμογής. Στο παράθυρο δίνονται λεπτομερείς πληροφορίες σχετικά με την κατάσταση προστασίας του υπολογιστή και προτείνονται πιθανές ενέργειες για τη διόρθωση προβλημάτων και την αντιμετώπιση απειλών.

Τα προβλήματα με την προστασία ομαδοποιούνται σε κατηγορίες. Για κάθε πρόβλημα, εμφανίζεται μια λίστα με ενέργειες που μπορείτε να πραγματοποιήσετε για να λύσετε το πρόβλημα.

Στην ενότητα **Συστάσεις** παρατίθενται οι ενέργειες που πρέπει να εκτελεστούν για τη βελτιστοποίηση της λειτουργίας της εφαρμογής την αποτελεσματικότερη χρήση της.

Η ενότητα **Εμφάνιση Ν ειδοποιήσεων που έχουν παραβλεφθεί** εμφανίζει τις ειδοποιήσεις στις οποίες έχει εφαρμοστεί η ενέργεια **Παράβλεψη**. Τα προβλήματα που παρατίθενται σε αυτή την ενότητα δεν επηρεάζουν το χρώμα της ένδειξης προστασίας στο κεντρικό παράθυρο της εφαρμογής.

Να ενημερώσετε τις βάσεις δεδομένων και τις λειτουργικές μονάδες της εφαρμογής

Αυτή η ενότητα περιέχει πληροφορίες σχετικά με τις ενημερώσεις των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής.

Πληροφορίες σχετικά με τις ενημερώσεις βάσεων δεδομένων και λειτουργικών μονάδων της εφαρμογής

Το πακέτο εγκατάστασης του Kaspersky Total Security περιλαμβάνει τις βάσεις δεδομένων και τις λειτουργικές μονάδες της εφαρμογής. Χρήση αυτών των βάσεων δεδομένων:

- Το Kaspersky Total Security εντοπίζει την πλειοψηφία των απειλών χρησιμοποιώντας το Kaspersky Security Network, η οποία απαιτεί σύνδεση στο Διαδίκτυο.
- Το Kaspersky Total Security εντοπίζει προγράμματα adware, αυτόματης κλήσης και άλλα νόμιμα λογισμικά που μπορούν να χρησιμοποιηθούν από εισβολείς για την καταστροφή του υπολογιστή σας ή των προσωπικών δεδομένων σας.

Για να έχετε πλήρη προστασία, συνιστούμε να ενημερώσετε τις βάσεις δεδομένων και τις λειτουργικές μονάδες της εφαρμογής αμέσως μόλις εγκαταστήσετε την εφαρμογή.

Οι βάσεις δεδομένων και οι λειτουργικές μονάδες της εφαρμογής ενημερώνονται σε στάδια:

 To Kaspersky Total Security ξεκινά να ενημερώνει τις βάσεις δεδομένων και τις λειτουργικές μονάδες της εφαρμογής σύμφωνα με τις καθορισμένες ρυθμίσεις: αυτόματα, με βάση ένα χρονοδιάγραμμα ή κατ' απαίτηση. Η εφαρμογή επικοινωνεί με μια πηγή ενημέρωσης που περιέχει ένα πακέτο ενημερώσεων βάσεων δεδομένων και λειτουργικών μονάδων της εφαρμογής. 2. Το Kaspersky Total Security συγκρίνει τις υπάρχουσες βάσεις δεδομένων με αυτές που είναι διαθέσιμες στην πηγή ενημέρωσης. Εάν οι βάσεις δεδομένων διαφέρουν, το Kaspersky Total Security λαμβάνει τα ελλείποντα τμήματα των βάσεων δεδομένων.

Η εφαρμογή χρησιμοποιεί στη συνέχεια τις ενημερωμένες βάσεις δεδομένων και λειτουργικές μονάδες της εφαρμογής για να σαρώσει τον υπολογιστή για ιούς και άλλες απειλές.

Πηγές ενημέρωσης

Μπορείτε να χρησιμοποιείτε τις παρακάτω πηγές ενημερώσεων:

- Διακομιστές ενημέρωσης της Kaspersky
- Διακομιστής ΗΤΤΡ ή FTP
- Φάκελος δικτύου

Ειδικές συνθήκες κατά την ενημέρωση βάσεων δεδομένων και λειτουργικών μονάδων της εφαρμογής

Οι ενημερώσεις των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής υπόκεινται στους εξής περιορισμούς και λεπτομέρειες:

- Οι βάσεις δεδομένων θεωρούνται μη ενημερωμένες μετά από μία ημέρα και τελείως απαρχαιωμένες μετά από επτά ημέρες.
- Για τη λήψη πακέτου ενημέρωσης από τους διακομιστές της Kaspersky, απαιτείται σύνδεση στο Διαδίκτυο.
- Οι ενημερώσεις των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής δεν είναι διαθέσιμες στις εξής περιπτώσεις:
 - Εάν έχει λήξει η άδεια χρήσης και δεν είναι διαθέσιμη περίοδος χάριτος ή η κατάσταση περιορισμένης λειτουργικότητας.
 - Εάν χρησιμοποιείται σύνδεση δεδομένων κινητής τηλεφωνίας στο Διαδίκτυο με ογκοχρέωση. Αυτός ο περιορισμός ισχύει για υπολογιστές που διαθέτουν Microsoft Windows 8 ή νεότερες εκδόσεις αυτού του λειτουργικού συστήματος, εάν έχουν ενεργοποιηθεί οι αυτόματες ή προγραμματισμένες ενημερώσεις και έχει τεθεί όριο κίνησης για τη σύνδεση δεδομένων κινητής τηλεφωνίας με ογκοχρέωση. Εάν

επιθυμείτε η εφαρμογή να ενημερώσει τις βάσεις δεδομένων και τις λειτουργικές μονάδες της εφαρμογής σε αυτή την περίπτωση, αποεπιλέξτε το πλαίσιο ελέγχου Περιορισμός κυκλοφορίας για συνδέσεις ογκοχρέωσης στις Ρυθμίσεις → Ρυθμίσεις δικτύου.

 Η εφαρμογή χρησιμοποιείται με συνδρομή και έχετε αναστείλει τη συνδρομή σας από τον δικτυακό τόπο του παρόχου υπηρεσιών.

Εγκατάσταση πακέτου ενημέρωσης

Όταν λαμβάνεται ένα πακέτο ενημέρωσης, το Kaspersky Total Security το εγκαθιστά αυτόματα. Για να ολοκληρώσετε την εγκατάσταση ενός πακέτου ενημέρωσης, πρέπει να επανεκκινήσετε τον υπολογιστή. Μέχρι να επανεκκινηθεί ο υπολογιστής, το εικονίδιο της εφαρμογής στην περιοχή ειδοποιήσεων είναι κόκκινο και το παράθυρο του **Κέντρο ειδοποιήσεων** του Kaspersky Total Security εμφανίζει μια προτροπή επανεκκίνησης του υπολογιστή.

Πώς να ξεκινήσετε την ενημέρωση των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής

Για να εκτελέσετε την ενημέρωση βάσεων δεδομένων και λειτουργικών μονάδων της εφαρμογής:

1. Ανοίξτε το κύριο παράθυρο της εφαρμογής και κάντε κλικ στο κουμπί **Ενημέρωση βάσης δεδομένων**.

Θα ανοίξει το παράθυρο Ενημέρωση βάσης δεδομένων.

2. Στο παράθυρο **Ενημέρωση βάσης δεδομένων**, κάντε κλικ στο κουμπί **Ενημέρωση**.

Σάρωση του υπολογιστή

Κατά τη διάρκεια της σάρωσης, το Kaspersky Total Security αναζητά μολυσμένα αρχεία και κακόβουλο λογισμικό. Υπάρχουν διάφοροι τύποι σαρώσεων που διαφέρουν ως προς τη διάρκεια και το εύρος αναζήτησης.

- Πλήρης σάρωση. Σάρωση σε όλες τις περιοχές του υπολογιστή. Αυτή η σάρωση απαιτεί πολύ χρόνο για να ολοκληρωθεί.
- Γρήγορη σάρωση. Σάρωση αντικειμένων που φορτώνονται κατά την εκκίνηση του λειτουργικού συστήματος, καθώς και της μνήμης συστήματος και των αρχείων εκκίνησης. Αυτή η σάρωση δεν απαιτεί πολύ χρόνο για να ολοκληρωθεί.

- Επιλεκτική σάρωση. Σάρωση του επιλεγμένου αρχείου ή φακέλου.
- Σάρωση αφαιρούμενων μονάδων δίσκου. Σάρωση αφαιρούμενων μονάδων δίσκου, όπως σκληρών δίσκων και μονάδων USB συνδεδεμένων στον υπολογιστή.
- Σάρωση μενού περιβάλλοντος. Αυτή η επιλογή σαρώνει αρχεία από το μενού περιβάλλοντος.
- Σάρωση παρασκηνίου. Σάρωση της μνήμης συστήματος, του διαμερίσματος συστήματος, των τομέων εκκίνησης και των αντικειμένων εκκίνησης, καθώς και αναζήτηση rootkit.
- Σάρωση για τρωτά σημεία. Σαρώνει τον υπολογιστή για τρωτά σημεία που μπορεί να εκμεταλλευτεί το κακόβουλο λογισμικό για να μολύνει το σύστημά σας.

Αφού εγκαταστήσετε το Kaspersky Total Security, σας συνιστούμε να εκτελέσετε πλήρη σάρωση του υπολογιστή σας.

Πώς να εκτελέσετε μια Πλήρη σάρωση

Στη διάρκεια μιας πλήρους σάρωσης, το Kaspersky Total Security σαρώνει από προεπιλογή τα παρακάτω αντικείμενα:

- Μνήμη συστήματος
- Αντικείμενα που φορτώθηκαν κατά την εκκίνηση του λειτουργικού συστήματος
- Χώρο αποθήκευσης αντιγράφων ασφαλείας συστήματος
- Σκληρούς δίσκους και αφαιρούμενες μονάδες δίσκου

Συνιστάται να εκτελέσετε μια πλήρη σάρωση αμέσως μετά την εγκατάσταση του Kaspersky Total Security στον υπολογιστή σας.

Για να ξεκινήσετε μια πλήρη σάρωση:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Σάρωση**.

Θα ανοίξει το παράθυρο **Σάρωση**.

3. Στο παράθυρο **Σάρωση**, επιλέξτε την ενότητα **Πλήρης σάρωση**.

4. Στην ενότητα Πλήρης σάρωση, κάντε κλικ στο κουμπί Εκτέλεση σάρωσης.

Το Kaspersky Total Security θα ξεκινήσει μια πλήρη σάρωση του υπολογιστή σας.

Πώς να εκτελέσετε μια Προσαρμοσμένη σάρωση

Η Επιλεκτική σάρωση σάς δίνει τη δυνατότητα να σαρώσετε ένα αρχείο, έναν φάκελο ή μια μονάδα δίσκου για ιούς και άλλες απειλές.

Για να ξεκινήσετε μια επιλεκτική σάρωση:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Σάρωση**.

Θα ανοίξει το παράθυρο **Σάρωση**.

- 3. Στο παράθυρο **Σάρωση**, επιλέξτε την ενότητα **Επιλεκτική σάρωση**.
- 4. Κάντε κλικ στο κουμπί **Επιλογή** και προσδιορίστε ένα αντικείμενο στο παράθυρο επιλογής αρχείου ή φακέλου που ανοίγει.
- 5. Κάντε κλικ στο κουμπί **Εκτέλεση σάρωσης**.

Πώς να εκτελέσετε μια Γρήγορη σάρωση

Στη διάρκεια μιας γρήγορης σάρωσης, το Kaspersky Total Security σαρώνει από προεπιλογή τα παρακάτω αντικείμενα:

- Αντικείμενα που φορτώνονται κατά την εκκίνηση του λειτουργικού συστήματος
- Μνήμη συστήματος
- Τομείς εκκίνησης δίσκων

Για να ξεκινήσετε μια γρήγορη σάρωση:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί Σάρωση.
 Θα ανοίξει το παράθυρο Σάρωση.

- 3. Στο παράθυρο **Σάρωση**, επιλέξτε την ενότητα **Γρήγορη σάρωση**.
- 4. Στην ενότητα **Γρήγορη σάρωση**, κάντε κλικ στο κουμπί **Εκτέλεση σάρωσης**.

Το Kaspersky Total Security θα ξεκινήσει μια γρήγορη σάρωση του υπολογιστή σας.

Πώς να εκτελέσετε μια σάρωση αφαιρούμενης μονάδας δίσκου

Οι αφαιρούμενες μονάδες δίσκου που συνδέετε στον υπολογιστή ενδέχεται να περιέχουν ιούς ή άλλες εφαρμογές που αποτελούν απειλή. Το Kaspersky Total Security σαρώνει αφαιρούμενες μονάδες δίσκου για να αποτρέψει τη μόλυνση του υπολογιστή σας. Μπορείτε να ρυθμίσετε τις παραμέτρους μιας αφαιρούμενης μονάδας δίσκου ώστε να ξεκινά χειροκίνητα ή αυτόματα, όταν μια αφαιρούμενη μονάδα δίσκου συνδέεται στον υπολογιστή. Η αυτόματη σάρωση αφαιρούμενων μονάδων δίσκου είναι ενεργοποιημένη από προεπιλογή.

Για χειροκίνητη σάρωση μιας αφαιρούμενης μονάδας δίσκου:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Σάρωση**.

Θα ανοίξει το παράθυρο **Σάρωση**.

- Στο παράθυρο Σάρωση, επιλέξτε την ενότητα Σάρωση αφαιρούμενων μονάδων δίσκου.
- Στην αναπτυσσόμενη λίστα, επιλέξτε το γράμμα της μονάδας δίσκου της εξωτερικής συσκευής και κάντε κλικ στο κουμπί Εκτέλεση σάρωσης.

Το Kaspersky Total Security θα ξεκινήσει τη σάρωση της συνδεδεμένης συσκευής.

Πώς να εκτελέσετε μια σάρωση αρχείου ή φακέλου μενού περιβάλλοντος

Για να εκτελέσετε τη σάρωση αρχείου ή φακέλου μενού περιβάλλοντος, εκτελέστε τις ακόλουθες ενέργειες:

- 1. Κάντε δεξί κλικ στο αρχείο ή στον φάκελο που θέλετε να σαρώσετε.
- 2. Στο μενού περιβάλλοντος που ανοίγει, επιλέξτε **Σάρωση για ιούς**.

Το Kaspersky Total Security θα ξεκινήσει τη σάρωση του επιλεγμένου αρχείου ή φακέλου.

Πώς να ενεργοποιήσετε ή να απενεργοποιήσετε μια σάρωση παρασκηνίου

Η *Σάρωση παρασκηνίου* είναι μια λειτουργία αυτόματης σάρωσης του Kaspersky Total Security που δεν εμφανίζει ειδοποιήσεις. Αυτή η σάρωση απαιτεί λιγότερους πόρους υπολογιστή σε σχέση με άλλους τύπους σαρώσεων (για παράδειγμα, Πλήρης σάρωση). Σε αυτή την κατάσταση, το Kaspersky Total Security σαρώνει τη μνήμη συστήματος, τους όγκους συστήματος, τους τομείς εκκίνησης και τα αντικείμενα εκκίνησης και πραγματοποιεί αναζητήσεις για rootkit.

Ξεκινά μια σάρωση παρασκηνίου στις ακόλουθες περιπτώσεις:

- Μετά την ενημέρωση των βάσεων δεδομένων προστασίας από ιούς.
- Τριάντα λεπτά μετά την εκκίνηση του Kaspersky Total Security.
- Κάθε έξι ώρες.
- Εάν ο υπολογιστής παραμείνει αδρανής για πέντε ή περισσότερα λεπτά (μετά την ενεργοποίηση της προφύλαξης οθόνης).

Η σάρωση παρασκηνίου διακόπτεται όταν πληρούται οποιαδήποτε από τις ακόλουθες συνθήκες:

- Ο υπολογιστής ενεργοποιείται ξανά.
- Εάν δεν έχει εκτελεστεί Αδρανής σάρωση για περισσότερες από δέκα ημέρες, τότε η σάρωση δεν θα διακοπεί και θα επιτραπεί να ολοκληρωθεί.
- Ο υπολογιστής (φορητός υπολογιστής) μεταβαίνει σε λειτουργία μπαταρίας.

Κατά την εκτέλεση μιας σάρωσης παρασκηνίου, το Kaspersky Total Security δεν σαρώνει αρχεία των οποίων τα περιεχόμενα βρίσκονται στον χώρο αποθήκευσης στο cloud του OneDrive.

Για να ενεργοποιήσετε ή να απενεργοποιήσετε μια σάρωση στο παρασκήνιο:

1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.

2. Κάντε κλικ στο κουμπί **Σάρωση**.

Θα ανοίξει το παράθυρο **Σάρωση**.

Στο παράθυρο Σάρωση, κάντε κλικ στο εικονίδιο 🧔 στον αποκλεισμό Σάρωση παρασκηνίου.

Ανοίγει το παράθυρο **Ρυθμίσεις σάρωσης παρασκηνίου**.

4. Στο παράθυρο **Ρυθμίσεις σάρωσης παρασκηνίου**, αλλάξτε τον διακόπτη εναλλαγής σε **Ενεργό** ή **Ανενεργό**.

Πώς να δημιουργήσετε ένα πρόγραμμα σάρωσης

Για να δημιουργήσετε ένα χρονοδιάγραμμα σάρωσης:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Σάρωση**.

Θα ανοίξει το παράθυρο **Σάρωση**.

- 3. Στο παράθυρο **Σάρωση**, επιλέξτε τον τύπο σάρωσης και κάντε κλικ στο εικονίδιο 🧔.
- 4. Στο ανοιχτό παράθυρο, κάντε κλικ στη σύνδεση **Χρονοδιάγραμμα σάρωσης** για να προχωρήσετε στο παράθυρο **Χρονοδιάγραμμα σάρωσης**.
- 5. Στο παράθυρο **Χρονοδιάγραμμα σάρωσης**, στη λίστα **Εκτέλεση σάρωσης**, επιλέξτε μια περίοδο, όπως **Καθημερινά**, και καθορίστε την ώρα έναρξης της σάρωσης.

Δεν είναι δυνατή η δημιουργία χρονοδιαγράμματος σάρωσης για τον τύπο σάρωσης "Σάρωση από το Μενού περιβάλλοντος".

Πώς να αναζητήσετε τρωτά σημεία σε εφαρμογές που είναι εγκατεστημένες στον υπολογιστή σας

Οι εφαρμογές που είναι εγκατεστημένες στον υπολογιστή σας μπορεί να διαθέτουν τρωτά σημεία τα οποία μπορούν να γίνουν αντικείμενα εκμετάλλευσης από κακόβουλα λογισμικά. Η σάρωση του υπολογιστή σας θα βοηθήσει στον εντοπισμό αυτών των τρωτών σημείων και στο να αποτραπεί η μόλυνση του υπολογιστή σας.

Για να ξεκινήσετε μια σάρωση για τρωτά σημεία:

1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.

- Στο κάτω μέρος του κύριου παραθύρου, κάντε κλικ στο κουμπί Περισσότερα εργαλεία.
 Ανοίγει το παράθυρο Εργαλεία.
- 3. Μεταβείτε στην ενότητα **Διαχείριση εφαρμογών**.
- 4. Κάντε κλικ στη σύνδεση **Σάρωση για τρωτά σημεία** για να ανοίξει το παράθυρο **Σάρωση** για τρωτά σημεία.
- 5. Στην ενότητα **Σάρωση για τρωτά σημεία**, κάντε κλικ στο κουμπί **Έναρξη σάρωσης**.

Το Kaspersky Total Security ξεκινά τη σάρωση του υπολογιστή σας για τρωτά σημεία.

Από το Kaspersky Total Security 2021 και μετά, η λειτουργία σάρωσης για τρωτά σημεία του λειτουργικού συστήματος δεν περιλαμβάνεται πλέον στην εφαρμογή. Εάν θέλετε να πραγματοποιήσετε σάρωση για τρωτά σημεία του λειτουργικού συστήματος, μπορείτε να <u>επιστρέψετε στην προηγούμενη έκδοση της εφαρμογής</u>.

Σάρωση αρχείων στον χώρο αποθήκευσης στο cloud στο OneDrive

Σε Windows 10 RS3 ή νεότερες εκδόσεις, το Kaspersky Total Security δεν σαρώνει αρχεία στον χώρο αποθήκευσης στο cloud στο OneDrive. Αν η εφαρμογή εντοπίσει τέτοιου είδους αρχεία στη διάρκεια σάρωσης, εμφανίζει μια ειδοποίηση που δηλώνει ότι τα αρχεία που βρίσκονται σε χώρο αποθήκευσης στο cloud δεν σαρώθηκαν.

Τα ακόλουθα στοιχεία δεν σαρώνουν αρχεία στον χώρο αποθήκευσης στο cloud στο OneDrive:

- Πλήρης σάρωση
- Επιλεκτική σάρωση
- Γρήγορη σάρωση
- Σάρωση παρασκηνίου

Η αναφορά για τη λειτουργία του Kaspersky Total Security περιέχει μια λίστα αρχείων στον χώρο αποθήκευσης στο cloud στο OneDrive τα οποία παραλείφθηκαν κατά τη σάρωση.

Τα αρχεία που λήφθηκαν από τον χώρο αποθήκευσης στο cloud στο OneDrive σε έναν τοπικό υπολογιστή σαρώνονται από στοιχεία προστασίας σε πραγματικό χρόνο. Αν μια σάρωση αρχείων αναβλήθηκε και το αρχείο απεστάλη ξανά στον χώρο αποθήκευσης στο cloud στο OneDrive προτού ξεκινήσει η σάρωση, αυτό το αρχείο μπορεί να παραλειφθεί στη διάρκεια σάρωσης.

Κατά την εκτέλεση εφαρμογών και δεσμών ενεργειών, τα στοιχεία Έλεγχος εφαρμογών και Παρακολούθηση συστημάτων κάνουν λήψη εφαρμογών από το χώρο αποθήκευσης στο cloud του OneDrive στον τοπικό υπολογιστή προς σάρωση.

Για να βεβαιωθείτε ότι τα αρχεία OneDrive εμφανίζονται στην Εξερεύνηση, ενεργοποιήστε τη δυνατότητα <u>Αρχεία κατ' απαίτηση στην εφαρμογή πελάτη</u> <u>OneDrive</u> ^{II}. Εάν είστε συνδεδεμένοι στο Διαδίκτυο, μπορείτε να τα χρησιμοποιήσετε όπως και τα άλλα αρχεία στον υπολογιστή σας.

Τρόπος επαναφοράς ενός αρχείου που διαγράφηκε ή απολυμάνθηκε από την εφαρμογή

Αντίγραφα ασφαλείας αρχείων που διαγράφηκαν ή απολυμάνθηκαν από το Kaspersky Total Security τοποθετούνται σε ειδικό φάκελο στον υπολογιστή σας με το όνομα *Kapavτίva*. Τα αντίγραφα ασφαλείας των αρχείων αποθηκεύονται σε μια ειδική μορφή, η οποία δεν αποτελεί απειλή για τον υπολογιστή. Μπορείτε να επαναφέρετε ένα αρχείο που διαγράφηκε ή απολυμάνθηκε από την εφαρμογή από το αντίγραφο ασφαλείας που έχει αποθηκευτεί στον φάκελο Καραντίνα.

Σας συνιστούμε να αποφύγετε την επαναφορά διαγραμμένων ή απολυμασμένων αρχείων, διότι μπορεί να αποτελούν απειλή για τον υπολογιστή σας!

To Kaspersky Total Security δεν απολυμαίνει τις εφαρμογές του Windows Store. Αν τα αποτελέσματα του ελέγχου υποδείξουν ότι μια από αυτές τις εφαρμογές είναι επικίνδυνη, θα διαγραφεί από τον υπολογιστή σας. Όταν γίνεται διαγραφή μιας εφαρμογής του Windows Store, το Kaspersky Total Security δεν δημιουργεί αντίγραφο ασφαλείας της. Για να επαναφέρετε αντικείμενα αυτού του τύπου, θα πρέπει να χρησιμοποιήσετε τα εργαλεία ανάκτησης που περιλαμβάνει το λειτουργικό σας σύστημα (για λεπτομέρειες, δείτε την τεκμηρίωση που συνοδεύει το λειτουργικό σύστημα που έχει εγκατασταθεί στον υπολογιστή σας) ή να κάνετε ενημέρωση εφαρμογών μέσω του Windows Store.

Για να επαναφέρετε ένα αρχείο που διαγράφηκε ή απολυμάνθηκε από την εφαρμογή:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Περισσότερα εργαλεία** που βρίσκεται στο κάτω μέρος του κεντρικού παραθύρου για να ανοίξετε το παράθυρο **Εργαλεία**.
- 3. Στο παράθυρο **Εργαλεία**, μεταβείτε στην ενότητα **Ασφάλεια**.
- Στην ενότητα Ασφάλεια, κάντε κλικ στη σύνδεση Καραντίνα για να ανοίξετε το παράθυρο Καραντίνα.
- 5. Στο παράθυρο Καραντίνα που θα ανοίξει, επιλέξτε το αρχείο το οποίο θέλετε από τη λίστα και κάντε κλικ στο κουμπί Επαναφορά.

Πώς να κάνετε ανάκτηση του λειτουργικού συστήματος μετά από μόλυνση

Αυτή η ενότητα περιέχει πληροφορίες σχετικά με την επαναφορά του λειτουργικού συστήματος αφού έχει μολυνθεί με κακόβουλο λογισμικό.

Ανάκτηση του λειτουργικού συστήματος μετά από μόλυνση

Αν υποψιάζεστε ότι το λειτουργικό σύστημα του υπολογιστή σας έχει καταστραφεί ή τροποποιηθεί λόγω δραστηριότητας κακόβουλου λογισμικού ή αστοχιών συστήματος, χρησιμοποιήστε τον *Οδηγό αντιμετώπισης προβλημάτων των Microsoft Windows μετά από μόλυνση* με τον οποίο γίνεται εκκαθάριση του συστήματος από οποιαδήποτε ίχνη κακόβουλων αντικειμένων. Η Kaspersky προτείνει να εκτελέσετε τον οδηγό μετά από την απολύμανση του υπολογιστή, για να βεβαιωθείτε ότι έχουν διορθωθεί όλες οι απειλές και οι βλάβες λόγω των μολύνσεων.

Ο Οδηγός ελέγχει εάν έχουν πραγματοποιηθεί αλλαγές στο σύστημα, όπως αποκλεισμός της πρόσβασης στο δίκτυο, αλλαγή επεκτάσεων γνωστών μορφών αρχείων, κλείδωμα της γραμμής εργασιών κ.λπ. Κάθε τύπος βλάβης οφείλεται σε διαφορετικές αιτίες. Ορισμένες από αυτές τις αιτίες ενδέχεται να είναι, μεταξύ άλλων, η δραστηριότητα κακόβουλων προγραμμάτων, η εσφαλμένη ρύθμιση παραμέτρων συστήματος, οι αστοχίες συστήματος ή η εσφαλμένη λειτουργία των εφαρμογών βελτιστοποίησης του συστήματος.

Αφού ολοκληρωθεί η εξέταση, ο Οδηγός αναλύει τις πληροφορίες για να αξιολογήσει εάν υπάρχουν βλάβες στο σύστημα για τις οποίες απαιτείται άμεση ενέργεια. Ανάλογα με την εξέταση, ο Οδηγός δημιουργεί μια λίστα ενεργειών που είναι απαραίτητες για την εξουδετέρωση της βλάβης. Ο Οδηγός ομαδοποιεί αυτές τις ενέργειες σε κατηγορίες με βάση τη σοβαρότητα των προβλημάτων που εντοπίστηκαν.

Αντιμετώπιση προβλημάτων του λειτουργικού συστήματος χρησιμοποιώντας τον Οδηγό αντιμετώπισης προβλημάτων των Microsoft Windows

Για να εκτελέσετε τον Οδηγό αντιμετώπισης προβλημάτων των Microsoft Windows:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Στο κάτω μέρος του κύριου παραθύρου, κάντε κλικ στο κουμπί Περισσότερα εργαλεία.
 Ανοίγει το παράθυρο Εργαλεία.
- 3. Μεταβείτε στην ενότητα **Εκκαθάριση και βελτιστοποίηση**.
- 4. Κάντε κλικ στη σύνδεση **Αντιμετώπιση προβλημάτων των Microsoft Windows** για να εκτελέσετε τον Οδηγό αντιμετώπισης προβλημάτων των Microsoft Windows.

Ανοίγει το παράθυρο του Οδηγού αντιμετώπισης προβλημάτων των Microsoft Windows.

Ο Οδηγός αποτελείται από μια σειρά σελίδων (βήματα), στις οποίες μπορείτε να περιηγηθείτε με τα κουμπιά **Πίσω** και **Επόμενο**. Για να κλείσετε τον Οδηγό αφού ολοκληρωθεί, κάντε κλικ στο κουμπί **Ολοκληρώθηκε**. Για να διακόψετε τον Οδηγό σε οποιοδήποτε στάδιο κι αν βρίσκεται, κάντε κλικ στο κουμπί **Άκυρο**.

Ας δούμε αναλυτικότερα τα βήματα του Οδηγού.

Έναρξη ανάκτησης του λειτουργικού συστήματος

a. Επιλέξτε μία από τις δύο επιλογές για τη λειτουργία του Οδηγού:

- Αναζήτηση για βλάβες που προκλήθηκαν από δραστηριότητες κακόβουλου λογισμικού. Ο Οδηγός θα αναζητήσει προβλήματα και πιθανές βλάβες.
- Επαναφορά αλλαγών. Ο Οδηγός θα επαναφέρει τις επιδιορθώσεις που εφαρμόστηκαν σε προβλήματα και βλάβες που εντοπίστηκαν προηγούμενα.

b. Κάντε κλικ στο κουμπί **Επόμενο**.

Αναζήτηση για προβλήματα

Εάν επιλέξατε το στοιχείο **Αναζήτηση για βλάβες που προκλήθηκαν από δραστηριότητες** κακόβουλου λογισμικού, ο Οδηγός αναζητά προβλήματα και πιθανές βλάβες που πρέπει να επιδιορθωθούν. Όταν ολοκληρωθεί η αναζήτηση, ο Οδηγός θα συνεχίσει αυτόματα στο επόμενο βήμα.

Επιλογή ενεργειών για διόρθωση βλάβης

Οι βλάβες που εντοπίστηκαν στο προηγούμενο βήμα ομαδοποιούνται με βάση τον τύπο κινδύνου που ενέχουν. Για κάθε ομάδα βλαβών, η Kaspersky προτείνει ένα σύνολο ενεργειών για την επιδιόρθωση των βλαβών.

Υπάρχουν τρεις ομάδες:

- Οι Ιδιαίτερα συνιστώμενες ενέργειες εξαλείφουν τα προβλήματα που αποτελούν σοβαρή απειλή για την ασφάλεια. Συνιστάται να αποκαθιστάτε όλες τις βλάβες αυτής της ομάδας.
- Οι Συνιστώμενες ενέργειες αποσκοπούν στην αποκατάσταση της ζημιάς που ενδεχομένως συνιστά απειλή. Συνιστάται επίσης να αποκαθιστάτε τις βλάβες αυτής της ομάδας.
- Οι Πρόσθετες ενέργειες αποκαθιστούν βλάβες του λειτουργικού συστήματος, οι οποίες δεν αποτελούν άμεση απειλή αλλά ενδέχεται να αποτελέσουν κίνδυνο για την ασφάλεια του υπολογιστή στο μέλλον.

Αναπτύξτε τη λίστα της επιλεγμένης ομάδας για να δείτε τις βλάβες εντός της ομάδας.

Για να εμφανιστεί ο Οδηγός διόρθωσης ενός συγκεκριμένου τύπου βλάβης, επιλέξτε το πλαίσιο ελέγχου δίπλα στην περιγραφή της βλάβης. Από προεπιλογή, ο Οδηγός διορθώνει τις βλάβες που ανήκουν στις ομάδες των συνιστώμενων και των έντονα συνιστώμενων ενεργειών. Εάν δεν επιθυμείτε να διορθώσετε έναν συγκεκριμένο τύπο βλάβης, αποεπιλέξτε το πλαίσιο ελέγχου δίπλα του.

Συνιστάται ιδιαίτερα να μην αποεπιλέξετε τα πλαίσια ελέγχου που είναι επιλεγμένα από προεπιλογή, καθώς κάτι τέτοιο θα αφήσει τον υπολογιστή σας ευάλωτο στις απειλές.

Αφού ορίσετε το σύνολο των ενεργειών που θα εκτελέσει ο Οδηγός, κάντε κλικ στο κουμπί **Επόμενο**.

Επιδιόρθωση βλάβης

Ο Οδηγός θα εκτελέσει τις ενέργειες που επιλέχθηκαν στο προηγούμενο βήμα. Ενδέχεται να χρειαστεί αρκετή ώρα για τη διόρθωση της βλάβης. Μετά τη διόρθωση της βλάβης, ο Οδηγός προχωράει αυτόματα στο επόμενο βήμα.

Ολοκλήρωση Οδηγού

Κάντε κλικ στο κουμπί **Ολοκληρώθηκε** για έξοδο από τον Οδηγό.

Ανάκτηση έκτακτης ανάγκης του λειτουργικού συστήματος

Η εφαρμογή Kaspersky Rescue Disk προορίζεται για την ανάκτηση του λειτουργικού συστήματος σε περίπτωση έκτακτης ανάγκης. Μπορείτε να χρησιμοποιείτε τον Kaspersky Rescue Disk για τη σάρωση και την απολύμανση μολυσμένων υπολογιστών που δεν είναι δυνατόν να απολυμανθούν με χρήση άλλων μεθόδων (για παράδειγμα, με εφαρμογές προστασίας από ιούς).

Περισσότερες λεπτομέρειες σχετικά με τη χρήση του Kaspersky Rescue Disk είναι διαθέσιμες <u>στον δικτυακό τόπο τεχνικής υποστήριξης</u> .

Προστασία email

Αυτή η ενότητα παρέχει πληροφορίες σχετικά με την προστασία του email σας ενάντια σε ανεπιθύμητη αλληλογραφία, ιούς και άλλες απειλές.

Διαμόρφωση Προστασίας email από ιούς

Το Kaspersky Total Security επιτρέπει τη σάρωση μηνυμάτων email για επικίνδυνα αντικείμενα, χρησιμοποιώντας το στοιχείο Προστασία email από ιούς. Η Προστασία email από ιούς εκκινείται με την έναρξη του λειτουργικού συστήματος και παραμένει μόνιμα στη μνήμη RAM του υπολογιστή. Σαρώνει όλα τα μηνύματα email που αποστέλλονται ή λαμβάνονται με χρήση των πρωτοκόλλων POP3, SMTP, IMAP, και NNTP, καθώς και μέσω κρυπτογραφημένων συνδέσεων (SSL) με χρήση των πρωτοκόλλων POP3, SMTP και IMAP.

Από προεπιλογή, η Προστασία email από ιούς σαρώνει τόσο τα εισερχόμενα όσο και τα εξερχόμενα μηνύματα. Αν είναι απαραίτητο, μπορείτε να ενεργοποιήσετε τη σάρωση μόνο για εισερχόμενα μηνύματα.

Για να διαμορφώσετε την Προστασία email από ιούς:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- Στην ενότητα Προστασία επιλέξτε το στοιχείο Προστασία email από ιούς.
 Οι ρυθμίσεις Προστασίας email από ιούς εμφανίζονται στο παράθυρο.
- 4. Βεβαιωθείτε ότι ο διακόπτης στο πάνω μέρος του παραθύρου που ενεργοποιεί / απενεργοποιεί την Προστασία email από ιούς είναι ενεργοποιημένος.
- 5. Επιλέξτε ένα επίπεδο ασφαλείας:

- Συνιστάται. Όταν οριστεί αυτό το επίπεδο ασφάλειας, η Προστασία email από ιούς σαρώνει τα εισερχόμενα και τα εξερχόμενα μηνύματα και τις συνημμένες αρχειοθήκες και εκτελεί ευρετική ανάλυση με το επίπεδο λεπτομέρειας Μεσαία σάρωση.
- Χαμηλό. Εάν επιλέξετε αυτό το επίπεδο ασφάλειας, η Προστασία email από ιούς σαρώνει μόνο τα εισερχόμενα μηνύματα και δεν ελέγχει τα συνημμένα αρχεία.
- Υψηλό. Όταν οριστεί αυτό το επίπεδο ασφάλειας, η Προστασία email από ιούς σαρώνει τα εισερχόμενα και τα εξερχόμενα μηνύματα και τις συνημμένες αρχειοθήκες και εκτελεί ευρετική ανάλυση με το επίπεδο λεπτομέρειας Βαθιά σάρωση.
- 6. Στην ενότητα **Ενέργεια σε εντοπισμό απειλών** επιλέξτε μια ενέργεια που πρέπει να εκτελεί η Προστασία email από ιούς όταν εντοπίζεται ένα μολυσμένο αντικείμενο (για παράδειγμα, απολύμανση).

Εάν δεν εντοπιστούν απειλές σε ένα μήνυμα email, ή εάν όλα τα μολυσμένα αντικείμενα έχουν απολυμανθεί με επιτυχία, το μήνυμα θα γίνει διαθέσιμο για περαιτέρω χρήση. Εάν το στοιχείο αποτύχει να απολυμάνει ένα μολυσμένο αντικείμενο, η Προστασία email από ιούς μετονομάζει ή διαγράφει το αντικείμενο από το μήνυμα και προσθέτει στη γραμμή θέματος μια ειδοποίηση που δηλώνει ότι το μήνυμα έχει υποβληθεί σε επεξεργασία από το Kaspersky Total Security. Πριν από τη διαγραφή ενός αντικειμένου, το Kaspersky Total Security δημιουργεί ένα αντίγραφο ασφαλείας του και το τοποθετεί στην <u>Καραντίνα</u>.

Όταν εκτελείτε αναβάθμιση σε πιο πρόσφατη έκδοση της εφαρμογής, δεν αποθηκεύονται οι ρυθμίσεις Προστασίας email από ιούς που έχουν γίνει από τον χρήστη. Η νέα έκδοση της εφαρμογής θα χρησιμοποιήσει τις προεπιλεγμένες ρυθμίσεις Προστασίας email από ιούς.

Εάν το Kaspersky Total Security εντοπίσει τον κωδικό πρόσβασης για την αρχειοθήκη στο μήνυμα κατά τη διάρκεια της σάρωσης, ο κωδικός πρόσβασης χρησιμοποιείται για τη σάρωση των περιεχομένων της εν λόγω αρχειοθήκης για κακόβουλο λογισμικό. Ο κωδικός πρόσβασης δεν αποθηκεύεται. Η αρχειοθήκη αποσυσκευάζεται πριν από τη σάρωση. Εάν η εφαρμογή καταρρεύσει κατά την αποσυσκευασία της αρχειοθήκης, μπορείτε να διαγράψετε χειροκίνητα τα αρχεία που έχουν αποσυσκευαστεί στην ακόλουθη διαδρομή: %systemroot%\temp. Τα αρχεία έχουν το πρόθεμα PR.

Αποκλεισμός ανεπιθύμητων email (spam)

Εάν λαμβάνετε μια μεγάλη ποσότητα ανεπιθύμητων μηνυμάτων (spam), συνιστούμε να ενεργοποιήσετε το στοιχείο Πρόγραμμα Anti-Spam και να το ρυθμίσετε στο επίπεδο ασφάλειας **Συνιστάται**.

Για να ενεργοποιήσετε το Πρόγραμμα Anti-Spam και να ρυθμίσετε το επίπεδο ασφάλειας Συνιστάται:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.
- 4. Επιλέξτε το στοιχείο Πρόγραμμα Anti-Spam.

Το παράθυρο εμφανίζει τις ρυθμίσεις του Προγράμματος Anti-Spam.

- 5. Ενεργοποιήστε το Πρόγραμμα Anti-Spam χρησιμοποιώντας τον διακόπτη.
- 6. Στην ενότητα **Επίπεδο ασφαλείας** βεβαιωθείτε ότι έχει οριστεί το **Συνιστάται**.

Οι ακόλουθοι περιορισμοί ισχύουν για το Πρόγραμμα Anti-Spam:

- Το στοιχείο Πρόγραμμα Anti-Spam μπορεί να αναλύει μόνο τα μηνύματα που έχουν πλήρως καταφορτωθεί από τον διακομιστή αλληλογραφίας, ανεξάρτητα από το πρωτόκολλο που χρησιμοποιείται.
- Το στοιχείο Πρόγραμμα Anti-Spam δεν ελέγχει την αλληλογραφία που ανταλλάσσεται με χρήση πρωτοκόλλου MAPI.

Το στοιχείο Πρόγραμμα Anti-Spam απενεργοποιείται όταν πραγματοποιείται αναβάθμιση σε πιο πρόσφατη έκδοση της εφαρμογής. Μπορείτε να ενεργοποιήσετε το στοιχείο χειροκίνητα.

Σε <u>ορισμένες εκδόσεις της εφαρμογής</u>, για να ενεργοποιήσετε το στοιχείο Πρόγραμμα Anti-Spam, πρέπει να αποδεχτείτε τους όρους της δήλωσης σχετικά με την επεξεργασία δεδομένων για το Πρόγραμμα Anti-Spam.

Προστασία προσωπικών δεδομένων στο Διαδίκτυο

Η ενότητα αυτή παρέχει πληροφορίες για την ασφαλή περιήγησή σας στο Διαδίκτυο και την προστασία των δεδομένων σας από κλοπή.

Σχετικά με την προστασία των προσωπικών δεδομένων στο Διαδίκτυο

Το Kaspersky Total Security σάς βοηθάει να προστατεύσετε τα προσωπικά σας δεδομένα από κλοπή:

- Κωδικοί πρόσβασης, ονόματα χρήστη και άλλα στοιχεία εγγραφής
- Αριθμούς λογαριασμών και αριθμούς τραπεζικών καρτών

To Kaspersky Total Security περιλαμβάνει στοιχεία και εργαλεία που σας επιτρέπουν να προστατευτείτε από εγκληματίες που χρησιμοποιούν μεθόδους όπως <u>phishing</u> ή υποκλοπή των δεδομένων που καταχωρούνται στο πληκτρολόγιο για να αποκτήσουν πρόσβαση στα προσωπικά δεδομένα σας.

Η προστασία κατά του phishing παρέχεται μέσω του Προγράμματος κατά του phishing, το οποίο ενσωματώνεται στην Προστασία από ιούς στο Web και το Πρόγραμμα Anti-Spam. Ενεργοποιήστε τα στοιχεία αυτά για να διασφαλίσετε την εκτεταμένη προστασία κατά του phishing.

Η προστασία από υποκλοπή των δεδομένων που πληκτρολογείτε παρέχεται από τις λειτουργίες Πληκτρολόγιο οθόνης και Καταχώρηση σε ασφαλές πληκτρολόγιο.

Ο Οδηγός εκκαθάρισης ιδιωτικού απορρήτου έχει σχεδιαστεί για την εκκαθάριση από τον υπολογιστή όλων των πληροφοριών σχετικά με τις δραστηριότητες του χρήστη.

Τα στοιχεία Ασφαλείς τραπεζικές συναλλαγές και Kaspersky VPN προστατεύουν τα δεδομένα όταν χρησιμοποιείτε τραπεζικές υπηρεσίες διαδικτύου και πραγματοποιείτε αγορές σε διαδικτυακά καταστήματα.

Προστασία από μεταφορά προσωπικών δεδομένων μέσω του Διαδικτύου παρέχεται από ένα από τα εργαλεία <u>Γονικού ελέγχου</u>.

Πληροφορίες για το Πληκτρολόγιο οθόνης

Κατά την εργασία στο Διαδίκτυο, συχνά χρειάζεται να πληκτρολογήσετε προσωπικά δεδομένα σας ή το όνομα χρήστη και τον κωδικό πρόσβασης. Αυτό συμβαίνει, για παράδειγμα, κατά την εγγραφή λογαριασμού σε δικτυακούς τόπους, τις ηλεκτρονικές αγορές ή τις τραπεζικές συναλλαγές στο διαδίκτυο. Υπάρχει κίνδυνος υποκλοπής των προσωπικών δεδομένων με τη χρήση είτε υποκλοπέων πληκτρολογίου υλικού είτε καταγραφέων πληκτρολόγησης (keylogger), οι οποίοι αποτελούν προγράμματα που καταγράφουν τα δεδομένα που εισάγονται μέσω του πληκτρολογίου. Το Πληκτρολόγιο οθόνης αποτρέπει την υποκλοπή των δεδομένων που εισάγονται μέσω πληκτρολογίου.

Πολλά από τα προγράμματα που κατηγοριοποιούνται ως λογισμικό υποκλοπής έχουν τη δυνατότητα λήψης στιγμιότυπων οθόνης, τα οποία στη συνέχεια μεταδίδονται σε κάποιον εισβολέα για περαιτέρω ανάλυση και κλοπή προσωπικών δεδομένων του χρήστη. Το Πληκτρολόγιο οθόνης προστατεύει τα προσωπικά δεδομένα που καταχωρούνται από απόπειρες υποκλοπής με λήψη στιγμιοτύπων οθόνης.

Το Πληκτρολόγιο οθόνης έχει τις ακόλουθες δυνατότητες:

- Μπορείτε να κάνετε κλικ στα κουμπιά του Πληκτρολογίου οθόνης χρησιμοποιώντας το ποντίκι.
- Σε αντίθεση με τα πληκτρολόγια υλικού, είναι αδύνατο να πατήσετε πολλά πλήκτρα ταυτόχρονα στο Πληκτρολόγιο οθόνης. Αυτός είναι ο λόγος για τον οποίο συνδυασμοί πλήκτρων (όπως ALT+F4) απαιτούν να πατήσετε το πρώτο πλήκτρο (π.χ. ALT), έπειτα το δεύτερο πλήκτρο (π.χ. F4) και, στη συνέχεια, πάλι το πρώτο πλήκτρο. Το δεύτερο κλικ στο πλήκτρο λειτουργεί όπως όταν αφήνετε το πλήκτρο σε ένα πραγματικό πληκτρολόγιο.
- Η αλλαγή γλώσσας στο Πληκτρολόγιο οθόνης μπορεί να γίνει με την ίδια συντόμευση που έχει οριστεί στις ρυθμίσεις του λειτουργικού συστήματος για το πραγματικό πληκτρολόγιο. Για να το κάνετε αυτό, κάντε δεξί κλικ στο άλλο πλήκτρο (π.χ. αν στις ρυθμίσεις του λειτουργικού συστήματος έχει οριστεί η συντόμευση APIΣTEPO ALT+SHIFT για εναλλαγή της γλώσσας του πληκτρολογίου, πρέπει να κάνετε αριστερό κλικ στο πλήκτρο APIΣTEPO ALT και δεξί κλικ στο πλήκτρο SHIFT).

Για τη διασφάλιση της προστασίας των δεδομένων που έχουν εισαχθεί μέσω του Πληκτρολογίου οθόνης, κάντε επανεκκίνηση του υπολογιστή σας μετά την εγκατάσταση του Kaspersky Total Security.

Το Πληκτρολόγιο οθόνης έχει τους εξής περιορισμούς:

 Το Πληκτρολόγιο οθόνης αποτρέπει την υποκλοπή των προσωπικών δεδομένων μόνο κατά την εργασία με τα προγράμματα περιήγησης Microsoft Edge που βασίζεται στο Chromium, Mozilla Firefox και Google Chrome. Όταν χρησιμοποιείται με άλλα προγράμματα περιήγησης, το Πληκτρολόγιο οθόνης δεν προστατεύει από υποκλοπή τα προσωπικά δεδομένα που εισάγονται.

- Το Πληκτρολόγιο οθόνης δεν μπορεί να προστατεύσει τα προσωπικά δεδομένα σας εάν ο δικτυακός τόπος που ζήτησε την εισαγωγή των εν λόγω δεδομένων έχει πέσει θύμα χάκερ, επειδή σε αυτήν την περίπτωση οι πληροφορίες φτάνουν απευθείας στα χέρια των εισβολέων.
- Το Πληκτρολόγιο οθόνης δεν αποτρέπει τα στιγμιότυπα οθόνης που δημιουργούνται χρησιμοποιώντας το πλήκτρο Print Screen και άλλους συνδυασμούς πλήκτρων που προσδιορίζονται στις ρυθμίσεις του λειτουργικού συστήματος.

Το Kaspersky Total Security δεν παρέχει προστασία από μη εξουσιοδοτημένα στιγμιότυπα οθόνης στα Microsoft Windows 8 και 8.1 (64-bit μόνο) εάν το παράθυρο του Πληκτρολογίου οθόνης είναι ανοιχτό, αλλά δεν έχει ξεκινήσει η διεργασία του Προστατευμένου προγράμματος περιήγησης.

Στην παραπάνω λίστα περιγράφονται οι βασικοί περιορισμοί στη λειτουργία προστασίας της καταχώρησης δεδομένων. Μπορείτε να δείτε την πλήρη λίστα των περιορισμών στο σχετικό <u>άρθρο στον δικτυακό τόπο τεχνικής υποστήριξης της Kaspersky</u> .

Πώς να ανοίξετε το πληκτρολόγιο οθόνης

Μπορείτε να ανοίξετε το Πληκτρολόγιο οθόνης με τους ακόλουθους τρόπους:

- Από το παράθυρο της εφαρμογής
- Από τη γραμμή εργαλείων των Microsoft Edge που βασίζεται στο Chromium, Mozilla Firefox ή Google Chrome
- Χρησιμοποιώντας το εικονίδιο γρήγορης εκκίνησης του Πληκτρολογίου οθόνης στα πεδία εισαγωγής σε δικτυακούς τόπους

Μπορείτε να <u>διαμορφώσετε</u> τις ρυθμίσεις εμφάνισης του εικονιδίου γρήγορης εκκίνησης του Εικονικού πληκτρολογίου στα πεδία εισαγωγής σε δικτυακούς τόπους.

Όταν το Πληκτρολόγιο οθόνης χρησιμοποιείται, το Kaspersky Total Security απενεργοποιεί την επιλογή για αυτόματη συμπλήρωση των πεδίων καταχώρησης σε δικτυακούς τόπους.

• Με το πάτημα ενός συνδυασμού πλήκτρων του πληκτρολογίου

Έναρξη του Πληκτρολογίου οθόνης από το παράθυρο της εφαρμογής 💿

Για να ανοίξετε το Πληκτρολόγιο οθόνης από το παράθυρο της εφαρμογής:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Στο κάτω μέρος του κύριου παραθύρου, κάντε κλικ στο κουμπί Περισσότερα εργαλεία.

Ανοίγει το παράθυρο **Εργαλεία**.

- 3. Μεταβείτε στην ενότητα **Ασφάλεια**.
- 4. Κάντε κλικ στη σύνδεση **Πληκτρολόγιο οθόνης** για να ανοίξετε το Πληκτρολόγιο Οθόνης.

<u>Έναρξη του Πληκτρολογίου οθόνης από τη γραμμή εργαλείων του προγράμματος</u> <u>περιήγησης</u>

Για να ανοίξετε το Πληκτρολόγιο οθόνης από τη γραμμή εργαλείων σε προγράμματα περιήγησης όπως τα Microsoft Edge που βασίζεται στο Chromium, Mozilla Firefox ή Google Chrome:

- 1. Κάντε κλικ στο κουμπί 📀 **Kaspersky Protection** στη γραμμή εργαλείων του προγράμματος περιήγησης.
- 2. Επιλέξτε το στοιχείο **Πληκτρολόγιο οθόνης** από το μενού που ανοίγει.

Έναρξη Πληκτρολογίου οθόνης με χρήση του πληκτρολογίου του υπολογιστή 🖓

Για να ανοίξετε το Πληκτρολόγιο οθόνης με χρήση του πληκτρολογίου του υπολογιστή:

Πιέστε το συνδυασμό πλήκτρων CTRL+ALT+SHIFT+P.

Πώς να διαμορφώσετε την εμφάνιση του εικονιδίου του Πληκτρολογίου οθόνης

Για να διαμορφώσετε τις ρυθμίσεις εμφάνισης του εικονιδίου γρήγορης εκκίνησης του Πληκτρολογίου οθόνης στα πεδία εισαγωγής δεδομένων σε δικτυακούς τόπους:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Πρόσθετα**.

Το παράθυρο εμφανίζει τις ρυθμίσεις για την προστασία της καταχώρησης δεδομένων.

- 4. Στον αποκλεισμό **Πληκτρολόγιο οθόνης**, ενεργοποιήστε το πλαίσιο ελέγχου **Άνοιγμα του Πληκτρολογίου οθόνης εάν πιεστεί ο συνδυασμός πλήκτρων CTRL+ALT+SHIFT+P**.
- 5. Αν θέλετε το εικονίδιο γρήγορης εκκίνησης του Πληκτρολογίου οθόνης να εμφανίζεται στα πεδία εισόδου όλων των δικτυακών τόπων, ενεργοποιήστε το πλαίσιο ελέγχου **Εμφάνιση εικονιδίου γρήγορης εκκίνησης σε πεδία εισαγωγής δεδομένων**.
- 6. Εάν θέλετε το εικονίδιο γρήγορης εκκίνησης του Πληκτρολογίου οθόνης να εμφανίζεται μόνο όταν ανοίγουν τοποθεσίες web συγκεκριμένων κατηγοριών, επιλέξτε τα πλαίσια ελέγχου για τις κατηγορίες τοποθεσιών web στις οποίες το εικονίδιο γρήγορης εκκίνησης του Πληκτρολογίου οθόνης εμφανίζεται στα πεδία εισαγωγής.

Το εικονίδιο γρήγορης εκκίνησης του Πληκτρολογίου οθόνης εμφανίζεται κατά την πρόσβαση σε έναν δικτυακό τόπο που ανήκει σε οποιαδήποτε από τις επιλεγμένες κατηγορίες.

- 7. Εάν θέλετε να ενεργοποιήσετε ή να απενεργοποιήσετε την εμφάνιση του εικονιδίου γρήγορης εκκίνησης του Πληκτρολογίου οθόνης σε ένα συγκεκριμένο δικτυακό τόπο:
 - a. Στον αποκλεισμό Πληκτρολόγιο οθόνης, κάντε κλικ στη σύνδεση Διαχείριση
 εξαιρέσεων για να ανοίξετε το παράθυρο Εξαιρέσεις για το Πληκτρολόγιο οθόνης.
 - b. Στο κάτω μέρος του παραθύρου, κάντε κλικ στο κουμπί **Προσθήκη**.
 - c. Ανοίγει ένα παράθυρο για την προσθήκη εξαίρεσης για το Πληκτρολόγιο οθόνης.
 - d. Στο πεδίο **Μάσκα διεύθυνσης web**, καταχωρίστε τη διεύθυνση web ενός δικτυακού τόπου.
 - e. Στην ενότητα **Πεδίο**, επιλέξτε εάν θέλετε να εμφανίζεται (ή να μην εμφανίζεται) το εικονίδιο γρήγορης εκκίνησης του πληκτρολογίου οθόνης: στην καθορισμένη σελίδα ή σε όλες τις σελίδες του δικτυακού τόπου.

- f. Στην ενότητα **Εικονίδιο για το Πληκτρολόγιο οθόνης**, επιλέξτε εάν θέλετε να εμφανίζεται το εικονίδιο γρήγορης εκκίνησης του πληκτρολογίου οθόνης.
- g. Κάντε κλικ στο κουμπί **Προσθήκη**.

Ο συγκεκριμένος δικτυακός τόπος εμφανίζεται στη λίστα στο παράθυρο **Εξαιρέσεις** για το Πληκτρολόγιο οθόνης.

Κατά την πρόσβαση στο συγκεκριμένο δικτυακό τόπο, το εικονίδιο γρήγορης εκκίνησης του Πληκτρολογίου οθόνης θα εμφανιστεί στα πεδία εισαγωγής σύμφωνα με τις καθορισμένες ρυθμίσεις.

Πληροφορίες σχετικά με την προστασία δεδομένων που εισάγονται από το πληκτρολόγιο του υπολογιστή

Η προστασία των δεδομένων που εισάγονται από το πληκτρολόγιο του υπολογιστή επιτρέπει την αποφυγή της υποκλοπής των δεδομένων που καταχωρούνται σε δικτυακούς τόπους με το πληκτρολόγιο. Για να ενεργοποιήσετε την προστασία της εισαγωγής δεδομένων στο πληκτρολόγιο, η <u>επέκταση Kaspersky Protection θα πρέπει να ενεργοποιηθεί</u> στο πρόγραμμα περιήγησης. Μπορείτε να ρυθμίσετε τις παραμέτρους της προστασίας της καταχώρησης δεδομένων μέσω του πληκτρολογίου του υπολογιστή σε διάφορους δικτυακούς τόπους. Μόλις διαμορφωθεί η Καταχώρηση σε ασφαλές πληκτρολόγιο, ένα αναδυόμενο μήνυμα που δηλώνει ότι η Καταχώρηση σε ασφαλές πληκτρολόγιο είναι ενεργοποιημένη εμφανίζεται δίπλα στο πεδίο στο οποίο έχει τοποθετηθεί ο δείκτης του ποντικιού. Από προεπιλογή, η Καταχώρηση σε ασφαλές πληκτρολόγιο είναι ενεργοποιημένη για όλες τις κατηγορίες τοποθεσιών web εκτός τη Διαδικτυακή επικοινωνία.

Η Καταχώρηση σε ασφαλές πληκτρολόγιο έχει τους εξής περιορισμούς:

- Η Καταχώρηση σε ασφαλές πληκτρολόγιο είναι διαθέσιμη μόνο για τα προγράμματα περιήγησης Microsoft Edge που βασίζεται στο Chromium, Mozilla Firefox και Google Chrome. Εάν εργάζεστε με άλλα προγράμματα περιήγησης, τα δεδομένα που εισάγετε μέσω του πραγματικού πληκτρολογίου δεν προστατεύονται από υποκλοπές.
- Η Καταχώρηση σε ασφαλές πληκτρολόγιο δεν λειτουργεί σε προγράμματα περιήγησης που εκτελούνται στην εφαρμογή Sandboxie.
- Η προστασία των δεδομένων που καταχωρούνται μέσω του πληκτρολογίου του υπολογιστή δεν μπορεί να προστατεύσει τα προσωπικά δεδομένα σας εάν ο δικτυακός τόπος που ζήτησε την εισαγωγή των εν λόγω δεδομένων έχει πέσει θύμα χάκερ, επειδή σε αυτήν την περίπτωση οι πληροφορίες φτάνουν απευθείας στα χέρια των εισβολέων.

Στην παραπάνω λίστα περιγράφονται οι βασικοί περιορισμοί στη λειτουργία προστασίας της καταχώρησης δεδομένων. Μπορείτε να δείτε την πλήρη λίστα των περιορισμών στο σχετικό <u>άρθρο στον δικτυακό τόπο τεχνικής υποστήριξης της Kaspersky</u>

Περιορισμοί Ασφαλούς καταχώρησης δεδομένων

Η Ασφαλής καταχώρηση δεδομένων στο Kaspersky Total Security έχει τους εξής περιορισμούς:

- Η προστασία λειτουργεί μόνο στα ακόλουθα προγράμματα περιήγησης: Microsoft Edge με βάση τα Chromium, Mozilla Firefox, Mozilla Firefox ESR και Google Chrome, όταν η επέκταση Kaspersky Protection είναι εγκατεστημένη και ενεργοποιημένη.
- Η προστασία λειτουργεί μόνο για σελίδες που πληρούν τις ακόλουθες προϋποθέσεις:
 - Η σελίδα βρίσκεται σε μια λίστα διευθύνσεων URL ή μια κατηγορία σελίδων που απαιτούν Καταχώρηση σε ασφαλές πληκτρολόγιο.
 - Η σελίδα είναι ανοιχτή σε ένα Προστατευμένο πρόγραμμα περιήγησης.
 - Η σελίδα δεν βρίσκεται στη λίστα εξαίρεσης διευθύνσεων URL.
 - Η σελίδα περιέχει ένα πεδίο για την εισαγωγή κωδικού πρόσβασης. Ταυτόχρονα, το πλαίσιο ελέγχου δίπλα στην κατηγορία "Πεδία εισαγωγής κωδικών πρόσβασης σε όλες τις τοποθεσίες web" θα πρέπει να έχει επιλεγεί στις ρυθμίσεις της εφαρμογής.
 - Για να επαληθεύσετε εάν το πλαίσιο ελέγχου είναι επιλεγμένο, μεταβείτε στις ρυθμίσεις Πρόσθετα → Ασφαλής καταχώρηση δεδομένων. Στην ενότητα "Καταχώρηση σε ασφαλές πληκτρολόγιο", κάντε κλικ στην επιλογή "Επεξεργασία κατηγοριών".
- Η προστασία λειτουργεί μόνο για πεδία που πληρούν τις ακόλουθες προϋποθέσεις:
 - Το πεδίο εισαγωγής είναι μία γραμμή και αντιστοιχεί στην ετικέτα HTML <input>.
 - Το πεδίο εισαγωγής δεν είναι κρυφό: η τιμή του χαρακτηριστικού τύπου δεν ισούται με "κρυφό" και στα στυλ CSS το πεδίο εμφάνισης δεν έχει οριστεί σε "κανένα".

- Τα πεδία εισαγωγής δεν είναι πεδία τύπου υποβολής, επιλογής, πλαισίου ελέγχου, κουμπιού ή εικόνας.
- Το πεδίο εισαγωγής δεν πρέπει να είναι μόνο για ανάγνωση (readOnly).
- Το πεδίο εισαγωγής θα πρέπει να είναι έτοιμο για εισαγωγή (με εστίαση).
- Εάν το πεδίο έχει το χαρακτηριστικό μέγιστου μήκους (maxlength), ο ελάχιστος αριθμός χαρακτήρων που μπορούν να εισαχθούν πρέπει να είναι περισσότεροι από τρεις.
- Η προστασία δεν λειτουργεί στις ακόλουθες περιπτώσεις:
 - Τα δεδομένα εισάγονται χρησιμοποιώντας την τεχνολογία ΙΜΕ.
 - Το πεδίο εισαγωγής δεν είναι πεδίο εισαγωγής κωδικού πρόσβασης.

Στη διάρκεια της περιόδου μετά την εγκατάσταση του Kaspersky Total Security, αλλά πριν από την επανεκκίνηση του υπολογιστή για πρώτη φορά, η εφαρμογή δεν θα παρεμποδίσει τον πρώτο χαρακτήρα που εισάγει ο χρήστης (σε οποιαδήποτε εφαρμογή).

Εάν αντιμετωπίζετε δυσκολίες, <u>στείλτε ένα αίτημα</u> 🖬 με λεπτομερή περιγραφή του προβλήματος στην ομάδα τεχνικής υποστήριξης της Kaspersky μέσω του My Kaspersky.

Για οδηγίες σχετικά με την εργασία με το My Kaspersky, ανατρέξτε στη Βοήθεια 🗹 .

Τρόπος ρύθμισης των παραμέτρων προστασίας των δεδομένων που εισάγονται από το πληκτρολόγιο του υπολογιστή

Για να ρυθμίσετε τις παραμέτρους της προστασίας των δεδομένων που εισάγονται από το πληκτρολόγιο του υπολογιστή:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- Στην ενότητα Πρόσθετα, επιλέξτε την υποενότητα Ασφαλής καταχώρηση δεδομένων.
 Το παράθυρο εμφανίζει τις ρυθμίσεις για την προστασία της καταχώρησης δεδομένων.

- 4. Στο κάτω μέρος του παραθύρου, στην ενότητα Καταχώρηση σε ασφαλές πληκτρολόγιο, επιλέξτε το πλαίσιο ελέγχου Ενεργοποίηση καταχώρησης σε ασφαλές πληκτρολόγιο.
- 5. Ανοίξτε το παράθυρο **Ρυθμίσεις για την Ασφαλή καταχώρηση δεδομένων** κάνοντας κλικ στη σύνδεση **Επεξεργασία κατηγοριών** στο κάτω μέρος της ενότητας **Καταχώρηση σε ασφαλές πληκτρολόγιο**.
- 6. Επιλέξτε τα πλαίσια ελέγχου για τις κατηγορίες των δικτυακών τόπων όπου θέλετε να προστατεύσετε τα δεδομένα που εισάγονται μέσω του πληκτρολογίου.
- 7. Αν θέλετε να ενεργοποιήσετε ή να απενεργοποιήσετε την προστασία της καταχώρησης δεδομένων μέσω του πληκτρολογίου του υπολογιστή σε έναν συγκεκριμένο δικτυακό τόπο:
 - a. Ανοίξτε το παράθυρο **Εξαιρέσεις για την Καταχώρηση σε ασφαλές πληκτρολόγιο** κάνοντας κλικ στη σύνδεση **Διαχείριση εξαιρέσεων**.
 - b. Στο παράθυρο, κάντε κλικ στο κουμπί **Προσθήκη**.
 - c. Ανοίγει ένα παράθυρο για την προσθήκη εξαίρεσης στην Καταχώρηση σε ασφαλές πληκτρολόγιο.
 - d. Στο παράθυρο που ανοίγει, στο πεδίο **Μάσκα διεύθυνσης web** καταχωρήστε μια διεύθυνση ενός δικτυακού τόπου.
 - e. Επιλέξτε μία από τις επιλογές Ασφαλούς καταχώρησης δεδομένων σε αυτόν τον δικτυακό τόπο (**Εφαρμογή στην καθορισμένη σελίδα** ή **Εφαρμογή σε ολόκληρη την τοποθεσία web**).
 - f. Επιλέξτε την ενέργεια που θα εκτελεστεί από την Ασφαλή καταχώριση δεδομένων σε αυτό το δικτυακό τόπο (**Προστασία** ή **Χωρίς προστασία**).
 - g. Κάντε κλικ στο κουμπί **Προσθήκη**.

Ο συγκεκριμένος δικτυακός τόπος εμφανίζεται στη λίστα στο παράθυρο **Εξαιρέσεις για την Καταχώρηση σε ασφαλές πληκτρολόγιο**. Κατά την πρόσβαση σε αυτήν την τοποθεσία web, η Ασφαλής καταχώρηση δεδομένων θα είναι ενεργή και θα λειτουργεί σύμφωνα με τις ρυθμίσεις.

Έλεγχος δικτυακού τόπου ως προς την ασφάλεια

To Kaspersky Total Security σάς παρέχει τη δυνατότητα ελέγχου της ασφάλειας ενός δικτυακού τόπου πριν κάνετε κλικ σε έναν σύνδεσμο για να τον ανοίξετε. Οι δικτυακοί τόποι ελέγχονται χρησιμοποιώντας τον *Σύμβουλος URL.*

Το στοιχείο "Σύμβουλος URL" ελέγχει τις συνδέσεις στις ιστοσελίδες που ανοίγουν στον Microsoft Edge που βασίζεται στο Chromium, το Google Chrome ή το Mozilla Firefox. Το Kaspersky Total Security εμφανίζει ένα από τα παρακάτω εικονίδια δίπλα σε κάθε σύνδεση που έχει ελεγχθεί:

🥑 – αν ο συνδεδεμένος δικτυακός τόπος είναι ασφαλής σύμφωνα με την Kaspersky

 αν δεν υπάρχουν πληροφορίες σχετικά με την κατάσταση ασφαλείας του συνδεδεμένου δικτυακού τόπου

Από προεπιλογή, το Kaspersky Total Security ελέγχει τις συνδέσεις μόνο στα αποτελέσματα αναζήτησης. Μπορείτε να ενεργοποιήσετε την επιλογή ελέγχου των συνδέσεων σε κάθε δικτυακό τόπο.

Για να ενεργοποιήσετε την επιλογή ελέγχου των συνδέσεων σε κάθε δικτυακό τόπο:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- Στην ενότητα Προστασία επιλέξτε την υποενότητα Προστασία από ιούς στο Web.
 Το παράθυρο εμφανίζει τις ρυθμίσεις για την Προστασία από ιούς στο Web.
- 4. Στο κάτω μέρος του παραθύρου, κάντε κλικ στη σύνδεση Ρυθμίσεις για προχωρημένους. Ανοίγει το παράθυρο ρυθμίσεων για προχωρημένους της Προστασίας από ιούς στο Web.
- 5. Στην ενότητα **Σύμβουλος URL** ενεργοποιήστε το πλαίσιο ελέγχου Έλεγχος URL.

- 6. Εάν θέλετε το Kaspersky Total Security να σαρώνει το περιεχόμενο όλων των δικτυακών τόπων, επιλέξτε **Σε όλες τις τοποθεσίες web εκτός από τις καθορισμένες**.
- 7. Εάν είναι απαραίτητο, καθορίστε τις ιστοσελίδες που εμπιστεύεστε στο παράθυρο Εξαιρέσεις. Ανοίξτε αυτό το παράθυρο κάνοντας κλικ στη σύνδεση Διαχείριση εξαιρέσεων. Το Kaspersky Total Security δεν θα σαρώνει το περιεχόμενο των καθορισμένων ιστοσελίδων.
- 8. Αν θέλετε το Kaspersky Total Security να ελέγχει το περιεχόμενο των συγκεκριμένων ιστοσελίδων μόνο:
 - a. Επιλέξτε **Μόνο στις καθορισμένες τοποθεσίες web**.
 - b. Κάντε κλικ στη σύνδεση **Ρύθμιση παραμέτρων ελεγμένων τοποθεσιών web** για να ανοίξετε το παράθυρο **Ελεγμένες τοποθεσίες web**.
 - c. Κάντε κλικ στο κουμπί **Προσθήκη**.
 - d. Εισαγάγετε τη διεύθυνση της ιστοσελίδας, το περιεχόμενο της οποίας θέλετε να ελέγξετε.
 - e. Επιλέξτε την κατάσταση ελέγχου του δικτυακού τόπου (εάν η κατάσταση είναι *Ενεργό*, το Kaspersky Total Security ελέγχει το περιεχόμενο του δικτυακού τόπου).
 - f. Κάντε κλικ στο κουμπί **Προσθήκη**.

Η συγκεκριμένη ιστοσελίδα εμφανίζεται στη λίστα του παραθύρου **Ελεγμένες τοποθεσίες web**. Το Kaspersky Total Security ελέγχει τις διευθύνσεις URL σε αυτόν τον δικτυακό τόπο.

- 9. Για να διαμορφώσετε τις ρυθμίσεις για προχωρημένους για τον έλεγχο URL, στο παράθυρο Ρυθμίσεις για προχωρημένους για την Προστασία από ιούς στο Web, στην ενότητα Σύμβουλος URL, κάντε κλικ στη σύνδεση Ρύθμιση παραμέτρων Συμβούλου URL για να ανοίξετε το παράθυρο Σύμβουλος URL.
- Εάν θέλετε το Kaspersky Total Security να σας ενημερώνει για την ασφάλεια των συνδέσμων σε όλες τις ιστοσελίδες, στην ενότητα Ελεγμένες διευθύνσεις URL, επιλέξτε Όλες οι διευθύνσεις URL.
- Εάν θέλετε το Kaspersky Total Security να εμφανίζει πληροφορίες για το εάν ο σύνδεσμος ανήκει σε συγκεκριμένη κατηγορία περιεχομένου δικτυακού τόπου (για παράδειγμα, *Βωμολοχίες, αισχρότητες*):

- a. Επιλέξτε το πλαίσιο ελέγχου **Εμφάνιση πληροφοριών σχετικά με τις κατηγορίες περιεχομένου των τοποθεσιών web**.
- b. Επιλέξτε τα πλαίσια ελέγχου δίπλα στις κατηγορίες του περιεχομένου δικτυακού τόπου για το ποιες πληροφορίες πρέπει να εμφανίζονται στα σχόλια.

To Kaspersky Total Security ελέγχει τις συνδέσεις στους καθορισμένους δικτυακούς τόπους και εμφανίζει πληροφορίες σχετικά με τις κατηγορίες των συνδέσεων σύμφωνα με τις επιλεγμένες ρυθμίσεις.

Τρόπος αλλαγής των ρυθμίσεων κρυπτογραφημένων συνδέσεων

Οι κρυπτογραφημένες συνδέσεις δημιουργούνται μέσω των πρωτοκόλλων SSL και TLS. Από προεπιλογή, το Kaspersky Total Security σαρώνει κρυπτογραφημένων τέτοιες συνδέσεις κατόπιν αίτησης από τα στοιχεία προστασίας, όπως Προστασία email από ιούς, Πρόγραμμα Anti-Spam, Ασφαλείς τραπεζικές συναλλαγές, Σύμβουλος URL, Ιδιωτική περιήγηση, Προστασία από ιούς στο Web, και Πρόγραμμα Anti-Banner.

Για την αλλαγή των ρυθμίσεων κρυπτογραφημένων συνδέσεων:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί 🧔 που βρίσκεται στο κάτω μέρος του παραθύρου.

Ανοίγει το παράθυρο **Ρυθμίσεις**.

- 3. Μεταβείτε στην ενότητα **Ρυθμίσεις δικτύου**.
- 4. Επιλέξτε την ενέργεια που θέλετε να εκτελείται κατά τη σύνδεση σε δικτυακούς τόπους μέσω κρυπτογραφημένης σύνδεσης:
 - Να μη γίνεται σάρωση των κρυπτογραφημένων συνδέσεων. Η εφαρμογή δεν σαρώνει κρυπτογραφημένες συνδέσεις.
 - Σάρωση κρυπτογραφημένων συνδέσεων κατόπιν αίτησης από τα στοιχεία προστασίας. Η εφαρμογή σαρώνει κρυπτογραφημένες συνδέσεις μόνο κατόπιν αίτησης από Σύμβουλο URL. Αυτή η ενέργεια έχει οριστεί ως προεπιλογή.
 - Να γίνεται πάντα σάρωση των κρυπτογραφημένων συνδέσεων. Η εφαρμογή σαρώνει πάντα κρυπτογραφημένες συνδέσεις.

- 5. Επιλέξτε την ενέργεια που θέλετε να εκτελείται όταν υπάρχουν σφάλματα κατά τη σάρωση κρυπτογραφημένων συνδέσεων:
 - Παράβλεψη. Αν είναι επιλεγμένη αυτή η ενέργεια, η εφαρμογή τερματίζει τη σύνδεση με τον δικτυακό τόπο στον οποίο παρουσιάστηκε σφάλμα σάρωσης.
 - Ερώτηση. Αν υπάρχει σφάλμα κατά τη σάρωση κρυπτογραφημένης σύνδεσης με έναν δικτυακό τόπο, η εφαρμογή εμφανίζει μια ειδοποίηση από την οποία μπορείτε να επιλέξετε μια ενέργεια:
 - Παράβλεψη. Η εφαρμογή τερματίζει τη σύνδεση με τον δικτυακό τόπο στον οποίο παρουσιάστηκε σφάλμα σάρωσης.
 - Προσθήκη τομέα στις εξαιρέσεις. Η εφαρμογή προσθέτει τη διεύθυνση του δικτυακού τόπου στη λίστα εξαιρέσεων. Η εφαρμογή δεν σαρώνει τις κρυπτογραφημένες συνδέσεις στους δικτυακούς τόπους της λίστας εξαιρέσεων. Αυτές οι τοποθεσίες web εμφανίζονται στο παράθυρο Εξαιρέσεις, το οποίο μπορεί να ανοίξει κάνοντας κλικ στη σύνδεση Διαχείριση εξαιρέσεων.

Αυτή η επιλογή έχει οριστεί ως προεπιλογή.

- Προσθήκη τομέα στις εξαιρέσεις. Η εφαρμογή προσθέτει τον δικτυακό τόπο στη λίστα εξαιρέσεων. Η εφαρμογή δεν σαρώνει τις κρυπτογραφημένες συνδέσεις στους δικτυακούς τόπους της λίστας εξαιρέσεων. Αυτές οι τοποθεσίες web εμφανίζονται στο παράθυρο Εξαιρέσεις, το οποίο μπορεί να ανοίξει κάνοντας κλικ στη σύνδεση Διαχείριση εξαιρέσεων.
- 6. Κάντε κλικ στη σύνδεση **Διαχείριση εξαιρέσεων** για να ανοίξετε το παράθυρο **Εξαιρέσεις** και εκτελέστε τις ακόλουθες ενέργειες:
 - a. Κάντε κλικ στο κουμπί **Προσθήκη** για να προσθέσετε τον δικτυακό τόπο στη λίστα εξαιρέσεων για τη σάρωση κρυπτογραφημένων συνδέσεων.
 - b. Εισαγάγετε το όνομα τομέα του δικτυακού τόπου στο πεδίο Όνομα τομέα.
 - c. Κάντε κλικ στο κουμπί **Προσθήκη**.

Η εφαρμογή δεν θα σαρώνει τις κρυπτογραφημένες συνδέσεις με αυτόν τον δικτυακό τόπο. Σημειώστε ότι η προσθήκη δικτυακού τόπου στη λίστα εξαιρέσεων μπορεί να περιορίσει τη λειτουργικότητα της σάρωσης του δικτυακού τόπου από στοιχεία προστασίας, όπως Ασφαλείς τραπεζικές συναλλαγές, Σύμβουλος URL, Ιδιωτική περιήγηση, Προστασία από ιούς στο Web και Πρόγραμμα Anti-Banner.

Πληροφορίες για την ασφαλή σύνδεση σε δίκτυα Wi-Fi

Το επίπεδο προστασίας των δημόσιων δικτύων Wi-Fi ενδεχομένως να μην είναι επαρκές, για παράδειγμα, εάν ένα δίκτυο Wi-Fi χρησιμοποιεί ένα ευάλωτο πρωτόκολλο κρυπτογράφησης ή έναν αδύναμο κωδικό πρόσβασης. Όταν πραγματοποιείτε αγορές στο Διαδίκτυο μέσω ενός μη ασφαλούς δικτύου Wi-Fi, οι κωδικοί πρόσβασης και άλλα εμπιστευτικά δεδομένα μεταδίδονται σε μορφή μη κρυπτογραφημένου κειμένου. Χάκερ μπορεί να υποκλέψουν τα εμπιστευτικά δεδομένα σας, να βρουν τον αριθμό της τραπεζικής κάρτας σας και να αποκτήσουν πρόσβαση στα χρήματά σας.

Όταν πραγματοποιείται σύνδεση σε δίκτυο Wi-Fi, η εφαρμογή ελέγχει το εν λόγω δίκτυο. Εάν το δίκτυο Wi-Fi δεν είναι ασφαλές, η εφαρμογή σάς προτρέπει να ενεργοποιήσετε την ασφαλή σύνδεση μέσω ενός ειδικά εκχωρημένου διακομιστή ο οποίος βρίσκεται σε περιοχή που καθορίζετε εσείς. Τα δεδομένα του δικτυακού τόπου μεταδίδονται πρώτα στον εκχωρημένο διακομιστή. Στη συνέχεια, η εφαρμογή στέλνει τα δεδομένα στη δική σας συσκευή μέσω μιας κρυπτογραφημένης ασφαλούς σύνδεσης.

Για να χρησιμοποιήσετε το στοιχείο Kaspersky VPN, πρέπει να <u>εκτελέσετε την εφαρμογή</u> <u>Kaspersky VPN Secure Connection</u>. Η εφαρμογή Kaspersky VPN Secure Connection εγκαθίσταται μαζί με το Kaspersky Total Security.

Το στοιχείο Kaspersky VPN προσφέρει τα ακόλουθα πλεονεκτήματα:

- Ασφαλής χρήση συστημάτων πληρωμής και τοποθεσιών κράτησης. Οι εισβολείς δεν θα μπορούν να υποκλέψουν τον αριθμό της τραπεζικής κάρτας σας όταν κάνετε ηλεκτρονικές πληρωμές, κρατήσεις δωματίων σε ξενοδοχεία ή όταν ενοικιάζετε αυτοκίνητα.
- Προστασία των μυστικών πληροφοριών σας. Κανείς δεν θα μπορεί να προσδιορίσει τη διεύθυνση IP του υπολογιστή ή της τοποθεσίας σας.
- Προστασία του ιδιωτικού απορρήτου σας. Κανείς δεν θα μπορεί να υποκλέψει και να διαβάσει την ιδιωτική αλληλογραφία σας σε κοινωνικά δίκτυα.

Το Kaspersky VPN μπορεί επίσης να χρησιμοποιηθεί και για άλλους τύπους συνδέσεων δικτύου, όπως για τοπική σύνδεση στο Διαδίκτυο ή σύνδεση modem USB.

Από προεπιλογή, το Kaspersky VPN Secure Connection δεν σας προτρέπει να ενεργοποιήσετε το VPN, εάν χρησιμοποιείται πρωτόκολλο HTTPS για τη σύνδεση σε δικτυακό τόπο.

Μια αλλαγή της εικονικής τοποθεσίας κατά την επίσκεψη των δικτυακών τόπων τραπεζών, συστημάτων πληρωμής, δικτυακών τόπων κράτησης, κοινωνικών δικτύων, καναλιών συνομιλίας και δικτυακών τόπων email θα μπορούσε να οδηγήσει σε ενεργοποίηση των συστημάτων καταπολέμησης της απάτης (συστήματα που στοχεύουν στην ανάλυση των online οικονομικών συναλλαγών για σημάδια δόλιων ενεργειών). Η χρήση του Kaspersky VPN μπορεί να ρυθμίζεται από την τοπική νομοθεσία. Μπορείτε να χρησιμοποιείτε το Kaspersky VPN μόνο για τον σκοπό για τον οποίο προορίζεται και χωρίς να παραβιάζετε την τοπική νομοθεσία.

Τρόπος εκτέλεσης του Kaspersky VPN Secure Connection

Το Kaspersky VPN Secure Connection εγκαθίσταται μαζί με το Kaspersky Total Security. Μπορείτε να εκκινήσετε το Kaspersky VPN Secure Connection από το μενού **Έναρξη** (στο λειτουργικό σύστημα Microsoft Windows 7 ή σε νεότερη έκδοση), από την οθόνη έναρξης (στο λειτουργικό σύστημα Microsoft Windows 8 ή σε νεότερες εκδόσεις) ή από το παράθυρο του Kaspersky Total Security.

Για εκκίνηση του Kaspersky VPN Secure Connection από το παράθυρο Kaspersky Total Security:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Στο κάτω μέρος του κύριου παραθύρου, κάντε κλικ στο κουμπί Περισσότερα εργαλεία.
 Ανοίγει το παράθυρο Εργαλεία.
- 3. Μεταβείτε στην ενότητα **Το δίκτυό μου**.
- 4. Κάντε κλικ στη σύνδεση **Kaspersky VPN** για να ανοίξει το παράθυρο **Kaspersky VPN**.
- 5. Κάντε κλικ στο κουμπί **Άνοιγμα**.

Αυτό ανοίγει το κύριο παράθυρο της εφαρμογής του Kaspersky VPN Secure Connection.

Περισσότερες λεπτομέρειες σχετικά με τη λειτουργία του Kaspersky VPN Secure Connection <u>διατίθενται στα αρχεία βοήθειας της παρούσας εφαρμογής</u> .

Διαμόρφωση ειδοποιήσεων σχετικά με τα τρωτά σημεία σε δίκτυα Wi-Fi

Εάν το Kaspersky VPN Secure Connection δεν είναι εγκατεστημένο στον υπολογιστή σας, το Kaspersky Total Security εμφανίζει μια ειδοποίηση σχετικά με τη σύνδεση σε δίκτυα Wi-Fi και τη μη ασφαλή μετάδοση του κωδικού πρόσβασής σας μέσω του Διαδικτύου. Μπορείτε να επιτρέψετε ή να αποκλείσετε τη σύνδεση και τη μετάδοση κωδικών πρόσβασης στο παράθυρο ειδοποιήσεων.

Μετά την εγκατάσταση του Kaspersky VPN Secure Connection, οι ρυθμίσεις για την εμφάνιση ειδοποιήσεων κατά τη σύνδεση σε δίκτυα Wi-Fi και τη μετάδοση μη κρυπτογραφημένων κωδικών πρόσβασης καθίστανται ανενεργές. Μπορείτε να διαμορφώσετε τις ρυθμίσεις ειδοποίησης για συνδέσεις σε δίκτυα Wi-Fi στο <u>Kaspersky VPN Secure Connection</u> 2.

Για να διαμορφώσετε τις ειδοποιήσεις σχετικά με τα τρωτά σημεία των δικτύων Wi-Fi:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.
- 4. Επιλέξτε το στοιχείο του Τείχους προστασίας.

Το παράθυρο εμφανίζει τις ρυθμίσεις του στοιχείου Τείχους προστασίας.

- 5. Επιλέξτε το Να εμφανίζονται ειδοποιήσεις για τρωτά σημεία στα δίκτυα Wi-Fi εάν θέλετε να λαμβάνετε ειδοποιήσεις όταν συνδέεστε σε ευάλωτα δίκτυα Wi-Fi. Εάν δεν θέλετε να λαμβάνετε ειδοποιήσεις, αποεπιλέξτε το πλαίσιο ελέγχου. Η πρόσβαση σε αυτό το πλαίσιο ελέγχου είναι δυνατή αν το Kaspersky VPN Secure Connection δεν είναι εγκατεστημένο στον υπολογιστή.
- 6. Εάν είναι επιλεγμένο το πλαίσιο ελέγχου **Να εμφανίζονται ειδοποιήσεις για τρωτά σημεία στα δίκτυα Wi-Fi**, μπορείτε να επεξεργαστείτε τις ρυθμίσεις για προχωρημένους για την εμφάνιση των ειδοποιήσεων:
 - Επιλέξτε το πλαίσιο ελέγχου Να εμποδίζεται η μετάδοση και να εμφανίζεται ειδοποίηση σε περίπτωση μη ασφαλούς μετάδοσης κωδικών πρόσβασης μέσω του Διαδικτύου για να αποκλειστούν όλες οι μεταδόσεις κωδικών πρόσβασης σε μορφή μη κρυπτογραφημένου κειμένου όταν συμπληρώνετε τα πεδία Κωδικός πρόσβασης στο Διαδίκτυο.
 - Κάντε κλικ στη σύνδεση Ενεργοποίηση για να επαναφέρετε τις προεπιλεγμένες τιμές των ρυθμίσεων όσον αφορά την εμφάνιση των ειδοποιήσεων σχετικά με τη μετάδοση κωδικών πρόσβασης σε μη κρυπτογραφημένη μορφή. Εάν είχατε απενεργοποιήσει προηγουμένως την εμφάνιση ειδοποιήσεων σχετικά με τη μετάδοση κωδικών

πρόσβασης σε μη κρυπτογραφημένη μορφή, η εμφάνιση αυτών των ειδοποιήσεων θα ενεργοποιηθεί εκ νέου.

Προστασία οικονομικών συναλλαγών και διαδικτυακών αγορών

Αυτή η ενότητα παρέχει πληροφορίες για το πώς να προστατεύετε τις οικονομικές συναλλαγές και online αγορές σας με το Kaspersky Total Security.

Πληροφορίες για την προστασία οικονομικών συναλλαγών και διαδικτυακών αγορών

Για την προστασία των εμπιστευτικών δεδομένων που πληκτρολογείτε σε δικτυακούς τόπους τραπεζών και συστημάτων πληρωμών (όπως αριθμοί τραπεζικών καρτών και κωδικοί πρόσβασης σε τραπεζικές συναλλαγές στο Διαδίκτυο), καθώς και για την πρόληψη πιθανής κλοπής χρημάτων όταν κάνετε ηλεκτρονικές πληρωμές, το Kaspersky Total Security σας ζητά να ανοίγετε τέτοιους δικτυακούς τόπους στο Προστατευμένο πρόγραμμα περιήγησης.

Το *Προστατευμένο πρόγραμμα περιήγησης* είναι μια ειδική λειτουργία του προγράμματος περιήγησης για την προστασία των δεδομένων σας όταν επισκέπτεστε δικτυακούς τόπους τραπεζών ή συστημάτων πληρωμών. Το Προστατευμένο πρόγραμμα περιήγησης εκκινείται σε απομονωμένο περιβάλλον για την αποτροπή της έγχυσης κώδικα από άλλες εφαρμογές στη διεργασία του Προστατευμένου προγράμματος περιήγησης. Το Kaspersky Total Security δημιουργεί ειδικά προφίλ για τα προγράμματα περιήγησης Mozilla Firefox και Google Chrome ούτως ώστε τα πρόσθετα τρίτων να μην μπορούν να επηρεάσουν τη λειτουργία του Προστατευμένου προγράμματος περιήγησης. Η εφαρμογή δεν επηρεάζει τα δεδομένα που μπορεί να αποθηκεύουν τα προγράμματα περιήγησης στα προφίλ που έχουν δημιουργηθεί για αυτά.

Εάν χρησιμοποιείτε Microsoft Edge που βασίζεται στο Chromium, Google Chrome, Mozilla Firefox ή Internet Explorer, το Προστατευμένο πρόγραμμα περιήγησης ανοίγει σε ένα καινούριο παράθυρο.

Η εφαρμογή χρησιμοποιεί την <u>επέκταση Kaspersky Protection</u> για να παρέχει ένα πλήθος λειτουργιών του Προστατευμένου προγράμματος περιήγησης.

Τα προγράμματα περιήγησης που δεν πληρούν τις <u>απαιτήσεις λογισμικού</u> δεν μπορούν να εκτελεστούν στη λειτουργία Προστατευμένου προγράμματος περιήγησης. Αντί για τέτοια προγράμματα περιήγησης, είτε ο Microsoft Edge που βασίζεται στο Chromium είτε ένα άλλο πρόγραμμα περιήγησης που έχει διαμορφωθεί στις ρυθμίσεις της εφαρμογής εκκινείται στη λειτουργία Προστατευμένου προγράμματος περιήγησης. Είναι αδύνατο να εκτελεστεί Προστατευμένο πρόγραμμα περιήγησης υπό τις ακόλουθες συνθήκες:

- Το πλαίσιο ελέγχου έχει αποεπιλεγεί στην υποενότητα Ενεργοποίηση Αυτοάμυνας της ενότητας Γενικά του παραθύρου ρυθμίσεων εφαρμογής.
- Το Javascript είναι απενεργοποιημένο στο πρόγραμμα περιήγησης.

Εκτέλεση Προστατευμένου προγράμματος περιήγησης στο Yandex Browser

Το Kaspersky Total Security υποστηρίζει την προστασία των οικονομικών συναλλαγών σας στο Yandex Browser με ορισμένους περιορισμούς. Για την εκτέλεση του Προστατευμένου προγράμματος περιήγησης, η εφαρμογή προσθέτει μια ειδική δέσμη ενεργειών στην ιστοσελίδα (και στην κίνηση). Η επέκταση Kaspersky Protection δεν είναι διαθέσιμη. Τα στοιχεία Ιδιωτική περιήγηση και Πρόγραμμα Anti-Banner λειτουργούν, αλλά δεν είναι δυνατό να ρυθμιστούν οι παράμετροί τους στο Yandex Browser.

Ιδιότητες του Προστατευμένου προγράμματος περιήγησης

Στη λειτουργία Προστατευμένου προγράμματος περιήγησης, η εφαρμογή παρέχει προστασία ενάντια στους εξής τύπους απειλών:

- Μη αξιόπιστες λειτουργικές μονάδες. Η εφαρμογή εκτελεί έλεγχο για μη αξιόπιστες λειτουργικές μονάδες κάθε φορά που επισκέπτεστε έναν δικτυακό τόπο τράπεζας ή συστήματος πληρωμών.
- Rootkit. Η εφαρμογή εκτελεί σάρωση για rootkit κατά την εκκίνηση του Προστατευμένου προγράμματος περιήγησης.
- Μη έγκυρα πιστοποιητικά των δικτυακών τόπων τραπεζών ή συστημάτων πληρωμών. Η εφαρμογή ελέγχει τα πιστοποιητικά όταν επισκέπτεστε έναν δικτυακό τόπο τράπεζας ή συστήματος πληρωμών. Ο έλεγχος εκτελείται με τη βοήθεια μιας βάσης δεδομένων μη έγκυρων πιστοποιητικών.

Κατάσταση του Προστατευμένου προγράμματος περιήγησης

Όταν ανοίγετε έναν δικτυακό τόπο στο Προστατευμένο πρόγραμμα περιήγησης, εμφανίζεται ένα πλαίσιο στο περίγραμμα του παραθύρου του προγράμματος περιήγησης. Το χρώμα του πλαισίου υποδεικνύει την κατάσταση προστασίας. Το πλαίσιο του παραθύρου του προγράμματος περιήγησης μπορεί να εμφανίσει τις εξής χρωματικές ενδείξεις:

- Πράσινο πλαίσιο. Υποδεικνύει ότι όλοι οι έλεγχοι έχουν εκτελεστεί με επιτυχία. Μπορείτε να συνεχίσετε να χρησιμοποιείτε το Προστατευμένο πρόγραμμα περιήγησης.
- Κίτρινο πλαίσιο. Υποδεικνύει ότι οι έλεγχοι αποκάλυψαν προβλήματα ασφάλειας που πρέπει να επιλυθούν.

Η εφαρμογή μπορεί να εντοπίσει τις εξής απειλές και προβλήματα ασφάλειας:

- Μη αξιόπιστη μονάδα. Απαιτείται σάρωση και απολύμανση του υπολογιστή.
- Rootkit. Απαιτείται σάρωση και απολύμανση του υπολογιστή.
- Μη έγκυρο πιστοποιητικό δικτυακού τόπου τράπεζας ή συστήματος πληρωμών.

Εάν δεν εξαλείψετε τις απειλές που εντοπίστηκαν, η ασφάλεια της περιόδου λειτουργίας σύνδεσης στον δικτυακό τόπο της τράπεζας ή του συστήματος πληρωμών δεν είναι εγγυημένη. Συμβάντα που περιλαμβάνουν την εκκίνηση και χρήση του Προστατευμένου προγράμματος περιήγησης με μειωμένη προστασία, καταγράφονται στο μητρώο καταγραφής συμβάντων των Windows.

Σχετικά με την προστασία ενάντια στα στιγμιότυπα οθόνης

Για να προστατεύσετε τα δεδομένα σας όταν περιηγείστε σε προστατευμένους δικτυακούς τόπους, το Kaspersky Total Security αποτρέπει τη λήψη μη εξουσιοδοτημένων στιγμιοτύπων οθόνης από λογισμικά υποκλοπής. Η προστασία ενάντια στα στιγμιότυπα οθόνης είναι ενεργοποιημένη εκ προεπιλογής. Η προστασία από στιγμιότυπα εκτελείται ακόμα και εάν έχει απενεργοποιηθεί η <u>εικονικοποίηση υλικού</u>.

Σχετικά με την προστασία δεδομένων προχείρου

Το Kaspersky Total Security αποκλείει τη μη εξουσιοδοτημένη πρόσβαση των εφαρμογών στο πρόχειρο όταν πραγματοποιείτε ηλεκτρονικές πληρωμές, αποτρέποντας έτσι την κλοπή των δεδομένων σας από εγκληματίες. Ο αποκλεισμός αυτός ενεργοποιείται μόνο αν μια μη αξιόπιστη εφαρμογή επιχειρήσει να αποκτήσει μη εξουσιοδοτημένη πρόσβαση στο πρόχειρό σας. Εάν αντιγράψετε χειροκίνητα τα δεδομένα από το παράθυρο μιας εφαρμογής στο παράθυρο μιας άλλης εφαρμογής (για παράδειγμα, από το Σημειωματάριο στο παράθυρο προγράμματος επεξεργασίας κειμένου), η πρόσβαση στο πρόχειρο θα επιτραπεί.
Η προστασία προχείρου δεν εκτελείται εάν είναι απενεργοποιημένη <u>εικονικοποίηση υλικού</u> στον υπολογιστή σας.

Εάν εκκινηθεί το Προστατευμένο πρόγραμμα περιήγησης στο λειτουργικό σύστημα των Microsoft Windows 10, το Kaspersky Total Security θα αποκλείσει την αλληλεπίδραση των καθολικών εφαρμογών των Windows με το Πρόχειρο.

Τρόπος αλλαγής των ρυθμίσεων των Ασφαλών τραπεζικών συναλλαγών

Για να ρυθμίσετε τις παραμέτρους της λειτουργίας Ασφαλείς τραπεζικές συναλλαγές:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.
- 4. Επιλέξτε το στοιχείο **Ασφαλείς τραπεζικές συναλλαγές**.

Το παράθυρο εμφανίζει τις ρυθμίσεις του στοιχείου Ασφαλών τραπεζικών συναλλαγών.

- 5. Για να ενεργοποιήσετε τη λειτουργία Ασφαλείς τραπεζικές συναλλαγές, χρησιμοποιήστε το διακόπτη στο επάνω μέρος του παραθύρου.
- 6. Στην ενότητα Κατά την πρώτη πρόσβαση σε τοποθεσίες web τραπεζών και συστημάτων πληρωμής, επιλέξτε την ενέργεια που θέλετε να εκτελέσει η εφαρμογή την πρώτη φορά που θα ανοίξετε τον δικτυακό τόπο μιας τράπεζας ή ενός συστήματος πληρωμής στο δικό σας πρόγραμμα περιήγησης σας:
 - Επιλέξτε Εκτέλεση προστατευμένου προγράμματος περιήγησης εάν επιθυμείτε η εφαρμογή να ανοίγει τον δικτυακό τόπο στο Προστατευμένο πρόγραμμα περιήγησης.
 - Επιλέξτε Προτροπή χρήστη εάν θέλετε η εφαρμογή να σας ρωτάει εάν επιθυμείτε να ανοίγετε ή όχι τον δικτυακό τόπο στο Προστατευμένο πρόγραμμα περιήγησης όταν επισκέπτεστε τον δικτυακό τόπο.
 - Επιλέξτε Να μην εκτελείται το Προστατευμένο πρόγραμμα περιήγησης εάν επιθυμείτε η εφαρμογή να μην ανοίγει τον δικτυακό τόπο στο Προστατευμένο πρόγραμμα περιήγησης.

7. Στην ενότητα Πρόσθετα, ανοίξτε την αναπτυσσόμενη λίστα Για μετάβαση σε τοποθεσίες web από το παράθυρο της λειτουργίας Ασφαλείς τραπεζικές συναλλαγές, να χρησιμοποιηθεί και επιλέξτε το πρόγραμμα περιήγησης που θα εκτελεί η εφαρμογή στη λειτουργία Προστατευμένου προγράμματος περιήγησης όταν επισκέπτεστε τον δικτυακό τόπο μιας τράπεζας ή ενός συστήματος πληρωμής από το παράθυρο Ασφαλείς τραπεζικές συναλλαγές.

Μπορείτε να επιλέξετε ένα από τα προγράμματα περιήγησης που είναι εγκατεστημένα στον υπολογιστή σας ή να χρησιμοποιήσετε το προεπιλεγμένο πρόγραμμα περιήγησης του λειτουργικού συστήματος.

Πώς να ρυθμίσετε τις παραμέτρους της λειτουργίας Ασφαλείς τραπεζικές συναλλαγές για έναν συγκεκριμένο δικτυακό τόπο

Για να ρυθμίσετε τις παραμέτρους της λειτουργίας Ασφαλείς τραπεζικές συναλλαγές για έναν συγκεκριμένο δικτυακό τόπο:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Ασφαλείς τραπεζικές συναλλαγές**.

Ανοίγει το παράθυρο **Ασφαλείς τραπεζικές συναλλαγές**. Εάν ανοίγετε το παράθυρο για πρώτη φορά, το Kaspersky Total Security θα σας προσφέρει τη δυνατότητα να δείτε πώς λειτουργούν οι Ασφαλείς τραπεζικές συναλλαγές. Μπορείτε να παραλείψετε αυτήν την ενημερωτική περιήγηση.

- 3. Κάντε κλικ στη σύνδεση **Προσθήκη τοποθεσίας web στις Ασφαλείς τραπεζικές συναλλαγές** για να ανοίξετε τα πεδία προσθήκης τοποθεσίας web.
- 4. Στο πεδίο Τοποθεσία web για Ασφαλείς τραπεζικές συναλλαγές, πληκτρολογήστε τη διεύθυνση URL ενός δικτυακού τόπου ο οποίος θέλετε να ανοίγει σε Προστατευμένο πρόγραμμα περιήγησης.

Η διεύθυνση web του δικτυακού τόπου πρέπει να ξεκινά με το πρόθεμα του πρωτοκόλλου HTTPS (για παράδειγμα, https://example.com), το οποίο χρησιμοποιείται ως προεπιλογή από το προστατευμένο πρόγραμμα περιήγησης.

- 5. Επιλέξτε την ενέργεια που θέλετε να πραγματοποιεί το Προστατευμένο πρόγραμμα περιήγησης όταν ανοίγετε τον δικτυακό τόπο:
 - Εάν θέλετε ο δικτυακός τόπος να ανοίγει σε Προστατευμένο πρόγραμμα περιήγησης κάθε φορά που τον επισκέπτεστε, επιλέξτε Εκτέλεση προστατευμένου

προγράμματος περιήγησης.

- Εάν θέλετε το Kaspersky Total Security να σας ειδοποιεί για την επιθυμητή ενέργεια όταν ανοίγει ο δικτυακός τόπος, επιλέξτε Προτροπή χρήστη.
- Εάν θέλετε να απενεργοποιήσετε τη λειτουργία Ασφαλείς τραπεζικές συναλλαγές για τον δικτυακό τόπο, επιλέξτε Να μην εκτελείται το Προστατευμένο πρόγραμμα περιήγησης.
- 6. Κάντε κλικ στη σύνδεση **Προσθήκη περιγραφής** για να ανοίξετε το πεδίο **Περιγραφή** και να εισαγάγετε το όνομα ή την περιγραφή αυτού του δικτυακού τόπου.
- 7. Κάντε κλικ στο κουμπί **Προσθήκη**.

Η τοποθεσία web θα εμφανίζεται στη λίστα.

Τρόπος αποστολής σχολίων σχετικά με Ασφαλείς τραπεζικές συναλλαγές

Μπορείτε να στείλετε στην Kaspersky τα σχόλιά σας για τη λειτουργία του στοιχείου Ασφαλείς τραπεζικές συναλλαγές ή να υποβάλετε αναφορά για πρόβλημα στο στοιχείο αυτό.

<u>Πώς να στείλετε σχόλια</u> 🖓

Για να αποστείλετε σχόλια σχετικά με τη λειτουργία του στοιχείου Ασφαλείς τραπεζικές συναλλαγές:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Ασφαλείς τραπεζικές συναλλαγές**.

Ανοίγει το παράθυρο **Ασφαλείς τραπεζικές συναλλαγές**. Εάν ανοίγετε το παράθυρο για πρώτη φορά, το Kaspersky Total Security θα σας προσφέρει τη δυνατότητα να δείτε πώς λειτουργούν οι Ασφαλείς τραπεζικές συναλλαγές. Μπορείτε να παραλείψετε αυτήν την ενημερωτική περιήγηση.

- Κάντε κλικ στη σύνδεση Αποστολή σχολίων για να ανοίξετε ένα παράθυρο στο οποίο μπορείτε να αφήσετε σχόλια σχετικά με την απόδοση του στοιχείου Ασφαλείς τραπεζικές συναλλαγές.
- 4. Βαθμολογήστε τις Ασφαλείς τραπεζικές συναλλαγές σε κλίμακα 5 επιπέδων επιλέγοντας από 1 έως 5 αστέρια.

- 5. Εάν θέλετε να προσθέσετε κάτι στα σχόλιά σας, εισάγετε το κείμενο στο πεδίο **Λεπτομέρειες**.
- 6. Κάντε κλικ στο κουμπί **Αποστολή**.

Πώς να αναφέρετε ένα πρόβλημα 🖓

Για να υποβάλετε αναφορά σχετικά με πρόβλημα στο Προστατευμένο πρόγραμμα περιήγησης:

 Κάντε κλικ στη σύνδεση Αναφορά προβλήματος του αναδυόμενου παραθύρου Προστατευμένο πρόγραμμα περιήγησης του Kaspersky Total Security στο κάτω μέρος του Προστατευμένου προγράμματος περιήγησης.

Το παράθυρο που ανοίγει σας επιτρέπει να αναφέρετε ένα πρόβλημα με Ασφαλείς τραπεζικές συναλλαγές.

- Στην αναπτυσσόμενη λίστα Πρόβλημα, επιλέξτε το στοιχείο που περιγράφει με μεγαλύτερη ακρίβεια το πρόβλημά σας:
 - Δεν το χρησιμοποιώ. Επιλέξτε αυτό το στοιχείο εάν δεν χρησιμοποιείτε
 Ασφαλείς τραπεζικές συναλλαγές ή εάν αποφασίσατε να αρνηθείτε τη χρήση
 Ασφαλών τραπεζικών συναλλαγών.
 - Η τοποθεσία web ανοίγει αργά. Επιλέξτε αυτό το στοιχείο εάν ο δικτυακός τόπος χρειάζεται περισσότερο χρόνο για να ανοίξει από ό,τι σε ένα κανονικό πρόγραμμα περιήγησης.
 - Το Προστατευμένο πρόγραμμα περιήγησης εκκινείται όταν δεν χρειάζεται.
 Επιλέξτε αυτό το στοιχείο εάν ανοίγουν δικτυακοί τόποι που δεν απαιτούν τη χρήση των Ασφαλών τραπεζικών συναλλαγών στο Προστατευμένο πρόγραμμα περιήγησης.
 - Ο έλεγχος ταυτότητας της τοποθεσίας web αποτυχαίνει. Επιλέξτε αυτό το στοιχείο εάν προκύπτουν σφάλματα κατά την προσπάθεια εξουσιοδότησης σε δικτυακό τόπο που ανοίχτηκε στο Προστατευμένο πρόγραμμα περιήγησης.
 - Η τοποθεσία web δεν εμφανίζεται σωστά ή δεν ανοίγει. Επιλέξτε αυτό το στοιχείο εάν οι δικτυακοί τόποι δεν ανοίγουν στο Προστατευμένο πρόγραμμα περιήγησης ή εάν εμφανίζονται με σφάλματα ή στρεβλώσεις.
 - **Σφάλματα επαλήθευσης του πιστοποιητικού τοποθεσίας web**. Επιλέξτε αυτό το στοιχείο εάν εμφανίζονται μηνύματα σφάλματος κατά την επικύρωση

των πιστοποιητικών δικτυακών τόπων.

- Δεν είναι δυνατή η λήψη στιγμιότυπου οθόνης όταν εκτελείται το
 Προστατευμένο πρόγραμμα περιήγησης. Επιλέξτε αυτό το στοιχείο εάν δεν δημιουργούνται στιγμιότυπα στο Προστατευμένο πρόγραμμα περιήγησης.
- Σφάλματα κατά την εισαγωγή δεδομένων μέσω πληκτρολογίου ή από το Πρόχειρο. Επιλέξτε αυτό το στοιχείο εάν προκύπτουν σφάλματα κατά την καταχώρηση δεδομένων στο Προστατευμένο πρόγραμμα περιήγησης.
- Δεν γίνεται εκτύπωση ιστοσελίδας που είναι ανοιχτή στο Προστατευμένο πρόγραμμα περιήγησης. Επιλέξτε αυτό το στοιχείο εάν δεν μπορείτε να εκτυπώσετε μια ανοικτή σελίδα ενός δικτυακού τόπου.
- Εμφανίζεται ένα μήνυμα που προειδοποιεί ότι δεν είναι εγκατεστημένες σημαντικές ενημερώσεις του λειτουργικού συστήματος. Επιλέξτε αυτό το στοιχείο εάν εμφανίζεται το μήνυμα "Δεν έχουν εγκατασταθεί κρίσιμες ενημερώσεις συστήματος" όταν εκτελείται το Προστατευμένο πρόγραμμα περιήγησης.
- Άλλο ένα πρόγραμμα περιήγησης εκτελείται ως Προστατευμένο πρόγραμμα περιήγησης. Επιλέξτε αυτό το στοιχείο εάν έχει ανοιχθεί πρόγραμμα περιήγησης σε προστατευμένη λειτουργία διαφορετικό από αυτό στο οποίο ξεκινήσατε.
- Σφάλματα λειτουργίας. Επιλέξτε αυτό το στοιχείο εάν το Προστατευμένο πρόγραμμα περιήγησης επέστρεψε σφάλμα.
- Άλλο. Επιλέξτε αυτό το στοιχείο εάν αντιμετωπίζετε προβλήματα που δεν καλύπτονται από τα άλλα στοιχεία.
- Για να στείλετε πρόσθετες πληροφορίες για το πρόβλημά σας στην Kaspersky, εισαγάγετε μια περιγραφή του στο πεδίο κειμένου Λεπτομέρειες.
- 4. Κάντε κλικ στο κουμπί **Αποστολή**.

Εάν η εφαρμογή αποτύχει να στείλει τα σχόλιά σας (για παράδειγμα, δεν είναι διαθέσιμη η σύνδεση στο Διαδίκτυο), αυτά τα σχόλια θα αποθηκευτούν στον υπολογιστή σας. Τα σχόλια αποθηκεύονται φανερά για 30 ημέρες.

Μπορείτε να στέλνετε σχόλια σχετικά με τη λειτουργία του στοιχείου Ασφαλείς τραπεζικές συναλλαγές έως και 10 φορές την ημέρα.

Μπορείτε, επίσης, να στείλετε σχόλια μετά την απενεργοποίηση του στοιχείου Ασφαλείς τραπεζικές συναλλαγές. Μετά την απενεργοποίηση του στοιχείου, μπορείτε να στέλνετε σχόλια μία φορά το μήνα.

Έναρξη του Kaspersky Password Manager

To Kaspersky Password Manager είναι σχεδιασμένο για την ασφαλή αποθήκευση και τον συγχρονισμό των κωδικών πρόσβασης στις συσκευές σας. Το Kaspersky Password Manager πρέπει να εγκατασταθεί ανεξάρτητα από το Kaspersky Total Security. Για παράδειγμα, μπορείτε να χρησιμοποιήσετε τη συντόμευση **Κωδικοί πρόσβασης Kaspersky** που δημιουργήθηκε στην επιφάνεια εργασίας του υπολογιστή σας κατά την εγκατάσταση του Kaspersky Total Security.

Μετά την εγκατάσταση, μπορείτε να ξεκινήσετε το Kaspersky Password Manager από το μενού **Έναρξη** (στα Microsoft Windows 7 ή Microsoft Windows 10), από την οθόνη έναρξης (στα Microsoft Windows 8 ή Microsoft Windows 8.1) ή από το παράθυρο του Kaspersky Total Security.

<u>Πώς να ξεκινήσετε το Kaspersky Password Manager από το παράθυρο του Kaspersky Total</u> <u>Security</u> 🔋

Για να ξεκινήσετε το Kaspersky Password Manager που είναι ήδη εγκατεστημένο:

- 1. Ανοίξτε το κύριο παράθυρο του Kaspersky Total Security.
- 2. Κάντε κλικ στο κουμπί **Διαχείριση κωδικών πρόσβασης**.
- 3. Στο παράθυρο, κάντε κλικ στο κουμπί **Εκτέλεση**.

Ανοίγει το παράθυρο Kaspersky Password Manager.

<u>Πώς να κάνετε λήψη και εγκατάσταση του Kaspersky Password Manager</u> 🕑

Για να κάνετε λήψη και εγκατάσταση του Kaspersky Password Manager, και να προστατέψετε τους κωδικούς πρόσβασής σας,

εκτελέστε μία από τις ακόλουθες ενέργειες:

 Κάντε κλικ στο κουμπί Διαχείριση κωδικών πρόσβασης στο κύριο παράθυρο του Kaspersky Total Security. Κάντε κλικ στο κουμπί Μάθετε περισσότερα στο παράθυρο Κέντρο ειδοποιήσεων στην ενότητα Συστάσεις δίπλα στην προτροπή να εγκαταστήσετε το Kaspersky Password Manager.

Το Kaspersky Total Security θα προχωρήσει τη λήψη του πακέτου εγκατάστασης του Kaspersky Password Manager θα εγκαταστήσει την εφαρμογή στον υπολογιστή σας.

Το πακέτο εγκατάστασης του Kaspersky Password Manager που έχετε λάβει, παραμένει στον υπολογιστή σας ανεξαρτήτως εάν έχει χρησιμοποιηθεί ή όχι για την εγκατάσταση του Kaspersky Password Manager.

Ανατρέξτε στη *<u>Βοήθεια του Kaspersky Password Manager</u>* για οδηγίες σχετικά με τη χρήση του Kaspersky Password Manager.

Προστασία παρακολούθησης στο web

Η ενότητα αυτή παρέχει πληροφορίες για τον τρόπο με τον οποίο το Kaspersky Total Security μπορεί να σας προστατεύσει ενάντια στην παρακολούθηση της online δραστηριότητάς σας.

Πληροφορίες σχετικά με την Ιδιωτική περιήγηση

Ορισμένες τοποθεσίες web χρησιμοποιούν υπηρεσίες παρακολούθησης για τη συλλογή πληροφοριών σχετικά με τις δραστηριότητές σας στο Διαδίκτυο. Στη συνέχεια, αυτές οι πληροφορίες αναλύονται και χρησιμοποιούνται με σκοπό την εμφάνιση διαφημίσεων.

Το στοιχείο *Ιδιωτική περιήγηση* έχει σχεδιαστεί ώστε να αποτρέπει τη συλλογή πληροφοριών για την online δραστηριότητά σας.

Στη *λειτουργία εντοπισμού*, το στοιχείο Ιδιωτική περιήγηση εντοπίζει και καταμετράει τις προσπάθειες συλλογής δεδομένων και καταγράφει αυτές τις πληροφορίες σε μια <u>αναφορά</u>. Η λειτουργία εντοπισμού είναι ενεργοποιημένη από προεπιλογή, ενώ η συλλογή δεδομένων <u>επιτρέπεται σε όλους τους δικτυακούς τόπους</u>.

Στη *λειτουργία αποκλεισμού*, το στοιχείο Ιδιωτική περιήγηση εντοπίζει και αποκλείει τις προσπάθειες συλλογής δεδομένων και οι πληροφορίες σχετικά με αυτές τις προσπάθειες καταγράφονται σε μια <u>αναφορά</u>. Σε αυτήν τη λειτουργία, η συλλογή δεδομένων αποκλείεται σε όλους τους δικτυακούς τόπους με εξαίρεση των εξής:

• δικτυακοί τόποι που <u>έχουν προστεθεί στις εξαιρέσεις</u>

- Τοποθεσίες web της Kaspersky και των συνεργατών της
- δικτυακοί τόποι που μπορεί να καταστούν μη λειτουργικοί ως αποτέλεσμα του αποκλεισμού των υπηρεσιών παρακολούθησης, σύμφωνα με τις πληροφορίες που είναι στη διάθεση της Kaspersky

Ο μετρητής αποκλεισμένων αποπειρών συλλογής δεδομένων εμφανίζει τον συνολικό αριθμό αποκλεισμών σε ολόκληρη την τοποθεσία ανάλογα με το πόσες ιστοσελίδες είναι ανοικτές στο πρόγραμμα περιήγησης. Αν μία σελίδα είναι ανοικτή στο πρόγραμμα περιήγησης, μετριούνται μόνο οι αποκλεισμένες απόπειρες συλλογής δεδομένων σε αυτή τη σελίδα. Αν στο πρόγραμμα περιήγησης είναι ανοικτές διάφορες σελίδες της ίδιας τοποθεσίας, μετριούνται οι αποκλεισμένες απόπειρες συλλογής δεδομένων σε όλες τις σελίδες της τοποθεσίας που έχουν ανοιχτεί στο πρόγραμμα περιήγησης.

Μπορείτε να διαχειριστείτε το στοιχείο Ιδιωτική περιήγηση μέσω του περιβάλλοντος εργασίας του Kaspersky Total Security ή με τη βοήθεια της επέκτασης Kaspersky Protection στο δικό σας <u>πρόγραμμα περιήγησης</u>.

Η Ιδιωτική περιήγηση έχει τους εξής περιορισμούς:

- Η εφαρμογή δεν αποκλείει τη συλλογή δεδομένων από υπηρεσίες παρακολούθησης της κατηγορίας "Μέσα κοινωνικής δικτύωσης" όταν βρίσκεστε στον δικτυακό τόπο του αντίστοιχου κοινωνικού δικτύου.
- Εάν ο δικτυακός τόπος από τον οποίο προήλθε η προσπάθεια συλλογής δεδομένων δεν ήταν δυνατόν να προσδιοριστεί, το Kaspersky Total Security δεν αποκλείει τη συγκεκριμένη προσπάθεια συλλογής δεδομένων και δεν εμφανίζει πληροφορίες για αυτήν.
- Εάν ο δικτυακός τόπος από τον οποίο προήλθε προσπάθεια συλλογής δεδομένων ήταν δυνατόν να προσδιοριστεί, αλλά δεν μπορεί αντιστοιχιστεί με κάποιον από τους δικτυακούς τόπους που είναι ανοιχτοί τη δεδομένη στιγμή στο πρόγραμμα περιήγησης, το Kaspersky Total Security εφαρμόζει την ενέργεια που έχει καθοριστεί στις ρυθμίσεις της Ιδιωτικής περιήγησης (αποκλείει ή επιτρέπει τη συλλογή δεδομένων). Η εφαρμογή εμφανίζει πληροφορίες σχετικά με την προσπάθεια συλλογής δεδομένων σε αναφορές, αλλά δεν περιλαμβάνει αυτές τις πληροφορίες στα στατιστικά στοιχεία Ιδιωτικής περιήγησης που εμφανίζονται στο πρόγραμμα περιήγησης.

Αποκλεισμός συλλογής δεδομένων

Για να αποκλειστεί η συλλογή δεδομένων:

1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.

- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Στην ενότητα **Προστασία**, επιλέξτε το στοιχείο Ιδιωτική περιήγηση.

Ανοίγει το παράθυρο **Ρυθμίσεις της Ιδιωτικής περιήγησης**.

- 4. Εάν το στοιχείο είναι απενεργοποιημένο, ενεργοποιήστε το ρυθμίζοντας τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου σε **Ενεργό**.
- 5. Επιλέξτε **Να αποκλειστεί η συλλογή δεδομένων**.

Το Kaspersky Total Security θα αποκλείσει τις προσπάθειες συλλογής δεδομένων σε όλους τους δικτυακούς τόπους εκτός από τις <u>εξαιρέσεις</u>.

- 6. Εάν θέλετε να αποκλειστεί ή να επιτραπεί η συλλογή δεδομένων με βάση τις κατηγορίες των υπηρεσιών παρακολούθησης:
 - a. Κάντε κλικ στη σύνδεση **Κατηγορίες και εξαιρέσεις** για να ανοίξετε το παράθυρο **Κατηγορίες και εξαιρέσεις**.
 - b. Από προεπιλογή, η συλλογή δεδομένων είναι αποκλεισμένη για όλες τις κατηγορίες των υπηρεσιών παρακολούθησης και όλα τα κοινωνικά δίκτυα. Αποεπιλέξτε τα πλαίσια ελέγχου απέναντι από τις κατηγορίες των υπηρεσιών παρακολούθησης και τα κοινωνικά δίκτυα για τα οποία θέλετε να επιτραπεί η συλλογή δεδομένων.

Να επιτρέπεται η συλλογή δεδομένων σε όλους τους δικτυακούς τόπους

Για να επιτρέψετε τη συλλογή δεδομένων σε όλους τους δικτυακούς τόπους:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- Στην ενότητα Προστασία, επιλέξτε το στοιχείο Ιδιωτική περιήγηση.
 Ανοίγει το παράθυρο Ρυθμίσεις της Ιδιωτικής περιήγησης.
- 4. Εάν το στοιχείο είναι απενεργοποιημένο, ενεργοποιήστε το ρυθμίζοντας τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου σε **Ενεργό**.
- 5. Επιλέξτε το στοιχείο **Μόνο συλλογή στατιστικών στοιχείων**.

To Kaspersky Total Security εντοπίζει και καταμετρά τις προσπάθειες παρακολούθησης της online δραστηριότητάς σας χωρίς να τις αποκλείει. Μπορείτε να δείτε τα αποτελέσματα της λειτουργίας του στοιχείου στην <u>αναφορά</u>.

Να επιτραπεί η συλλογή δεδομένων ως εξαίρεση

Μπορείτε να επιτρέψετε την παρακολούθηση της δραστηριότητάς σας σε καθορισμένους δικτυακούς τόπους ως εξαίρεση.

Για να επιτρέψετε τη συλλογή δεδομένων ως εξαίρεση:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Στην ενότητα **Προστασία**, επιλέξτε το στοιχείο Ιδιωτική περιήγηση.

Ανοίγει το παράθυρο **Ρυθμίσεις της Ιδιωτικής περιήγησης**.

- 4. Εάν το στοιχείο είναι απενεργοποιημένο, ενεργοποιήστε το ρυθμίζοντας τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου σε **Ενεργό**.
- 5. Επιλέξτε **Να αποκλειστεί η συλλογή δεδομένων**.

Το Kaspersky Total Security θα αποκλείσει τις προσπάθειες συλλογής δεδομένων σε όλους τους δικτυακούς τόπους εκτός από τις εξαιρέσεις.

- 6. Από προεπιλογή, υπάρχει μια εξαίρεση ως προς το να επιτρέπεται η συλλογή δεδομένων στους δικτυακούς τόπους της Kaspersky και των συνεργατών της. Εάν θέλετε να αποκλείσετε τη συλλογή δεδομένων σε αυτούς τους δικτυακούς τόπους, αποεπιλέξτε το πλαίσιο ελέγχου Να επιτρέπεται η συλλογή δεδομένων σχετικά με τις τοποθεσίες web της Kaspersky και των συνεργατών της.
- 7. Από προεπιλογή, υπάρχει μια εξαίρεση ως προς το να επιτρέπεται η συλλογή δεδομένων στους δικτυακούς τόπους που μπορεί να καταστούν μη λειτουργικοί ως αποτέλεσμα του αποκλεισμού της συλλογής δεδομένων, σύμφωνα με τις πληροφορίες που είναι στη διάθεση της Kaspersky. Εάν θέλετε να αποκλείσετε τη συλλογή δεδομένων σε αυτούς τους δικτυακούς τόπους, αποεπιλέξτε το πλαίσιο ελέγχου Να επιτρέπεται η συλλογή δεδομένων σχετικά με μη συμβατές τοποθεσίες web.

Η Kaspersky ενημερώνει τη λίστα των μη συμβατών δικτυακών τόπων όταν επιλύονται τα προβλήματα συμβατότητας.

- 8. Εάν θέλετε να καθορίσετε τις δικές σας εξαιρέσεις:
 - a. Κάντε κλικ στη σύνδεση **Κατηγορίες και εξαιρέσεις** για να ανοίξετε το παράθυρο **Κατηγορίες και εξαιρέσεις**.
 - b. Κάντε κλικ στη σύνδεση **Εξαιρέσεις** για να ανοίξετε το παράθυρο **Εξαιρέσεις ιδιωτικής περιήγησης**.
 - c. Κάντε κλικ στο κουμπί **Προσθήκη**.
 - d. Στο παράθυρο που θα εμφανιστεί, εισαγάγετε τη διεύθυνση του δικτυακού τόπου στον οποίο θέλετε να επιτρέψετε την παρακολούθηση της δραστηριότητας και κάντε κλικ στο κουμπί **Προσθήκη**.

Ο καθορισμένος δικτυακός τόπος προστίθεται στη λίστα εξαιρέσεων.

Μπορείτε επίσης να επιτρέψετε τη συλλογή δεδομένων σε έναν επιλεγμένο δικτυακό τόπο όταν τον ανοίγετε στο <u>πρόγραμμα περιήγησης</u>.

Προβολή αναφοράς για προσπάθειες συλλογής δεδομένων

Για την προβολή μιας αναφοράς για προσπάθειες συλλογής δεδομένων:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Ιδιωτική προστασία**.

Ανοίγει το παράθυρο Ιδιωτική προστασία.

Στο παράθυρο **Ιδιωτική προστασία**, η ενότητα **Ιδιωτική περιήγηση** δείχνει μια ενοποιημένη αναφορά με πληροφορίες σχετικά με τις προσπάθειες συλλογής δεδομένων για την online δραστηριότητά σας.

Μπορείτε, επίσης, να προβάλλετε την αναφορά για προσπάθειες συλλογής δεδομένων <u>σε ένα</u> <u>πρόγραμμα περιήγησης</u> ή στην <u>αναφορά αποτελεσματικότητας εφαρμογής</u>.

Διαχείριση του στοιχείου Ιδιωτική περιήγηση σε ένα πρόγραμμα περιήγησης

Μπορείτε να διαχειριστείτε το στοιχείο Ιδιωτική περιήγηση απευθείας από ένα πρόγραμμα περιήγησης:

- Ενεργοποιήστε το στοιχείο εάν είναι απενεργοποιημένο
- Προβολή στατιστικών στοιχείων για εντοπισμένες προσπάθειες συλλογής δεδομένων
- Μεταβείτε στο παράθυρο ρυθμίσεων ιδιωτικής περιήγησης
- Να αποκλειστεί ή να επιτραπεί η συλλογή δεδομένων

Για να διαχειριστείτε το στοιχείο Ιδιωτική περιήγηση από το πρόγραμμα περιήγησης,

Κάντε κλικ στο κουμπί 🥑 **Kaspersky Protection** στη γραμμή εργαλείων του προγράμματος περιήγησης.

Το μενού που θα εμφανιστεί περιέχει πληροφορίες σχετικά με τη λειτουργία και τα στοιχεία ελέγχου του στοιχείου.

Προστασία προγράμματος Anti-Banner κατά την περιήγηση σε δικτυακούς τόπους

Η ενότητα αυτή παρέχει πληροφορίες για τον τρόπο με τον οποίο το Kaspersky Total Security μπορεί να σας προστατεύσει από διαφημιστικά πλαίσια στο Διαδίκτυο.

Πληροφορίες για το Πρόγραμμα Anti-Banner

Το στοιχείο Πρόγραμμα Anti-Banner είναι σχεδιασμένο για να παρέχει προστασία από τα διαφημιστικά πλαίσια κατά την περιήγησή σας στο web. Το Πρόγραμμα Anti-Banner αποκλείει τα διαφημιστικά πλαίσια που εμφανίζονται στους δικτυακούς τόπους που επισκέπτεστε και στο περιβάλλον εργασίας ορισμένων εφαρμογών. Το Πρόγραμμα Anti-Banner αποκλείει τα διαφημιστικά πλαίσια από τη λίστα των γνωστών διαφημιστικών πλαισίων που είναι ενσωματωμένη στις βάσεις δεδομένων του Kaspersky Total Security. Μπορείτε να διαχειριστείτε τον αποκλεισμό των διαφημιστικών πλαισίων μέσω του περιβάλλοντος εργασίας του Kaspersky Total Security ή απευθείας στο πρόγραμμα Από προεπιλογή, τα διαφημιστικά πλαίσια επιτρέπονται στους δικτυακούς τόπους που περιλαμβάνονται στη λίστα **Τοποθεσίες web της Kaspersky**. Αυτή η λίστα αναπτύσσεται από ειδικούς της Kaspersky και περιλαμβάνει τους δικτυακούς τόπους της Kaspersky και των συνεργατών της οι οποίοι φιλοξενούν τις διαφημίσεις της Kaspersky. Μπορείτε να προβάλετε αυτή τη λίστα ή να απενεργοποιήσετε τη χρήση αυτής της λίστας εάν θεωρείτε ότι είναι απαραίτητος ο αποκλεισμός των διαφημιστικών πλαισίων στους δικτυακούς τόπους της Kaspersky και των συνεργατών της.

Ο μετρητής αποκλεισμένων διαφημιστικών πλαισίων εμφανίζει τον συνολικό αριθμό αποκλεισμένων διαφημιστικών πλαισίων σε ολόκληρη την τοποθεσία ανάλογα με το πόσες ιστοσελίδες είναι ανοικτές στο πρόγραμμα περιήγησης. Αν μία σελίδα είναι ανοικτή στο πρόγραμμα περιήγησης, μετριούνται μόνο οι αποκλεισμοί σε αυτή τη σελίδα. Αν στο πρόγραμμα περιήγησης είναι ανοικτές διάφορες σελίδες της ίδιας τοποθεσίας, μετριούνται τα αποκλεισμένα διαφημιστικά πλαίσια σε όλες τις σελίδες της τοποθεσίας που έχουν ανοιχτεί στο πρόγραμμα περιήγησης.

Οι πληροφορίες σχετικά με τη λειτουργία του Προγράμματος Anti-Banner είναι διαθέσιμες στις <u>αναφορές</u>.

Οι ακόλουθοι περιορισμοί ισχύουν για το Πρόγραμμα Anti-Banner:

- Εάν η ιστοσελίδα στην οποία βρίσκεται το διαφημιστικό πλαίσιο δεν ήταν δυνατόν να προσδιοριστεί, το Kaspersky Total Security δεν αποκλείει το συγκεκριμένο διαφημιστικό πλαίσιο και δεν εμφανίζει πληροφορίες για αυτό.
- Εάν η ιστοσελίδα στην οποία βρίσκεται το διαφημιστικό πλαίσιο ήταν δυνατόν να προσδιοριστεί αλλά δεν ήταν δυνατόν να αντιστοιχιστεί σε οποιαδήποτε μεμονωμένη ιστοσελίδα που είναι ανοιγμένη στο πρόγραμμα περιήγησης, το Kaspersky Total Security αποκλείει το διαφημιστικό πλαίσιο ή επιτρέπει την εμφάνιση του διαφημιστικού πλαισίου ανάλογα με τις πληροφορίες που έχουν προσδιοριστεί. Η εφαρμογή εμφανίζει πληροφορίες σχετικά με το διαφημιστικό πλαίσιο σε αναφορές, αλλά δεν περιλαμβάνει αυτές τις πληροφορίες στα στατιστικά στοιχεία του Προγράμματος Anti-Banner που εμφανίζονται στο πρόγραμμα περιήγησης.
- Τα στατιστικά στοιχεία του Προγράμματος Anti-Banner που εμφανίζονται στο πρόγραμμα περιήγησης μπορεί να περιλαμβάνουν διαφημιστικά πλαίσια που αποκλείστηκαν την προηγούμενη φορά που πραγματοποιήθηκε φόρτωση των ιστοσελίδων, συμπεριλαμβανομένων των διαφημιστικών πλαισίων που αποκλείστηκαν νωρίτερα και που φορτώθηκαν ξανά.
- Τα στατιστικά στοιχεία του Προγράμματος Anti-Banner που εμφανίζονται στο πρόγραμμα περιήγησης δεν περιλαμβάνουν τα διαφημιστικά πλαίσια που αποκλείστηκαν στο δυναμικό περιεχόμενο μιας σελίδας μετά τη φόρτωση ενός δικτυακού τόπου.

- Μετά από εγκατάσταση του Kaspersky Total Security 2016 Έκδοση συντήρησης 1, οι ακόλουθες ρυθμίσεις καθίστανται μη διαθέσιμες προς επεξεργασία μέσω του περιβάλλοντος εργασίας χρήστη και ρυθμίζονται στις προεπιλεγμένες τιμές τους:
 - Χρήση της λίστας διαφημιστικών πλαισίων του Kaspersky Total Security
 - Αντιστοίχιση διευθύνσεων ΙΡ σε ονόματα τομέων
 - Χρήση της λίστας αποκλεισμένων διευθύνσεων URL
 - Χρήση της λίστας επιτρεπόμενων διευθύνσεων URL

Η λίστα που ανοίξατε νωρίτερα κάνοντας κλικ στη σύνδεση **Διαμόρφωση** αποκλεισμένων διευθύνσεων URL είναι τώρα διαθέσιμη κάνοντας κλικ στη σύνδεση **Αποκλεισμένα διαφημιστικά πλαίσια** στην τρέχουσα έκδοση. Η λίστα που ανοίξατε νωρίτερα κάνοντας κλικ στη σύνδεση **Διαμόρφωση επιτρεπόμενων διευθύνσεων URL** είναι τώρα διαθέσιμη κάνοντας κλικ στη σύνδεση **Επιτρεπόμενα διαφημιστικά** πλαίσια στην τρέχουσα έκδοση.

 Το Kaspersky Total Security δεν μπορεί να αποκλείσει ορισμένα διαφημιστικά πλαίσια στον Internet Explorer, επειδή ορισμένες δυνατότητες JavaScript δεν υποστηρίζονται από αυτό το πρόγραμμα περιήγησης.

Πώς να ενεργοποιήσετε το στοιχείο Πρόγραμμα Anti-Banner

Το στοιχείο Πρόγραμμα Anti-Banner είναι απενεργοποιημένο από προεπιλογή. Μπορείτε να το ενεργοποιήσετε μέσω του περιβάλλοντος εργασίας του Kaspersky Total Security ή με τη βοήθεια της επέκτασης Kaspersky Protection στο πρόγραμμα περιήγησής σας.

<u>Πώς να ενεργοποιήσετε το Πρόγραμμα Anti-Banner στο περιβάλλον εργασίας του Kaspersky Total Security</u>

Για να ενεργοποιήσετε το στοιχείο Πρόγραμμα Anti-Banner στο περιβάλλον εργασίας του Kaspersky Total Security:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.

4. Επιλέξτε το στοιχείο Πρόγραμμα Anti-Banner.

Ανοίγει το παράθυρο **Ρυθμίσεις του Προγράμματος Anti-Banner**.

5. Ενεργοποιήστε το στοιχείο, χρησιμοποιήστε το διακόπτη στο επάνω μέρος του παραθύρου.

<u>Πώς να ενεργοποιήσετε το Πρόγραμμα Anti-Banner στο παράθυρο του προγράμματος</u> <u>περιήγησης</u> ?

Για να ενεργοποιήσετε το στοιχείο Πρόγραμμα Anti-Banner στο παράθυρο του προγράμματος περιήγησης:

- 1. Κάντε κλικ στο κουμπί 🔮 **Kaspersky Protection** στη γραμμή εργαλείων του προγράμματος περιήγησης.
- 2. Στο αναπτυσσόμενο μενού στην ενότητα **Πρόγραμμα Anti-Banner**, κάντε κλικ στο κουμπί **Ενεργοποίηση**.

Μετά την ενεργοποίηση ή απενεργοποίηση του Προγράμματος Anti-Banner, πρέπει να ξαναφορτώσετε την ιστοσελίδα στον περιηγητή για να ισχύσουν οι αλλαγές.

Να αποκλειστούν τα διαφημιστικά πλαίσια

Το Πρόγραμμα Anti-Banner αποκλείει τα διαφημιστικά πλαίσια δικτυακών τόπων από τη λίστα των γνωστών διαφημιστικών πλαισίων που είναι ενσωματωμένη στις βάσεις δεδομένων του Kaspersky Total Security. Εάν ένα διαφημιστικό πλαίσιο εμφανιστεί σε μια ιστοσελίδα ακόμη και όταν εκτελείται το Πρόγραμμα Anti-Banner, αυτό θα μπορούσε να σημαίνει ότι το διαφημιστικό πλαίσιο δεν περιλαμβάνεται στη λίστα των γνωστών διαφημιστικών πλαισίων. Μπορείτε να αποκλείσετε χειροκίνητα την εμφάνιση του συγκεκριμένου διαφημιστικού πλαισίου.

Για να αποκλείσετε ένα διαφημιστικό πλαίσιο, πρέπει να το προσθέσετε στη λίστα των αποκλεισμένων διαφημιστικών πλαισίων. Αυτό μπορείτε να το κάνετε απευθείας στην ιστοσελίδα ή στο περιβάλλον εργασίας του Kaspersky Total Security.

Εάν ένα διαφημιστικό πλαίσιο βρίσκεται σε έναν δικτυακό τόπο που περιλαμβάνεται στη λίστα δικτυακών τόπων με <u>επιτρεπόμενα διαφημιστικά πλαίσια</u>, δεν μπορείτε να αποκλείσετε την εμφάνιση αυτού του διαφημιστικού πλαισίου.

Πώς να αποκλείσετε διαφημιστικό πλαίσιο σε μια ιστοσελίδα 🖓

Για να αποκλείσετε ένα διαφημιστικό πλαίσιο σε μια ιστοσελίδα:

- 1. Βεβαιωθείτε ότι η <u>επέκταση Kaspersky Protection</u> έχει εγκατασταθεί και ενεργοποιηθεί στο πρόγραμμα περιήγησης.
- 2. Εάν το Πρόγραμμα Anti-Banner είναι απενεργοποιημένο, ενεργοποιήστε το:
 - a. Κάντε κλικ στο κουμπί 🔮 **Kaspersky Protection** στη γραμμή εργαλείων του προγράμματος περιήγησης.
 - b. Στο αναπτυσσόμενο μενού στην ενότητα **Πρόγραμμα Anti-Banner**, κάντε κλικ στο κουμπί **Ενεργοποίηση**.
- Μετακινήστε τον δείκτη του ποντικιού πάνω από το διαφημιστικό πλαίσιο που θέλετε να αποκλείσετε και κάντε δεξιό κλικ.
- 4. Στο μενού περιβάλλοντος που ανοίγει, επιλέξτε **Προσθήκη στο Πρόγραμμα Anti-**Banner.

Ανοίγει το παράθυρο **Προσθήκη αποκλεισμένου διαφημιστικού πλαισίου**.

5. Στο παράθυρο **Προσθήκη αποκλεισμένου διαφημιστικού πλαισίου**, κάντε κλικ στο κουμπί **Προσθήκη**.

Η διεύθυνση URL του διαφημιστικού πλαισίου προστίθεται στην λίστα αποκλεισμένων διαφημιστικών πλαισίων.

6. Ανανεώστε την ιστοσελίδα στο πρόγραμμα περιήγησης για να αποτρέψετε την εμφάνιση του διαφημιστικού πλαισίου.

Το διαφημιστικό πλαίσιο δεν θα εμφανιστεί την επόμενη φορά που θα επισκεφτείτε την ιστοσελίδα.

<u>Πώς να αποκλείσετε διαφημιστικό πλαίσιο μέσω του περιβάλλοντος εργασίας του Kaspersky Total Security</u>

Για να αποκλείσετε ένα διαφημιστικό πλαίσιο μέσω του περιβάλλοντος εργασίας της επέκτασης Kaspersky Total Security:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.
- 4. Επιλέξτε το στοιχείο Πρόγραμμα Anti-Banner.

Ανοίγει το παράθυρο **Ρυθμίσεις του Προγράμματος Anti-Banner**.

- 5. Για να ενεργοποιήσετε το Πρόγραμμα Anti-Banner, χρησιμοποιήστε το διακόπτη στο επάνω μέρος του παραθύρου.
- 6. Στο παράθυρο Ρυθμίσεις του Προγράμματος Anti-Banner, κάντε κλικ στη σύνδεση Αποκλεισμένα διαφημιστικά πλαίσια για να ανοίξετε το παράθυρο Αποκλεισμένα διαφημιστικά πλαίσια.
- 7. Στο παράθυρο Αποκλεισμένα διαφημιστικά πλαίσια, κάντε κλικ στο κουμπί Προσθήκη.
- 8. Στο παράθυρο που ανοίγει, στο πεδίο **Μάσκα διεύθυνσης web (URL)** εισαγάγετε τη διεύθυνση ή τη μάσκα διεύθυνσης του διαφημιστικού πλαισίου.
- 9. Ορίστε την τιμή **Ενεργό** ως κατάσταση του διαφημιστικού πλαισίου.
- 10. Κάντε κλικ στο κουμπί **Προσθήκη**.

Το Kaspersky Total Security θα αποκλείσει το καθορισμένο διαφημιστικό πλαίσιο.

Να επιτρέπονται τα διαφημιστικά πλαίσια

Μπορείτε να επιτρέψετε ένα μεμονωμένο διαφημιστικό πλαίσιο, καθώς και όλα τα διαφημιστικά πλαίσια σε έναν δικτυακό τόπο που καθορίζετε εσείς.

<u>Πώς να εμφανίσετε μεμονωμένο διαφημιστικό πλαίσιο</u> ව

Για να επιτρέψετε ένα μεμονωμένο διαφημιστικό πλαίσιο:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.
- Επιλέξτε το στοιχείο Πρόγραμμα Anti-Banner.
 Ανοίγει το παράθυρο Ρυθμίσεις του Προγράμματος Anti-Banner.
- 5. Για να ενεργοποιήσετε το Πρόγραμμα Anti-Banner, χρησιμοποιήστε το διακόπτη στο επάνω μέρος του παραθύρου.
- 6. Στο παράθυρο Ρυθμίσεις του Προγράμματος Anti-Banner, κάντε κλικ στη σύνδεση Επιτρεπόμενα διαφημιστικά πλαίσια για να ανοίξετε το παράθυρο Επιτρεπόμενα διαφημιστικά πλαίσια.
- 7. Στο παράθυρο Επιτρεπόμενα διαφημιστικά πλαίσια, κάντε κλικ στο κουμπί Προσθήκη.
- 8. Στο παράθυρο που ανοίγει, στο πεδίο **Μάσκα διεύθυνσης web (URL)** εισαγάγετε τη διεύθυνση ή τη μάσκα διεύθυνσης του διαφημιστικού πλαισίου.
- 9. Επιλέξτε την κατάσταση **Ενεργό**.
- 10. Κάντε κλικ στο κουμπί **Προσθήκη**.

Το Kaspersky Total Security δεν θα αποκλείσει το καθορισμένο διαφημιστικό πλαίσιο.

Εάν κάποιο διαφημιστικό πλαίσιο προστέθηκε στη λίστα επιτρεπόμενων διαφημιστικών πλαισίων αλλά το διαφημιστικό πλαίσιο βρίσκεται εντός ενός μπλοκ διαφημίσεων του οποίου οι παράμετροι προκαλούν τον αποκλεισμό του από το Πρόγραμμα Anti-Banner κατά την επίσκεψη σε κάποιον δικτυακό τόπο, τότε το διαφημιστικό πλαίσιο θα αποκλειστεί μαζί με το μπλοκ διαφημίσεων.

<u>Πώς να εμφανίσετε όλα τα διαφημιστικά πλαίσια σε έναν δικτυακό τόπο </u>

Για να επιτρέψετε όλα τα διαφημιστικά πλαίσια σε έναν δικτυακό τόπο:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.
- Επιλέξτε το στοιχείο Πρόγραμμα Anti-Banner.
 Ανοίγει το παράθυρο Ρυθμίσεις του Προγράμματος Anti-Banner.
- 5. Για να ενεργοποιήσετε το Πρόγραμμα Anti-Banner, χρησιμοποιήστε το διακόπτη στο επάνω μέρος του παραθύρου.
- 6. Στο παράθυρο **Ρυθμίσεις του Προγράμματος Anti-Banner**, κάντε κλικ στη σύνδεση **Τοποθεσίες web με επιτρεπόμενα banner** για να ανοίξετε το παράθυρο **Τοποθεσίες web με επιτρεπόμενα banner**.
- 7. Στο παράθυρο Τοποθεσίες web με επιτρεπόμενα banner, κάντε κλικ στο κουμπί Προσθήκη.
- 8. Στο παράθυρο που ανοίγει, στο πεδίο **Τοποθεσία web**, εισαγάγετε τη διεύθυνση URL, για παράδειγμα, example.com.
- 9. Επιλέξτε την κατάσταση **Ενεργό**.
- 10. Κάντε κλικ στο κουμπί **Προσθήκη**.

Ο δικτυακός τόπος θα προστεθεί στη λίστα των δικτυακών τόπων με επιτρεπόμενα διαφημιστικά πλαίσια. Το Kaspersky Total Security δεν αποκλείει τα διαφημιστικά πλαίσια που περιλαμβάνονται στους δικτυακούς τόπους αυτής της λίστας, ακόμη και αν το διαφημιστικό πλαίσιο έχει <u>προστεθεί στη λίστα αποκλεισμένων διαφημιστικών</u> <u>πλαισίων</u>.

Πώς να ρυθμίσετε τα φίλτρα στο πρόγραμμα Anti-Banner

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.

4. Επιλέξτε το στοιχείο Πρόγραμμα Anti-Banner.

Ανοίγει το παράθυρο Ρυθμίσεις του Προγράμματος Anti-Banner.

- 5. Για να ενεργοποιήσετε το Πρόγραμμα Anti-Banner, χρησιμοποιήστε το διακόπτη στο επάνω μέρος του παραθύρου.
- 6. Κάντε κλικ στη σύνδεση **Λίστα φίλτρων** για να ανοίξετε το παράθυρο **Λίστα φίλτρων**.
- 7. Στο παράθυρο Λίστα φίλτρων, ρυθμίστε τις παραμέτρους των φίλτρων όπως είναι αναγκαίο:
 - Συνιστάται. Αυτή η ομάδα περιλαμβάνει το γενικό φίλτρο και το φίλτρο γλώσσας που αντιστοιχούν στην περιοχή σας. Αυτά τα φίλτρα είναι ενεργοποιημένα από προεπιλογή.
 - **Ανά θέμα**. Αυτή η ομάδα περιλαμβάνει δύο φίλτρα:
 - Μέσα κοινωνικής δικτύωσης. Ενεργοποιήστε αυτό το φίλτρο εάν θέλετε να αποκλείσετε στοιχεία όπως τα κουμπιά Μου αρέσει και Κοινοποίηση στους δικτυακούς τόπους των κοινωνικών δικτύων.
 - Ενοχλήσεις. Ενεργοποιήστε αυτό το φίλτρο εάν θέλετε να αποκλείσετε αναδυόμενα μηνύματα, παράθυρα και άλλα στοιχεία που δεν ανήκουν στο συγκεκριμένο δικτυακό τόπο.
 - Για συγκεκριμένη γλώσσα. Σε αυτή την ομάδα φίλτρων, μπορείτε να επιλέξετε μια γλώσσα. Η εφαρμογή θα αποκλείσει διαφημιστικά πλαίσια σε δικτυακούς τόπους στη συγκεκριμένη γλώσσα.

Τρόπος διαχείρισης του Προγράμματος Anti-Banner στο πρόγραμμα περιήγησης

Μπορείτε να διαχειριστείτε το στοιχείο Πρόγραμμα Anti-Banner απευθείας στο πρόγραμμα περιήγησης χρησιμοποιώντας την επέκταση Kaspersky Protection.

Η επέκταση Kaspersky Protection σας επιτρέπει να εκτελέσετε τις ακόλουθες ενέργειες:

- Ενεργοποίηση και απενεργοποίηση του στοιχείου
- Προβολή των στατιστικών στοιχείων για αποκλεισμένα διαφημιστικά πλαίσια
- Μετάβαση στο παράθυρο ρυθμίσεων για το Πρόγραμμα Anti-Banner

 Προβάλετε πληροφορίες σχετικά με το εάν θα αποκλείονται ή όχι τα διαφημιστικά πλαίσια σε έναν δικτυακό τόπο που τον ανοίγετε στο πρόγραμμα περιήγησης και διαχειριστείτε την εμφάνιση των διαφημιστικών πλαισίων σε έναν δικτυακό τόπο

<u>Πώς να διαχειριστείτε το στοιχείο Πρόγραμμα Anti-Banner μέσω της επέκτασης Kaspersky</u> <u>Protection</u> 🔋

Για διαχείριση του στοιχείου Πρόγραμμα Anti-Banner μέσω της επέκτασης Kaspersky Protection:

Κάντε κλικ στο κουμπί **Ο Kaspersky Protection** στη γραμμή εργαλείων του προγράμματος περιήγησης.

Το μενού που θα εμφανιστεί περιέχει πληροφορίες σχετικά με τη λειτουργία και τα στοιχεία ελέγχου του στοιχείου.

Προστασία της Webcam

Αυτή η ενότητα περιέχει πληροφορίες για να αποφύγετε να σας παρακολουθούν τρίτοι μέσω webcam.

Σχετικά με την πρόσβαση εφαρμογών στην webcam

Το στοιχείο Προστασία της Webcam είναι σχεδιασμένο να προστατεύει την webcam σας από μη εξουσιοδοτημένη πρόσβαση. Εάν είναι ενεργοποιημένη η Προστασία της Webcam και έχει επιλεγεί το πλαίσιο ελέγχου **Αποκλεισμός πρόσβασης στην webcam για όλες τις εφαρμογές**, το Kaspersky Total Security αποκλείει την πρόσβαση στη webcam για όλες τις εφαρμογές και σας ενημερώνει ότι η πρόσβαση έχει αποκλειστεί.

Εάν έχει αποεπιλεχθεί το πλαίσιο ελέγχου **Αποκλεισμός πρόσβασης στην webcam για όλες τις εφαρμογές**, το Kaspersky Total Security παρακολουθεί την πρόσβαση εφαρμογών στη webcam ανάλογα με την ομάδα αξιοπιστίας της εφαρμογής που ζητά την πρόσβαση. Το Kaspersky Total Security αποκλείει την πρόσβαση στην webcam σε εφαρμογές που έχουν περιληφθεί στις ομάδες εφαρμογών Υψηλού περιορισμού ή Μη αξιόπιστων εφαρμογών.

Στο παράθυρο ρυθμίσεων του Ελέγχου εφαρμογών, <u>μπορείτε να επιτρέψετε την πρόσβαση</u> <u>στην webcam</u> σε εφαρμογές που περιλαμβάνονται στις κατηγορίες Υψηλού περιορισμού και Μη αξιόπιστων. Εάν μια εφαρμογή από την ομάδα αξιοπιστίας Χαμηλού περιορισμού επιχειρήσει να συνδεθεί στην webcam, το Kaspersky Total Security εμφανίζει μια ειδοποίηση και σας ζητά να αποφασίσετε αν θα επιτραπεί η πρόσβαση στην webcam. Εάν πραγματοποιηθεί απόπειρα πρόσβασης στην webcam από μια εφαρμογή που δεν της επιτρέπεται η πρόσβαση από προεπιλογή, το Kaspersky Total Security εμφανίζει μια ειδοποίηση. Η ειδοποίηση σας ενημερώνει για το γεγονός ότι μια εφαρμογή που είναι εγκατεστημένη στον υπολογιστή (όπως το Skype) λαμβάνει εκείνη τη στιγμή δεδομένα βίντεο από την webcam. Στην αναπτυσσόμενη λίστα της ειδοποίησης μπορείτε να αποκλείσετε την εφαρμογή από την πρόσβαση στην webcam ή να <u>προχωρήσετε στη διαμόρφωση των</u> <u>ρυθμίσεων πρόσβασης της εφαρμογής στην webcam</u>. Η ειδοποίηση αυτή δεν εμφανίζεται εάν οι εφαρμογές εκτελούνται ήδη σε λειτουργία πλήρους οθόνης στον υπολογιστή.

Στην αναπτυσσόμενη λίστα της ειδοποίησης σχετικά με τη λήψη δεδομένων βίντεο από την εφαρμογή, μπορείτε επίσης να επιλέξετε να αποκρύπτονται οι ειδοποιήσεις ή να <u>προχωρήσετε στη ρύθμιση των παραμέτρων εμφάνισης της ειδοποίησης</u>.

Από προεπιλογή, το Kaspersky Total Security επιτρέπει την πρόσβαση στην webcam σε εφαρμογές που απαιτούν την άδειά σας, εάν το γραφικό περιβάλλον διεπαφής χρήστη (GUI) της εφαρμογής εξακολουθεί να φορτώνεται, καταργείται η φόρτωσή του ή δεν ανταποκρίνεται, και δεν μπορείτε να επιτρέψετε την πρόσβαση χειροκίνητα.

Η λειτουργία προστασίας της πρόσβασης στην webcam έχει τις εξής δυνατότητες και περιορισμούς:

- Η εφαρμογή ελέγχει το βίντεο και τις εικόνες που προέρχονται από την επεξεργασία δεδομένων της webcam.
- Η εφαρμογή ελέγχει το ηχητικό σήμα, εάν αποτελεί μέρος της ροής βίντεο που προέρχεται από την webcam.
- Το Kaspersky Total Security ελέγχει μόνο τις webcam που συνδέονται μέσω USB ή IEEE1394 και εμφανίζονται στη Διαχείριση συσκευών των Windows ως Συσκευές απεικόνισης.

Κάντε κλικ σε αυτή τη <u>σύνδεση</u> 🖾 για να δείτε τη λίστα με τις υποστηριζόμενες webcam.

Για να ενεργοποιήσετε την προστασία ενάντια στη μη εξουσιοδοτημένη πρόσβαση στην webcam, πρέπει να ενεργοποιήσετε το στοιχείο Ελέγχου εφαρμογών.

Η Προστασία της Webcam έχει <u>περιορισμούς εάν η εφαρμογή εγκαταστάθηκε στα πλαίσια</u> <u>της επετειακής ενημέρωσης των Microsoft Windows 10 (RedStone 1)</u>.

Τρόπος αλλαγής των ρυθμίσεων πρόσβασης εφαρμογών στη webcam

Για την αλλαγή των ρυθμίσεων πρόσβασης εφαρμογών στην webcam:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Στην ενότητα **Προστασία**, επιλέξτε το στοιχείο Προστασία της Webcam.
- 4. Διαμορφώστε τις ρυθμίσεις πρόσβασης της εφαρμογής στην webcam του υπολογιστή σας:
 - Για να αποκλείσετε την πρόσβαση στην webcam σε όλες τις εφαρμογές, επιλέξτε το πλαίσιο ελέγχου Αποκλεισμός πρόσβασης στην webcam για όλες τις εφαρμογές.
 - Για να λαμβάνετε ειδοποιήσεις όταν η webcam χρησιμοποιείται από μια εφαρμογή που της έχει εκχωρηθεί αυτό το δικαίωμα, επιλέξτε το πλαίσιο ελέγχου Εμφάνιση ειδοποίησης όταν η webcam χρησιμοποιείται από μια εφαρμογή στην οποία επιτρέπεται η πρόσβαση στην webcam.

Πώς να επιτρέψετε την πρόσβαση των εφαρμογών στην webcam

Για να επιτρέψετε σε μια εφαρμογή την πρόσβαση στην webcam:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Περισσότερα εργαλεία**.

Ανοίγει το παράθυρο **Εργαλεία**.

- 3. Στο παράθυρο **Εργαλεία**, μεταβείτε στην ενότητα **Διαχείριση εφαρμογών**.
- 4. Κάντε κλικ στη σύνδεση **Έλεγχος εφαρμογών** για να ανοίξετε το παράθυρο **Έλεγχος** εφαρμογών.
- 5. Στο παράθυρο **Έλεγχος εφαρμογών**, κάντε κλικ στη σύνδεση **Διαχείριση εφαρμογών** για να ανοίξετε το παράθυρο **Διαχείριση εφαρμογών**.
- 6. Επιλέξτε από τη λίστα την εφαρμογή στην οποία θέλετε να επιτρέψετε την πρόσβαση στην webcam. Κάντε διπλό κλικ στο όνομα της εφαρμογής για να ανοίξετε το παράθυρο **Κανόνες εφαρμογής**.
- 7. Στο παράθυρο **Κανόνες εφαρμογής**, μεταβείτε στην καρτέλα **Δικαιώματα**.

- 8. Στη λίστα με τις κατηγορίες δικαιωμάτων, επιλέξτε Τροποποίηση λειτουργικού συστήματος → Ύποπτες τροποποιήσεις στο λειτουργικό σύστημα → Πρόσβαση στην webcam.
- 9. Στη στήλη **Ενέργεια**, κάντε κλικ στο εικονίδιο για να εμφανιστεί το μενού περιβάλλοντος και, στη συνέχεια, επιλέξτε **Να επιτρέπεται**.
- 10. Κάντε κλικ στο κουμπί **Αποθήκευση**.

Η πρόσβαση της εφαρμογής στη webcam θα επιτραπεί εάν έχει αποεπιλεχθεί το πλαίσιο ελέγχου **Αποκλεισμός πρόσβασης στην webcam για όλες τις εφαρμογές**.

Εάν είναι επιλεγμένο το πλαίσιο ελέγχου **Αποκλεισμός πρόσβασης στην webcam για** όλες τις εφαρμογές, το Kaspersky Total Security αποκλείει την πρόσβαση εφαρμογών στη webcam ανεξάρτητα από την ομάδα αξιοπιστίας και τα δικαιώματα που διαμορφώθηκαν χειροκίνητα.

Προστασία για παιδιά

Σε αυτή την ενότητα θα μάθετε πώς μπορείτε να προστατεύσετε τα παιδιά σας στον πραγματικό και στον εικονικό κόσμο.

Σχετικά με την προστασία των παιδιών με χρήση του Kaspersky Safe Kids

Εάν έχετε εγκαταστήσει το Kaspersky Total Security στον υπολογιστή σας, μπορείτε να χρησιμοποιήσετε την εφαρμογή *Kaspersky Safe Kids*, μια λύση που συμβάλλει στην προστασία των παιδιών σας – δωρεάν.

Σχετικά με το Kaspersky Safe Kids

Το Kaspersky Safe Kids είναι μια λύση που μπορεί να χρησιμοποιηθεί σε διάφορες πλατφόρμες και σας βοηθά να παρακολουθείτε την ασφάλεια του παιδιού σας στον πραγματικό και στον εικονικό κόσμο. Εσείς θα αποφασίσετε τι είναι ασφαλές για το παιδί σας, όπως ποιες τοποθεσίες web μπορεί να επισκεφτεί, πόσες ώρες μπορεί να δαπανήσει στον υπολογιστή ή στο smartphone, και πού μπορεί να περπατήσει. Η εφαρμογή διασφαλίζει ότι το παιδί θα τηρήσει τους κανόνες που έχετε θέσει. Το Kaspersky Safe Kids είναι συμβατό με συσκευές Windows, macOS, Android και iOS. Εάν εγκαταστήσετε το Kaspersky Safe Kids στις συσκευές σας και στις συσκευές που χρησιμοποιεί το παιδί σας, μπορείτε να διαχειριστείτε την εφαρμογή στις συσκευές του παιδιού σας, χρησιμοποιώντας το λογαριασμό σας My Kaspersky ή τη λειτουργία γονικού ελέγχου της εφαρμογής στο κινητό τηλέφωνό σας.

Το Kaspersky Safe Kids διατίθεται σε δύο εκδόσεις: <u>Free και Premium</u> 🖬 .

Για να χρησιμοποιήσετε το Kaspersky Safe Kids, πρέπει να <u>κάνετε λήψη του πακέτου</u> <u>εγκατάστασης της εφαρμογής από το Διαδίκτυο και να εγκαταστήσετε χειροκίνητα την</u> <u>εφαρμογή</u> στον υπολογιστή.

Εάν χρησιμοποιείτε το Kaspersky Safe Kids

Το παιδί σας μπορεί να απενεργοποιήσει το Kaspersky Safe Kids χρησιμοποιώντας το Kaspersky Total Security. Για να αποφύγετε κάτι τέτοιο, σας συνιστούμε να <u>προστατέψετε την</u> <u>πρόσβαση στις ρυθμίσεις του Kaspersky Total Security με κωδικό πρόσβασης</u>.

Εάν συνδεθήκατε στο λειτουργικό σύστημα με ένα λογαριασμό που είναι συνδεδεμένος με ένα προφίλ παιδιού στο Kaspersky Safe Kids, το Kaspersky Total Security δεν θα εμφανίζει πλέον τις εξής ειδοποιήσεις:

- Ειδοποιήσεις σχετικά με ειδήσεις σχετικά με την ασφάλεια
- Ειδοποιήσεις σχετικά με τον εντοπισμό αδύναμων ρυθμίσεων στο λειτουργικό σύστημα
- Ειδοποιήσεις σχετικά με την τρέχουσα συσκευή που συνδέεται σε ένα δίκτυο Wi-Fi
- Ειδοποιήσεις σχετικά με συσκευή που συνδέεται σε οικιακό δίκτυο Wi-Fi
- Ειδοποιήσεις του προγράμματος περιήγησης σχετικά με ανεπαρκώς ισχυρό κωδικό πρόσβασης που εισάγεται σε μια τοποθεσία web
- Ειδοποιήσεις που σας προειδοποιούν ότι ο κωδικός πρόσβασης που εισάγετε σε μια τοποθεσία web έχει ήδη εισαχθεί από εσάς σε μια άλλη τοποθεσία web

Μπορείτε να ενεργοποιήσετε τις ειδοποιήσεις, επιλέγοντας το πλαίσιο ελέγχου **Εμφάνιση** ειδοποιήσεων σε λογαριασμούς παιδιών στο παράθυρο Ρυθμίσεις ειδοποιήσεων (Ρυθμίσεις -> Διεπαφή -> Ειδοποιήσεις).

Το Kaspersky Safe Kids δεν είναι διαθέσιμο σε όλες τις περιοχές.

Τρόπος εκτέλεσης του Kaspersky Safe Kids

Τρόπος λήψης και εγκατάστασης του Kaspersky Safe Kids 🛛

Για να προβείτε στη λήψη και εγκατάσταση του Kaspersky Safe Kids, εάν δεν έχει εγκατασταθεί ακόμη:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί Προστασία για παιδιά.
 Ανοίγει το παράθυρο Προστασία για παιδιά.
- 3. Κάντε κλικ στο κουμπί **Λήψη και εγκατάσταση**.

Το Kaspersky Total Security κάνει λήψη του πακέτου εγκατάστασης του Kaspersky Safe Kids και εγκαθιστά την εφαρμογή στον υπολογιστή σας.

<u>Τρόπος εκτέλεσης του Kaspersky Safe Kids</u> ?

Για να εκκινήσετε το Kaspersky Safe Kids που είναι ήδη εγκατεστημένο:

- 1. Ανοίξτε το κύριο παράθυρο του Kaspersky Total Security.
- 2. Κάντε κλικ στο κουμπί **Προστασία για παιδιά**.
- 3. Στο παράθυρο, κάντε κλικ στο κουμπί **Άνοιγμα**.

Το παράθυρο της εφαρμογής Kaspersky Safe Kids ανοίγει.

Χρήση του Kaspersky Safe Kids

Η αρχική ρύθμιση παραμέτρων και η χρήση του Kaspersky Safe Kids περιγράφονται στη Βοήθεια για το Kaspersky Safe Kids.

Για μετάβαση στη Βοήθεια για το Kaspersky Safe Kids:

1. Ανοίξτε την κύρια σελίδα της <u>Ηλεκτρονικής βοήθειας για το Kaspersky</u>.

 Στην ενότητα Kaspersky Safe Kids, επιλέξτε από την αναπτυσσόμενη λίστα το λειτουργικό σύστημα της συσκευής όπου είναι εγκαταστημένη η εφαρμογή.

Εμφανίζει τη βοήθεια του Kaspersky Safe Kids για το επιλεγμένο λειτουργικό σύστημα.

 Εάν πρέπει να αλλάξετε τη γλώσσα της βοήθειας, επιλέξτε την από την αναπτυσσόμενη λίστα στο επάνω μέρος της σελίδας.

Χειρισμός άγνωστων εφαρμογών

Το Kaspersky Total Security βοηθάει να ελαχιστοποιήσετε τον κίνδυνο από τη χρήση άγνωστων εφαρμογών (όπως ο κίνδυνος μόλυνσης με ιούς και άλλο κακόβουλο λογισμικό).

To Kaspersky Total Security περιλαμβάνει στοιχεία και εργαλεία που επιτρέπουν να διαπιστώσετε την αξιοπιστία μιας εφαρμογής και να ελέγχετε τις δραστηριότητες που εκτελεί στον υπολογιστή σας.

Έλεγχος αξιοπιστίας εφαρμογής

Το Kaspersky Total Security σάς επιτρέπει να επαληθεύετε την αξιοπιστία των εφαρμογών με χρήστες από όλον τον κόσμο. Η αξιοπιστία μιας εφαρμογής περιλαμβάνει τα παρακάτω κριτήρια:

- Όνομα προμηθευτή
- Πληροφορίες σχετικά με την ψηφιακή υπογραφή ? (αν η εφαρμογή είναι ψηφιακά υπογεγραμμένη)
- Πληροφορίες σχετικά με την ομάδα στην οποία έχει κατατάξει την εφαρμογή ο Έλεγχος εφαρμογών ή η πλειοψηφία των χρηστών του Kaspersky Security Network
- Τον αριθμό των χρηστών του Kaspersky Security Network που χρησιμοποιούν την εφαρμογή (διαθέσιμος εάν η εφαρμογή έχει συμπεριληφθεί στην ομάδα "Αξιόπιστες" στη βάση δεδομένων του Kaspersky Security Network)
- Τη χρονική στιγμή κατά την οποία η εφαρμογή έγινε γνωστή στο Kaspersky Security Network
- Τις χώρες στις οποίες είναι πιο διαδεδομένη η εφαρμογή

Ο έλεγχος αξιοπιστίας εφαρμογής είναι διαθέσιμος εάν έχετε συμφωνήσει να συμμετάσχετε στο Kaspersky Security Network.

Για να ενημερωθείτε για την αξιοπιστία μιας εφαρμογής:

Ανοίξτε το μενού περιβάλλοντος του εκτελέσιμου αρχείου της εφαρμογής και επιλέξτε Έλεγχος αξιοπιστίας στο KSN.

Αυτό ανοίγει ένα παράθυρο με πληροφορίες σχετικά με την αξιοπιστία της εφαρμογής στο Kaspersky Security Network.

Έλεγχος των δραστηριοτήτων εφαρμογών στον υπολογιστή και στο δίκτυο

Το στοιχείο Έλεγχος εφαρμογών εμποδίζει τις εφαρμογές από το να εκτελούν ενέργειες που μπορεί να είναι επικίνδυνες για το λειτουργικό σύστημα και ελέγχει την πρόσβαση στους πόρους του λειτουργικού συστήματος (συμπεριλαμβανομένων των πόρων αρχείων που βρίσκονται σε απομακρυσμένους υπολογιστές) και στα προσωπικά δεδομένα σας.

Ο Έλεγχος εφαρμογών παρακολουθεί τις ενέργειες που εκτελούνται στο λειτουργικό σύστημα από εφαρμογές που είναι εγκατεστημένες στον υπολογιστή και τις ρυθμίζει βάσει κανόνων. Αυτοί οι κανόνες περιορίζουν την ύποπτη δραστηριότητα των εφαρμογών, συμπεριλαμβανομένης της πρόσβασης των εφαρμογών σε προστατευμένους πόρους όπως αρχεία και φακέλους, κλειδιά μητρώου και διευθύνσεις δικτύου.

Σε λειτουργικά συστήματα 64 bit, δεν είναι δυνατή η διαμόρφωση των δικαιωμάτων εφαρμογών για τις ακόλουθες ενέργειες:

- Άμεση πρόσβαση σε φυσική μνήμη
- Διαχείριση προγράμματος οδήγησης εκτυπωτή
- Δημιουργία υπηρεσίας
- Ανάγνωση υπηρεσίας
- Επεξεργασία υπηρεσίας
- Αναδιαμόρφωση υπηρεσίας

- Διαχείριση υπηρεσίας
- Έναρξη υπηρεσίας
- Κατάργηση υπηρεσίας
- Πρόσβαση σε εσωτερικά δεδομένα προγράμματος περιήγησης
- Πρόσβαση σε κρίσιμα στοιχεία του λειτουργικού συστήματος
- Πρόσβαση σε χώρο αποθήκευσης κωδικών πρόσβασης
- Ρύθμιση προνομίων εντοπισμού σφαλμάτων
- Χρήση διασυνδέσεων προγραμμάτων του λειτουργικού συστήματος
- Χρήση διασυνδέσεων προγραμμάτων του λειτουργικού συστήματος (DNS)
- Χρήση διασυνδέσεων προγραμμάτων άλλων εφαρμογών
- Αλλαγή λειτουργικών μονάδων συστήματος (KnownDlls)
- Έναρξη προγραμμάτων οδήγησης

Στα Microsoft Windows και 8 Microsoft Windows 10 64 bit, δεν είναι δυνατή η διαμόρφωση των δικαιωμάτων εφαρμογών για τις ακόλουθες ενέργειες:

- Αποστολή μηνυμάτων παραθύρων σε άλλες διεργασίες
- Ύποπτες ενέργειες
- Εγκατάσταση καταγραφέων πληκτρολόγησης (keylogger)
- Υποκλοπή συμβάντων εισερχόμενης ροής
- Δημιουργία στιγμιοτύπων

Η δραστηριότητα δικτύου των εφαρμογών ελέγχεται από το στοιχείο Τείχος προστασίας.

Όταν γίνεται εκκίνηση μιας εφαρμογής στον υπολογιστή για πρώτη φορά, ο Έλεγχος εφαρμογών ελέγχει την ασφάλεια της εφαρμογής και την εντάσσει σε μια ομάδα (Αξιόπιστες, Μη αξιόπιστες, Υψηλού Περιορισμού ή Χαμηλού Περιορισμού). Η ομάδα ορίζει τους κανόνες που πρέπει να εφαρμόζει το Kaspersky Total Security για να ελέγχει τη δραστηριότητα αυτής της εφαρμογής. Το Kaspersky Total Security εκχωρεί εφαρμογές σε ομάδες αξιοπιστίας (Αξιόπιστες, Μη αξιόπιστες, Υψηλού Περιορισμού ή Χαμηλού Περιορισμού) μόνο αν είναι ενεργοποιημένος ο Έλεγχος εφαρμογών ή το Τείχος προστασίας ή και τα δύο αυτά στοιχεία. Αν και τα δύο στοιχεία είναι απενεργοποιημένα, η λειτουργία που εκχωρεί εφαρμογές σε ομάδες αξιοπιστίας δεν λειτουργεί.

Μπορείτε να επεξεργαστείτε τους κανόνες του Ελέγχου εφαρμογών χειροκίνητα.

Οι κανόνες που χρησιμοποιείτε για τις εφαρμογές μεταβιβάζονται στις εξαρτώμενες εφαρμογές. Για παράδειγμα, αν αρνηθείτε κάθε δραστηριότητα δικτύου για το cmd.exe, αυτή η δραστηριότητα δεν θα επιτρέπεται ούτε στο notepad.exe, όταν αυτό θα αρχίσει να χρησιμοποιεί το cmd.exe. Όταν μια εφαρμογή δεν είναι θυγατρική της εφαρμογής από την οποία προέρχεται, οι κανόνες δεν μεταβιβάζονται.

Ξεκινώντας με το Kaspersky Total Security 2021, η λειτουργία Αξιόπιστες εφαρμογές δεν περιλαμβάνεται πλέον στην εφαρμογή. Εάν θέλετε να συνεχίσετε να χρησιμοποιείτε αυτό το στοιχείο, μπορείτε να <u>επιστρέψετε στην προηγούμενη έκδοση της εφαρμογής</u>.

Τρόπος αλλαγής των ρυθμίσεων του Ελέγχου εφαρμογών

Για να αλλάξετε τις ρυθμίσεις Ελέγχου εφαρμογών:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.
- 4. Επιλέξτε το στοιχείο **Έλεγχος εφαρμογών**.
- 5. Στο παράθυρο **Έλεγχος εφαρμογών**, κάντε κλικ στη σύνδεση **Διαχείριση εφαρμογών** για να ανοίξετε το παράθυρο **Διαχείριση εφαρμογών**.
- 6. Επιλέξτε την εφαρμογή που χρειάζεστε στη λίστα και κάντε διπλό κλικ στο όνομά της για να ανοίξετε το παράθυρο **Κανόνες εφαρμογής**.
- 7. Για να διαμορφώσετε τους κανόνες πρόσβασης μιας εφαρμογής στους πόρους του λειτουργικού συστήματος:

- a. Στην καρτέλα Αρχεία και μητρώο συστήματος, επιλέξτε τη σχετική κατηγορία πόρων.
- b. Κάντε κλικ στο εικονίδιο στη στήλη με τη διαθέσιμη ενέργεια για τον πόρο (Ανάγνωση, Εγγραφή, Διαγραφή ή Δημιουργία) για να ανοίξετε το μενού. Στο μενού, επιλέξτε το σχετικό στοιχείο (Μεταβίβαση, Να επιτρέπεται, Επιλογή ενέργειας αυτόματα ή Αποκλεισμός).
- 8. Για να ρυθμίσετε τα δικαιώματα μιας εφαρμογής ως προς την εκτέλεση διαφόρων ενεργειών στο λειτουργικό σύστημα:
 - a. Στην καρτέλα **Δικαιώματα** επιλέξτε τη σχετική κατηγορία δικαιωμάτων.
 - b. Στην στήλη **Ενέργεια**, κάντε κλικ στο εικονίδιο για να ανοίξει το μενού και επιλέξτε το σχετικό στοιχείο (**Μεταβίβαση**, **Να επιτρέπεται**, **Επιλογή ενέργειας αυτόματα** ή **Αποκλεισμός**).
- 9. Για να ρυθμίσετε τα δικαιώματα μιας εφαρμογής ως προς την εκτέλεση διαφόρων ενεργειών στο δίκτυο:
 - a. Στην καρτέλα **Κανόνες δικτύου**, κάντε κλικ στο κουμπί **Προσθήκη**.

Ανοίγει το παράθυρο **Κανόνας δικτύου**.

- b. Στο παράθυρο που ανοίγει, καθορίστε τις απαραίτητες ρυθμίσεις κανόνων και επιλέξτε **Αποθήκευση**.
- c. Εκχωρήστε μια προτεραιότητα στον νέο κανόνα. Για να το κάνετε αυτό, επιλέξτε τον κανόνα και μετακινήστε τον επάνω ή κάτω στη λίστα.
- Για να εξαιρέσετε ορισμένες ενέργειες της εφαρμογής από τους περιορισμούς του Ελέγχου εφαρμογών, στην καρτέλα Εξαιρέσεις επιλέξτε τα πλαίσια ελέγχου που αντιστοιχούν στις ενέργειες που δεν θέλετε να ελέγχονται.
- 11. Κάντε κλικ στο κουμπί **Αποθήκευση**.

Όλες οι εξαιρέσεις που δημιουργούνται στους κανόνες για τις εφαρμογές είναι προσβάσιμες στο παράθυρο ρυθμίσεων του Kaspersky Total Security, στην ενότητα **Απειλές και εξαιρέσεις**.

Ο Έλεγχος εφαρμογών παρακολουθεί και περιορίζει τις ενέργειες της εφαρμογής σύμφωνα με τις ρυθμίσεις που έχουν οριστεί.

Πληροφορίες σχετικά με την προστασία μιας ροής ήχου που προέρχεται από συσκευές εγγραφής ήχου

Οι εισβολείς μπορεί να επιχειρήσουν να αποκτήσουν τη ροή ήχου από τις συσκευές εγγραφής ήχου χρησιμοποιώντας ειδικό λογισμικό. *Συσκευές εγγραφής ήχου* είναι μικρόφωνα που συνδέονται ή είναι ενσωματωμένα στον υπολογιστή και έχουν τη δυνατότητα να μεταδώσουν ροή ήχου μέσω της κάρτας ήχου (σήμα εισόδου). Το Kaspersky Total Security παρακολουθεί ποιες εφαρμογές λαμβάνουν ροή ήχου από συσκευές εγγραφής ήχου και προστατεύει τη ροή ήχου από μη εξουσιοδοτημένες υποκλοπές.

Από προεπιλογή, το Kaspersky Total Security εμποδίζει τις εφαρμογές από τις ομάδες αξιοπιστίας Μη αξιόπιστες και Υψηλού περιορισμού από τη λήψη της ροής ήχου που προέρχεται από τις συσκευές εγγραφής ήχου οι οποίες είναι συνδεδεμένες στον υπολογιστή. Μπορείτε να <u>επιτρέψετε χειροκίνητα στις εφαρμογές να λαμβάνουν ροή ήχου από συσκευές εγγραφής ήχου</u>.

Εάν μια εφαρμογή από την ομάδα αξιοπιστίας Χαμηλού περιορισμού επιχειρήσει να αποκτήσει πρόσβαση σε μια συσκευή εγγραφής ήχου, το Kaspersky Total Security εμφανίζει μια ειδοποίηση και σας ζητά να επιλέξετε εάν θα επιτρέψετε ή όχι στην εν λόγω εφαρμογή να λάβει ροή ήχου από μια συσκευή εγγραφής ήχου. Εάν το Kaspersky Total Security δεν είναι σε θέση να εμφανίσει αυτή την ειδοποίηση (για παράδειγμα όταν το γραφικό περιβάλλον εργασίας του Kaspersky Total Security δεν έχει φορτωθεί ακόμη), τότε στην εφαρμογή από την ομάδα αξιοπιστίας Χαμηλού περιορισμού θα επιτραπεί η λήψη ροής ήχου από μια συσκευή εγγραφής ήχου.

Από προεπιλογή, η λήψη ροής ήχου από συσκευές εγγραφής ήχου επιτρέπεται σε όλες τις εφαρμογές της ομάδας Αξιόπιστες.

Η προστασία ροής ήχου διαθέτει τις ακόλουθες ειδικές λειτουργίες:

- Το στοιχείο Έλεγχος εφαρμογών πρέπει να είναι ενεργοποιημένο για να λειτουργήσει αυτή η δυνατότητα.
- Μετά την αλλαγή των ρυθμίσεων πρόσβασης μιας εφαρμογής στις συσκευές εγγραφής ήχου (για παράδειγμα, όταν έχει απαγορευτεί στην εφαρμογή να λαμβάνει τη ροή ήχου από το παράθυρο ρυθμίσεων Ελέγχου εφαρμογών), η εφαρμογή αυτή πρέπει να επανεκκινηθεί για να σταματήσει η λήψη της ροής ήχου.
- Ο έλεγχος της πρόσβασης στη ροή ήχου από συσκευές εγγραφής ήχου δεν εξαρτάται από τις ρυθμίσεις πρόσβασης στη webcam που έχει μια εφαρμογή.
- Το Kaspersky Total Security προστατεύει την πρόσβαση μόνο σε ενσωματωμένα και εξωτερικά μικρόφωνα. Οι υπόλοιπες συσκευές ροής ήχου δεν υποστηρίζονται.

 Η Kaspersky Total Security επιτρέπει σε μια εφαρμογή να λάβει ροή ήχου και δεν εμφανίζει καμία ειδοποίηση εάν η εφαρμογή ξεκίνησε να λαμβάνει ροή ήχου πριν την εκκίνηση του Kaspersky Total Security ή εάν τοποθετήσατε την εφαρμογή στην ομάδα Μη αξιόπιστες ή Υψηλού Περιορισμού αφού η εφαρμογή ξεκίνησε να λαμβάνει ροή ήχου.

Το Kaspersky Total Security δεν εγγυάται την προστασία της ροής ήχου από συσκευές όπως φωτογραφικές μηχανές DSLR, βιντεοκάμερες και κάμερες δράσης.

Τρόπος αλλαγής των ρυθμίσεων προστασίας ροής ήχου

Για να αλλάξετε τις ρυθμίσεις προστασίας ροής ήχου:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Στο κάτω μέρος του κύριου παραθύρου, κάντε κλικ στο κουμπί Περισσότερα εργαλεία.
 Ανοίγει το παράθυρο Εργαλεία.
- 3. Μεταβείτε στην ενότητα **Διαχείριση εφαρμογών**.
- 4. Κάντε κλικ στη σύνδεση **Έλεγχος εφαρμογών** για να ανοίξετε το παράθυρο **Έλεγχος** εφαρμογών.
- 5. Κάντε κλικ στη σύνδεση **Διαχείριση εφαρμογών** για να ανοίξετε το παράθυρο **Διαχείριση εφαρμογών**.
- 6. Επιλέξτε από τη λίστα την εφαρμογή στην οποία θέλετε να επιτρέψετε την πρόσβαση στις συσκευές εγγραφής ήχου. Κάντε διπλό κλικ στην εφαρμογή για να ανοίξετε το παράθυρο Κανόνες εφαρμογής.
- 7. Στο παράθυρο **Κανόνες εφαρμογής**, μεταβείτε στην καρτέλα **Δικαιώματα**.
- 8. Στη λίστα με τις κατηγορίες δικαιωμάτων, επιλέξτε Τροποποίηση λειτουργικού συστήματος → Ύποπτες τροποποιήσεις στο λειτουργικό σύστημα → Πρόσβαση σε συσκευές εγγραφής ήχου.
- 9. Στη στήλη **Ενέργεια**, κάντε κλικ στο εικονίδιο και επιλέξτε ένα από τα στοιχεία του μενού:
 - Για να επιτρέψετε στην εφαρμογή να λαμβάνει τη ροή ήχου, κάντε κλικ στο Να επιτρέπεται.

- Για να απαγορεύσετε στην εφαρμογή να λαμβάνει τη ροή ήχου, κάντε κλικ στο Αποκλεισμός.
- 10. Για να λαμβάνετε ειδοποιήσεις σχετικά με περιστατικά κατά τα οποία εφαρμογές επιτρέπεται ή δεν επιτρέπεται να έχουν πρόσβαση στη ροή ήχου, στη στήλη Ενέργεια, κάντε κλικ στο εικονίδιο και επιλέξτε Καταγραφή συμβάντων.
- 11. Κάντε κλικ στο κουμπί **Αποθήκευση**.

Τρόπος αλλαγής των ρυθμίσεων της Διαχείρισης εφαρμογών

Για να αλλάξετε τις ρυθμίσεις Διαχείρισης εφαρμογών:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.
- 4. Κάντε κλικ στη σύνδεση **Διαχείριση εφαρμογών** για να ανοίξετε το παράθυρο **Ρυθμίσεις της Διαχείρισης εφαρμογών**.
- 5. Ενεργοποιήστε τον διακόπτη επιλογής **Διαχείριση εφαρμογών** για να εφαρμόσετε τις αλλαγές και να ενεργοποιήσετε το στοιχείο προστασίας Διαχείριση εφαρμογών.
- 6. Στην ομάδα ρυθμίσεων Βοηθός εγκατάστασης, επιλέξτε το πλαίσιο ελέγχου Κατά την εγκατάσταση εφαρμογών, αυτόματη εκκαθάριση πλαισίων ελέγχου για την εγκατάσταση πρόσθετου λογισμικού. Πλαίσιο ελέγχου Προειδοποίηση για τυχόν προσπάθειες εγκατάστασης πρόσθετων προγραμμάτων για αποκλεισμό εγκατάστασης πρόσθετου λογισμικού κατά τη διάρκεια εγκατάστασης νέων εφαρμογών. Εάν αποτραπούν ανεπιθύμητες λειτουργίες κατά τη διάρκεια της εγκατάστασης της νέας εφαρμογής, το Kaspersky Total Security θα σας ενημερώσει σχετικά.

Εάν το πλαίσιο ελέγχου **Κατά την εγκατάσταση εφαρμογών, αυτόματη εκκαθάριση** πλαισίων ελέγχου για την εγκατάσταση πρόσθετου λογισμικού αποεπιλέχθηκε αφότου ξεκινήσατε την εγκατάσταση μιας συγκεκριμένης εφαρμογής, ο βοηθός εγκατάστασης συνεχίζει να εκτελείται για τη διάρκεια της τρέχουσας εγκατάστασης. Τα πλαίσια ελέγχου απέναντι από εφαρμογές που προσφέρουν πρόσθετη εγκατάσταση αποεπιλέγονται και οι πρόσθετες εφαρμογές δεν εγκαθίστανται. Αυτή η λειτουργία θα απενεργοποιηθεί κατά την επόμενη εγκατάσταση. Οι πρόσθετες εφαρμογές θα εγκατασταθούν μαζί με την κύρια εφαρμογή. 7. Επιλέξτε το πλαίσιο ελέγχου Να μην εμφανίζονται βήματα εγκατάστασης που ενδεχομένως να περιέχουν διαφημίσεις και προσφορές για την εγκατάσταση πρόσθετων προγραμμάτων προκειμένου να αποκλείσετε την εμφάνιση των βημάτων εγκατάστασης με διαφημίσεις κατά την εγκατάσταση νέου λογισμικού στον υπολογιστή. Εάν καταργηθούν βήματα αυτής της εγκατάστασης, το Kaspersky Total Security θα σας ενημερώσει σχετικά.

Ενημέρωση εγκατεστημένων εφαρμογών

Αυτή η ενότητα παρέχει πληροφορίες για το πώς μπορείτε να χρησιμοποιείτε το Kaspersky Total Security για να ενημερώνετε εγκατεστημένες εφαρμογές.

Πληροφορίες για την Ενημέρωση λογισμικού

Εάν δεν έχετε ενημερώσει τις εφαρμογές στον υπολογιστή σας για μεγάλο χρονικό διάστημα, αυτές οι εφαρμογές ενδέχεται να περιλαμβάνουν τρωτά σημεία. Τέτοια τρωτά σημεία μπορεί να γίνουν αντικείμενο εκμετάλλευσης από εισβολείς με σκοπό την πρόκληση βλάβης στον υπολογιστή ή σας δεδομένα σας.

Η ενημέρωση των εγκατεστημένων εφαρμογών βελτιώνει την ασφάλεια του υπολογιστή σας. Με το Kaspersky Total Security μπορείτε να πραγματοποιείτε αναζήτηση για ενημερώσεις των εγκατεστημένων εφαρμογών και να κάνετε λήψη και εγκατάσταση των πρόσφατων ενημερώσεων.

Το Kaspersky Total Security διαιρεί τις ενημερώσεις εφαρμογών σε δύο τύπους:

- Σημαντικές ενημερώσεις που διορθώνουν τα τρωτά σημεία των εγκατεστημένων εφαρμογών και που βελτιώνουν την ασφάλεια του υπολογιστή σας.
- Συνιστάται ενημερώσεις που βελτιώνουν τη λειτουργία ή/και που πραγματοποιούν αλλαγές στις εγκατεστημένες εφαρμογές.

Το Kaspersky Total Security πραγματοποιεί τακτικά αναζήτηση για ενημερώσεις. Όταν το Kaspersky Total Security βρει μια νέα ενημέρωση για μια εφαρμογή που είναι εγκατεστημένη στον υπολογιστή σας, θα εμφανίσει μια αναδυόμενη ειδοποίηση στην περιοχή ειδοποιήσεων. Οι πληροφορίες σχετικά με τη διαθεσιμότητα, την ποσότητα και τον τύπο των διαθέσιμων ενημερώσεων εμφανίζονται στο Κέντρο ειδοποιήσεων. Μπορείτε να προβάλετε, να πραγματοποιήσετε λήψη και να <u>εγκαταστήσετε τις διαθέσιμες ενημερώσεις</u> μέσω του Κέντρο ειδοποιήσεων.

Μπορείτε, επίσης, να <u>εκκινήσετε χειροκίνητα την αναζήτηση για ενημερώσεις των</u> <u>εφαρμογών</u>.

Από προεπιλογή, το Kaspersky Total Security πραγματοποιεί αυτόματα λήψη και εγκατάσταση όλων των ενημερώσεων για γνωστές εφαρμογές εφόσον δεν χρειάζεται να αποδεχτείτε τις νέες άδειες χρήσης τελικού χρήστη για αυτές.

Στα Windows 8 και σε νεότερες εκδόσεις, το Kaspersky Total Security διακόπτει προσωρινά τις ενημερώσεις της εφαρμογής όταν χρησιμοποιείται σύνδεση στο Διαδίκτυο με ογκοχρέωση. Η λήψη των ενημερώσεων συνεχίζεται μόλις επαναφερθεί η απεριόριστη σύνδεση. Εάν κάνατε χειροκίνητα εκκίνηση της ενημέρωσης, η εφαρμογή θα πραγματοποιήσει λήψη της ενημέρωσης ανεξάρτητα από το αν χρησιμοποιείτε ή όχι μια περιορισμένη σύνδεση.

Ενδεχομένως να χρειαστείτε δικαιώματα διαχειριστή στον υπολογιστή για να ενημερώσετε συγκεκριμένες εφαρμογές.

Εφαρμογές που δεν επιθυμείτε να ενημερωθούν ή για τις οποίες δεν θέλετε να εγκατασταθούν μεμονωμένες ενημερώσεις το Kaspersky Total Security τις τοποθετεί στη λίστα εξαιρέσεων. Μπορείτε να <u>προβάλετε και να επεξεργαστείτε τη λίστα εξαιρέσεων</u>.

Πριν ξεκινήσετε την πρώτη αναζήτηση για ενημερώσεις των εφαρμογών, το Kaspersky Total Security ενδεχομένως να ζητήσει ενημέρωση των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής.

Τρόπος αλλαγής των ρυθμίσεων της Ενημέρωσης λογισμικού

Για να αλλάξετε τις ρυθμίσεις της Ενημέρωσης λογισμικού:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Στην ενότητα **Προστασία**, επιλέξτε το στοιχείο Ενημέρωση λογισμικού.

Ανοίγει το παράθυρο **Ρυθμίσεις της Ενημέρωσης λογισμικού**.

4. Εάν δεν επιθυμείτε το Kaspersky Total Security να πραγματοποιεί αυτόματα λήψη και εγκατάσταση των ενημερώσεων της εφαρμογής για τις οποίες δεν απαιτείται αποδοχή μιας νέας άδειας χρήσης τελικού χρήστη, αποεπιλέξτε το πλαίσιο ελέγχου Αυτόματη λήψη και εγκατάσταση των ενημερώσεων εάν δεν χρειάζεται να αποδεχτείτε τις νέες άδειες χρήσης.

Αυτό το πλαίσιο ελέγχου είναι επιλεγμένο από προεπιλογή.

5. Στην ενότητα **Αναζήτηση για ενημερώσεις της εφαρμογής**, επιλέξτε ποιες ενημερώσεις των εφαρμογών θέλετε να καταφορτώσει και να εγκαταστήσει το Kaspersky Total
Security:

- Επιλέξτε το Σημαντικές ενημερώσεις που βελτιώνουν την ασφάλεια του υπολογιστή εάν θέλετε το Kaspersky Total Security να εγκαταστήσει μόνο τις σημαντικές ενημερώσεις που διορθώνουν τα τρωτά σημεία λογισμικού του υπολογιστή και που βελτιώνουν την ασφάλεια του υπολογιστή σας.
- Επιλέξτε το Όλες οι ενημερώσεις για γνωστές εφαρμογές εάν θέλετε το Kaspersky Total Security να εγκαταστήσει όλες τις ενημερώσεις λογισμικού.

Αναζήτηση για ενημερώσεις της εφαρμογής

Για να εκκινήσετε μια αναζήτηση για ενημερώσεις της εφαρμογής:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί Περισσότερα εργαλεία.
 Ανοίγει το παράθυρο Εργαλεία.
- 3. Μεταβείτε στην ενότητα **Διαχείριση εφαρμογών**.
- 4. Κάντε κλικ στη σύνδεση **Ενημέρωση λογισμικού** για να ανοίξει το παράθυρο **Ενημέρωση λογισμικού**.
- 5. Κάντε κλικ στο κουμπί **Έναρξη σάρωσης**.

Αυτό εκκινεί την αναζήτηση για ενημερώσεις της εφαρμογής. Τα αποτελέσματα της αναζήτησης εμφανίζονται στο παράθυρο.

Πώς να ρυθμίσετε τις παραμέτρους της λειτουργίας αναζήτησης ενημερώσεων

Για να ρυθμίσετε τις παραμέτρους λειτουργίας της αναζήτησης για ενημερώσεις για εγκατεστημένες εφαρμογές:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί 🧔.
- 3. Επιλέξτε την ενότητα **Προστασία**.

4. Επιλέξτε το στοιχείο Ενημέρωση λογισμικού.

Ανοίγει το παράθυρο **Ρυθμίσεις της Ενημέρωσης λογισμικού**.

- 5. Στην ενότητα **Ενημέρωση**, επιλέξτε το πλαίσιο ελέγχου **Ενεργοποίηση αναζήτησης για ενημερώσεις της εφαρμογής**.
- 6. Κάντε κλικ στη σύνδεση **Ρύθμιση λειτουργίας αναζήτησης για ενημερώσεις** για να μεταβείτε στο παράθυρο **Ενημέρωση λειτουργίας αναζήτησης**.
- 7. Στην αναπτυσσόμενη λίστα Αναζήτηση για ενημερώσεις, επιλέξτε ένα από τα ακόλουθα στοιχεία:
 - Αυτόματα. Εάν επιλέξετε αυτό το στοιχείο, το Kaspersky Total Security θα εκτελεί μια αναζήτηση για ενημερώσεις εφαρμογής τουλάχιστον μία φορά κάθε 24 ώρες σύμφωνα με τις εσωτερικές ρυθμίσεις της εφαρμογής.
 - Κάθε λεπτό/Κάθε ώρα/Κάθε ημέρα/Εβδομαδιαία / Κάθε μήνα/Σε καθορισμένη ώρα. Εάν ορίσετε μία από αυτές τις επιλογές, το Kaspersky Total Security θα αναζητά ενημερώσεις βάσει του καθορισμένου χρονοδιαγράμματός σας έως το ακριβές λεπτό.
 Όταν έχει ενεργοποιηθεί μία από αυτές τις επιλογές, είναι διαθέσιμο το πλαίσιο ελέγχου Αναβολή εκτέλεσης μετά την εκκίνηση της εφαρμογής για Ν λεπτά.
 - Μετά την εκκίνηση της εφαρμογής. Μετά την εκκίνηση του Kaspersky Total Security, θα εκτελεί αναζήτηση για ενημερώσεις της εφαρμογής μετά από αναμονή για τον αριθμό των λεπτών που υποδεικνύονται στο πεδίο Έναρξη σε Ν λεπτά.
 - Έπειτα από κάθε ενημέρωση. Το Kaspersky Total Security θα εκτελεί αναζήτηση για ενημερώσεις της εφαρμογής μετά τη λήψη και εγκατάσταση ενός νέου πακέτου ενημέρωσης για το Kaspersky Total Security.
- 8. Επιλέξτε το πλαίσιο ελέγχου Αναζήτηση για ενημερώσεις την επόμενη ημέρα εάν ο υπολογιστής είναι απενεργοποιημένος για να εκκινηθεί η αναζήτηση μόλις ο υπολογιστής τεθεί σε λειτουργία μετά την παράλειψη μιας προγραμματισμένης αναζήτησης. Εάν δεν έχει επιλεγεί το πλαίσιο ελέγχου, η εφαρμογή θα εκκινήσει την αναζήτηση για ενημερώσεις μόνο κατά την προγραμματισμένη ώρα με τον υπολογιστή σε λειτουργία.
- 9. Επιλέξτε το πλαίσιο ελέγχου Αναζήτηση για ενημερώσεις εφαρμογών μόνο όταν η προστασία οθόνης είναι ενεργή ή όταν ο υπολογιστής είναι κλειδωμένος για να εκκινήσετε αναζήτηση για ενημερώσεις μόνο εάν δεν εργάζεστε στον υπολογιστή και για να μην επιβαρύνετε περισσότερο τους πόρους του υπολογιστή ενώ εργάζεστε. Εάν δεν έχει επιλεγεί το πλαίσιο ελέγχου, η εφαρμογή θα εκκινήσει την αναζήτηση κατά την προγραμματισμένη ώρα ανεξάρτητα εάν εργάζεστε στον υπολογιστή.

10. Για να αποθηκεύσετε τις ρυθμίσεις, κάντε κλικ στο κουμπί **Αποθήκευση**.

Προβολή της λίστας ενημερώσεων των εφαρμογών

To Kaspersky Total Security πραγματοποιεί τακτικά αναζητήσεις για ενημερώσεις των εφαρμογών που είναι εγκατεστημένες στον υπολογιστή σας. Οι πληροφορίες σχετικά με τον αριθμό και τον τύπο των ενημερώσεων που είναι διαθέσιμες για τις εφαρμογές μπορεί να προβληθούν στο Κέντρο ειδοποιήσεων.

Για να δείτε τη λίστα που δημιουργείται με βάση τα αποτελέσματα της αναζήτησης για ενημερώσεις εφαρμογών:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί Λεπτομέρειες που βρίσκεται στο πάνω μέρος του παραθύρου.
 Αυτό ανοίγει το παράθυρο Κέντρο ειδοποιήσεων.
- 3. Στην ενότητα **Προστασία**, κάντε κλικ στο κουμπί **Εμφάνιση** στη γραμμή με το μήνυμα σχετικά με τις ενημερώσεις των εφαρμογών.

Αυτό ανοίγει το παράθυρο **Ενημέρωση λογισμικού** με μια λίστα των διαθέσιμων ενημερώσεων των εφαρμογών.

- 4. Για να ενημερώσετε όλες τις εφαρμογές που εμφανίζονται στη λίστα, κάντε κλικ στο κουμπί **Ενημέρωση όλων** (δεν είναι διαθέσιμο σε όλες τις περιοχές).
- 5. Για να ενημερώσετε επιλεκτικά συγκεκριμένες εφαρμογές, εκτελέστε μια από τις ακόλουθες ενέργειες:
 - Κάντε κλικ στο κουμπί Ενημέρωση στη γραμμή που περιέχει την εφαρμογή που θέλετε να ενημερώσετε.

Σας συνιστούμε να διαβάσετε την άδεια χρήσης τελικού χρήστη πριν ενημερώσετε την εφαρμογή. Οι άδειες χρήσης τελικού χρήστη είναι διαθέσιμες στην αναπτυσσόμενη λίστα **Άδειες χρήσης**. Από προεπιλογή, η γλώσσα της άδειας χρήσης τελικού χρήστη αντιστοιχεί στη γλώσσα του περιβάλλοντος εργασίας της εφαρμογής. Εάν η άδεια χρήσης τελικού χρήστη δεν είναι διαθέσιμη στη γλώσσα του περιβάλλοντος εργασίας της εφαρμογής, το κείμενο της EULA (Άδεια Χρήσης Τελικού Χρήστη) παρέχεται στη γλώσσα του περιβάλλοντος εργασίας του Kaspersky Total Security. Σε όλες τις άλλες περιπτώσεις, το κείμενο της άδειας χρήσης τελικού χρήστη παρέχεται στα Αγγλικά ή στην πρώτη διαθέσιμη γλώσσα εάν το αγγλικό κείμενο δεν είναι διαθέσιμο.

Κάντε κλικ στο κουμπί για να ανοίξετε το μενού και επιλέξτε το Να μην ενημερωθεί αυτή η εφαρμογή εάν θέλετε να σταματήσει να σας ειδοποιεί το Kaspersky Total Security σχετικά με διαθέσιμες ενημερώσεις για την επιλεγμένη εφαρμογή.

Η επιλεγμένη εφαρμογή προστίθεται στη <u>λίστα εξαιρέσεων</u>. Το Kaspersky Total Security σταματά να δείχνει ειδοποιήσεις σχετικά με τις νέες ενημερώσεις που είναι διαθέσιμες για τη συγκεκριμένη εφαρμογή.

 Κάντε κλικ στο κουμπί για να ανοίξετε το μενού και επιλέξτε το Παράλειψη αυτής της ενημέρωσης εάν θέλετε να σταματήσει να σας ειδοποιεί το Kaspersky Total Security σχετικά με την επιλεγμένη ενημέρωση.

Η επιλεγμένη ενημέρωση της εφαρμογής μετακινείται στη λίστα εξαιρέσεων. Το Kaspersky Total Security εμφανίζει μια ειδοποίηση σχετικά με μια νέα ενημέρωση που είναι διαθέσιμη για τη συγκεκριμένη εφαρμογή.

Κάντε κλικ στο κουμπί για να ανοίξετε το μενού και επιλέξτε Άνοιγμα της τοποθεσίας web του πωλητή εάν θέλετε να πραγματοποιήσετε χειροκίνητα τη λήψη και εγκατάσταση της ενημέρωσης για την επιλεγμένη εφαρμογή.

Το προεπιλεγμένο πρόγραμμα περιήγησης του λειτουργικού συστήματος ανοίγει τον δικτυακό τόπο του πωλητή του λογισμικού. Μπορείτε να προβάλετε την ενημέρωση στον δικτυακό τόπο και να την καταφορτώσετε χειροκίνητα.

Το περιβάλλον εργασίας του παραθύρου, η Ενημέρωση λογισμικού και η προβολή της Άδειας Χρήσης Τελικού Χρήστη μπορεί να διαφέρουν ανάλογα με τη γλώσσα τοπικής προσαρμογής του Kaspersky Total Security.

Κατάργηση ενημέρωσης ή εφαρμογής από τη λίστα εξαιρέσεων

<u>Κατά την προβολή της λίστας ενημερώσεων των εφαρμογών</u> μπορείτε να παραλείψετε ειδοποιήσεις για μεμονωμένες ενημερώσεις ή να παραλείψετε ειδοποιήσεις για όλες τις ενημερώσεις συγκεκριμένων εφαρμογών. Το Kaspersky Total Security προσθέτει αυτές τις ενημερώσεις και τις εφαρμογές στη λίστα εξαιρέσεων.

Για να καταργήσετε μια ενημέρωση ή εφαρμογή από τη λίστα εξαιρέσεων:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- Στην ενότητα Προστασία, επιλέξτε το στοιχείο Ενημέρωση λογισμικού.
 Ανοίγει το παράθυρο Ρυθμίσεις της Ενημέρωσης λογισμικού.
- 4. Κάντε κλικ στη σύνδεση **Εξαιρέσεις** για να ανοίξετε το παράθυρο **Εξαιρέσεις**.

Η λίστα **Εξαιρέσεις** περιλαμβάνει τις εφαρμογές και ενημερώσεις για τις οποίες έχετε υποδείξει ότι δεν απαιτούνται ενημερώσεις, καθώς και μεμονωμένες ενημερώσεις εφαρμογών που δεν εγκαταστήσατε.

5. Επιλέξτε την ενημέρωση ή εφαρμογή στη λίστα και κάντε κλικ στο κουμπί **Κατάργηση από τη λίστα**.

Κατά τη διάρκεια της επόμενης αναζήτησης για ενημερώσεις, το Kaspersky Total Security θα σας ενημερώσει για τη διαθεσιμότητα των ενημερώσεων για εφαρμογές που έχετε καταργήσει από τη λίστα εξαιρέσεων.

Κατάργηση μη συμβατών εφαρμογών

Αυτή η ενότητα περιλαμβάνει πληροφορίες σχετικά με τον τρόπο με τον οποίο το Kaspersky Total Security μπορεί να σας βοηθήσει να διαγράψετε από τον υπολογιστή σας μη συμβατές εφαρμογές με το Kaspersky Total Security.

Σχετικά με την κατάργηση μη συμβατών εφαρμογών

To Kaspersky Total Security ελέγχει τακτικά αν υπάρχουν μη συμβατές εφαρμογές 😨 στον υπολογιστή σας. Όταν βρεθεί μια τέτοια εφαρμογή, το Kaspersky Total Security την προσθέτει στη λίστα των μη συμβατών εφαρμογών. Μπορείτε να δείτε τη λίστα και να αποφασίσετε τι θα κάνετε με τις μη συμβατές εφαρμογές.

Συνιστάται να διαγράψετε τις μη συμβατές εφαρμογές από τον υπολογιστή σας. Διαφορετικά, το Kaspersky Total Security δεν θα μπορεί να προστατεύσει πλήρως τον υπολογιστή σας.

Οι παρακάτω είναι μερικοί από τους λόγους για τους οποίους μια εφαρμογή τρίτου μέρους ενδέχεται να μην είναι συμβατή με το Kaspersky Total Security:

- Η εφαρμογή έρχεται σε διένεξη με την Προστασία αρχείων από ιούς.
- Η εφαρμογή έρχεται σε διένεξη με το Τείχος προστασίας.
- Η εφαρμογή έρχεται σε διένεξη με το Πρόγραμμα Anti-Spam.
- Η εφαρμογή παρεμβαίνει στην προστασία της κυκλοφορίας του δικτύου.
- Η εφαρμογή έρχεται σε διένεξη με την Κρυπτογράφηση δεδομένων.
- Η εφαρμογή έρχεται σε διένεξη με το Kaspersky Password Manager.

Πώς να καταργήσετε την εγκατάσταση των μη συμβατών εφαρμογών

Για να καταργήσετε μη συμβατές εφαρμογές, ακολουθήστε τα εξής βήματα:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί Λεπτομέρειες που βρίσκεται στο πάνω μέρος του παραθύρου.
 Αυτό ανοίγει το παράθυρο Κέντρο ειδοποιήσεων.
- 3. Στην ενότητα **Συστάσεις**, κάντε κλικ στο κουμπί **Εμφάνιση** στη γραμμή που περιέχει το μήνυμα σχετικά με τις εντοπισμένες μη συμβατές εφαρμογές.

Αυτό ανοίγει το παράθυρο **Μη συμβατό λογισμικό** που περιέχει μια λίστα με τις εντοπισμένες ασυμβίβαστες εφαρμογές που το Kaspersky Total Security μπορεί να καταργήσει.

4. Επιλέξτε τα πλαίσια ελέγχου δίπλα στα ονόματα των μη συμβατών εφαρμογών που πρέπει να καταργήσετε και κάντε κλικ στην επιλογή Κατάργηση. Το Kaspersky Total Security θα καταργήσει τις υποδεικνυόμενες εφαρμογές από τον υπολογιστή σας. Το Kaspersky Total Security καταργεί εφαρμογές χρησιμοποιώντας τα εργαλεία κατάργησης που αυτές παρέχουν. Κατά τη διαδικασία κατάργησης, μπορεί να σας ζητηθεί να συναινέσετε στην κατάργηση ή την τροποποίηση των ρυθμίσεων που αφορούν την κατάργηση εφαρμογών.

- 5. Εάν ο υπολογιστής εξακολουθεί να έχει μη συμβατές εφαρμογές τις οποίες το Kaspersky Total Security δεν θα καταργήσει, ανοίγει ένα παράθυρο που εμφανίζει μια λίστα με αυτές τις εφαρμογές. Για να καταργήσετε μη συμβατές εφαρμογές με μη αυτόματο τρόπο, κάντε κλικ στο στοιχείο **Κατάργηση μη αυτόματα**. Αυτό ανοίγει το τυπικό παράθυρο του λειτουργικού συστήματος που περιέχει μια λίστα των εγκατεστημένων εφαρμογών. Αφαιρέστε τις μη συμβατές εφαρμογές σύμφωνα με τις οδηγίες για το λειτουργικό σας σύστημα.
- 6. Αφού καταργήσετε τις μη συμβατές εφαρμογές, επανεκκινήστε τον υπολογιστή.

Εκκαθάριση λογισμικού υπολογιστή

Αυτή η ενότητα παρέχει πληροφορίες σχετικά με το πώς να χρησιμοποιείτε το Kaspersky Total Security για να εντοπίζετε εφαρμογές και επεκτάσεις προγραμμάτων περιήγησης που πιθανόν να θέλετε να καταργήσετε από τον υπολογιστή σας.

Σχετικά με την Εκκαθάριση λογισμικού υπολογιστή

Χρησιμοποιώντας το Kaspersky Total Security, μπορείτε να πραγματοποιήσετε αναζήτηση στον υπολογιστή σας για εφαρμογές και επεκτάσεις προγραμμάτων περιήγησης που πιθανόν να θέλετε να καταργήσετε. Για παράδειγμα, αυτές θα μπορούσαν να είναι εφαρμογές και επεκτάσεις προγραμμάτων περιήγησης που εγκαταστάθηκαν χωρίς τη συγκατάθεσή σας ή εφαρμογές και επεκτάσεις που χρησιμοποιείτε σπάνια.

To Kaspersky Total Security αναλύει τακτικά εφαρμογές και επεκτάσεις προγραμμάτων περιήγησης που είναι εγκατεστημένα στον υπολογιστή σας για να προσδιορίσει πιθανές αιτίες για την κατάργησή τους, και <u>κατηγοριοποιεί</u> τις εφαρμογές και επεκτάσεις προγραμμάτων περιήγησης που εντοπίζονται.

Μπορείτε να εκτελέσετε <u>χειροκίνητα</u> μια ανάλυση των εγκατεστημένων εφαρμογών και επεκτάσεων προγραμμάτων περιήγησης ή <u>να ρυθμίσετε τις παραμέτρους μιας</u> <u>προγραμματισμένης ανάλυσης</u>.

Οι πληροφορίες σχετικά με τις εντοπισμένες εφαρμογές και επεκτάσεις προγραμμάτων περιήγησης εμφανίζονται στο παράθυρο **Κέντρο ειδοποιήσεων**. Μπορείτε να προχωρήσετε σε προβολή της <u>λίστας εντοπισμένων αντικειμένων</u> από το Κέντρο ειδοποιήσεων.

Οι εφαρμογές και επεκτάσεις που επιθυμείτε να διατηρήσετε μπορούν να προστεθούν στη λίστα εξαιρέσεων. Μπορείτε να <u>προβάλετε και να επεξεργαστείτε τη λίστα εξαιρέσεων</u>.

Μπορείτε να κάνετε κλικ στη σύνδεση **Αναφορά ενοχλητικής εφαρμογής** για να αποστείλετε δεδομένα στην Kaspersky σχετικά με εφαρμογές που σας προκαλούν πρόβλημα.

Πώς να εκκινήσετε χειροκίνητα μια ανάλυση αντικειμένων

Για να εκκινήσετε χειροκίνητα μια ανάλυση αντικειμένων:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί Περισσότερα εργαλεία.
 Ανοίγει το παράθυρο Εργαλεία.
- 3. Στο παράθυρο **Εργαλεία**, μεταβείτε στην ενότητα **Εκκαθάριση και βελτιστοποίηση**.
- 4. Κάντε κλικ στη σύνδεση **Εκκαθάριση υπολογιστή** για να μεταβείτε στο παράθυρο **Εκκαθάριση υπολογιστή**.
- 5. Στο παράθυρο, κάντε κλικ στο κουμπί **Εκτέλεση**.

Ξεκινά ανάλυση αντικειμένων. Οι πληροφορίες για τα αποτελέσματα της ανάλυσης εμφανίζονται στο παράθυρο με τη μορφή συνδέσμου με λίστες εντοπισμένων εφαρμογών και επεκτάσεων προγραμμάτων περιήγησης. Κάντε κλικ στη σύνδεση για να μεταβείτε στη λίστα εντοπισμένων αντικειμένων.

Πώς να ρυθμίσετε τις παραμέτρους σε προγραμματισμένη ανάλυση

Για να ρυθμίσετε τις παραμέτρους σε προγραμματισμένη ανάλυση των εγκατεστημένων εφαρμογών και επεκτάσεων προγράμματος περιήγησης:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί 🤯.

Ανοίγει το παράθυρο **Ρυθμίσεις**.

- 3. Επιλέξτε την ενότητα **Προστασία**.
- 4. Επιλέξτε το στοιχείο Διαχείριση εφαρμογών.

Ανοίγει το παράθυρο **Ρυθμίσεις της Διαχείρισης εφαρμογών**.

- 5. Στην ενότητα **Εκκαθάριση υπολογιστή**, επιλέξτε το πλαίσιο ελέγχου **Ανάλυση** εγκατεστημένων εφαρμογών και επεκτάσεων του προγράμματος περιήγησης.
- 6. Κάντε κλικ στη σύνδεση **Ρύθμιση παραμέτρων χρονοδιαγράμματος** για να ανοίξετε το παράθυρο **Χρονοδιάγραμμα**.
- 7. Στην αναπτυσσόμενη λίστα Εκτέλεση ανάλυσης, επιλέξτε ένα από τα ακόλουθα στοιχεία:
 - Αυτόματα. Εάν επιλέξετε αυτό το στοιχείο, το Kaspersky Total Security θα εκτελεί ανάλυση μία φορά κάθε 24 ώρες την ώρα που έχει οριστεί από προεπιλογή.
 - Κάθε λεπτό/Κάθε ώρα/Κάθε ημέρα/Εβδομαδιαία / Κάθε μήνα/Σε καθορισμένη ώρα. Εάν ορίσετε μία από αυτές τις επιλογές, το Kaspersky Total Security θα εκτελέσει μια ανάλυση βάσει του καθορισμένου χρονοδιαγράμματός σας έως το ακριβές λεπτό.
 Όταν έχει ενεργοποιηθεί μία από αυτές τις επιλογές, είναι διαθέσιμο το πλαίσιο ελέγχου Αναβολή εκτέλεσης μετά την εκκίνηση της εφαρμογής για Ν λεπτά.
 - Μετά την εκκίνηση της εφαρμογής. Μετά την εκκίνηση του Kaspersky Total Security, θα εκτελεί μια ανάλυση μετά από αναμονή για τον αριθμό των λεπτών που υποδεικνύονται στο πεδίο Έναρξη σε Ν λεπτά.
 - Έπειτα από κάθε ενημέρωση. Το Kaspersky Total Security θα εκτελεί μια ανάλυση μετά τη λήψη και την εγκατάσταση ενός νέου πακέτου ενημέρωσης.
- 8. Επιλέξτε το πλαίσιο ελέγχου Εκτέλεση ανάλυσης αντικειμένων την επόμενη ημέρα εάν ο υπολογιστής είναι απενεργοποιημένος για να εκτελέσετε ανάλυση όταν ο υπολογιστής είναι ενεργοποιημένος εάν δεν πραγματοποιήθηκε κάποια προγραμματισμένη ανάλυση. Εάν δεν έχει επιλεγεί το πλαίσιο ελέγχου, η εφαρμογή θα εκτελέσει την ανάλυση μόνο κατά την προγραμματισμένη ώρα ενώ ο υπολογιστής είναι ενεργοποιημένος.
- 9. Επιλέξτε το πλαίσιο ελέγχου Εκτέλεση ανάλυσης αντικειμένων μόνο όταν η προστασία οθόνης είναι ενεργή ή όταν ο υπολογιστής είναι κλειδωμένος για να εκτελέσετε ανάλυση αντικειμένων μόνο εάν δεν εργάζεστε στον υπολογιστή και για να μην επιβαρύνετε περισσότερο τους πόρους του υπολογιστή ενώ εργάζεστε. Εάν δεν έχει επιλεγεί το πλαίσιο ελέγχου, η εφαρμογή θα εκτελέσει την ανάλυση κατά την προγραμματισμένη ώρα ανεξάρτητα εάν εργάζεστε στον υπολογιστή.
- 10. Για να αποθηκεύσετε τις αλλαγές στις ρυθμίσεις, κάντε κλικ στο κουμπί **Αποθήκευση**.

Πώς να επιλέξετε κατηγορίες αντικειμένων για ανάλυση

Για να επιλέξετε κατηγορίες αντικειμένων που εντοπίσθηκαν κατά την ανάλυση:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί 🥸.

Ανοίγει το παράθυρο **Ρυθμίσεις**.

- 3. Επιλέξτε την ενότητα **Προστασία**.
- 4. Επιλέξτε **Διαχείριση εφαρμογών**.

Ανοίγει το παράθυρο **Ρυθμίσεις της Διαχείρισης εφαρμογών**.

- 5. Κάντε κλικ στη σύνδεση **Επιλογή κατηγοριών για αντικείμενα** για να μεταβείτε στο παράθυρο **Κατηγορίες αντικειμένων**.
- 6. Πραγματοποιήστε τις ακόλουθες ενέργειες:
 - Για να διενεργήσετε ανάλυση των εγκατεστημένων εφαρμογών, επιλέξτε το πλαίσιο ελέγχου Εφαρμογές.
 - Για να διενεργήσετε ανάλυση των εγκατεστημένων επεκτάσεων προγράμματος περιήγησης, επιλέξτε το πλαίσιο ελέγχου Επεκτάσεις προγράμματος περιήγησης.
- 7. Επιλέξτε τις κατηγορίες εφαρμογών και επεκτάσεων προγράμματος περιήγησης που θέλετε να βρείτε και πιθανόν καταργήσετε. Για να το κάνετε αυτό, επιλέξτε τα πλαίσια ελέγχου απέναντι από τις επιλεγμένες κατηγορίες.
- 8. Κάντε κλικ στο κουμπί **Αποθήκευση**.

Κατηγορίες αντικειμένων που εντοπίστηκαν

Αυτές οι κατηγορίες περιγράφονται στον πίνακα παρακάτω.

Κατηγορίες εφαρμογών

Κατηγορία εφαρμογών και επεκτάσεων προγραμμάτων περιήγησης Περιγραφή

Παροχή εσφαλμένων πληροφοριών	Σύμφωνα με την Kaspersky*, η εφαρμογή ή επέκταση προγράμματος περιήγησης σάς παρέχει εσφαλμένες πληροφορίες σχετικά με την κατάσταση του λειτουργικού συστήματος ή τις εγκατεστημένες εφαρμογές προκειμένου να σας προτρέψει να αγοράσετε και να εγκαταστήσετε άλλες εφαρμογές προς το συμφέρον του πωλητή.
Εγκαταστάθηκε χωρίς τη συγκατάθεσή σας	Σύμφωνα με την Kaspersky*, η εφαρμογή ή επέκταση προγράμματος περιήγησης εγκαταστάθηκε στον υπολογιστή σας χωρίς τη ρητή συγκατάθεσή σας που παρέχεται σε ηλεκτρονική μορφή.
Εμφάνιση ανώνυμων μηνυμάτων ή διαφημιστικών πλαισίων	Σύμφωνα με την Kaspersky*, η εφαρμογή ή επέκταση προγράμματος περιήγησης εμφανίζει, με ανωνυμία, μηνύματα και ειδοποιήσεις στον υπολογιστή σας.
Επιβράδυνση της εκκίνησης του υπολογιστή	Σύμφωνα με την Kaspersky*, η εφαρμογή ή επέκταση προγράμματος περιήγησης εκκινείται αυτόματα κατά την εκκίνηση του λειτουργικού συστήματος χωρίς τη ρητή συγκατάθεσή σας.
Ακούσια εγκατάσταση	Σύμφωνα με την Kaspersky*, η εγκατάσταση της εφαρμογής ή της επέκτασης προγράμματος περιήγησης σας επιβλήθηκε, για παράδειγμα, μέσω αποκλεισμού του προγράμματος περιήγησης ή του λειτουργικού συστήματος.
Απόκρυψη της λειτουργίας τους	Σύμφωνα με την Kaspersky*, η εφαρμογή ή η επέκταση προγράμματος περιήγησης αποκρύβει τη λειτουργία της από εσάς: π.χ., δεν έχει ορατά παράθυρα και δεν εμφανίζει κάποιο εικονίδιο στην περιοχή ειδοποιήσεων της γραμμής εργασιών.
Δεν υποστηρίζεται από πωλητή και περιέχει τρωτά σημεία	Ο πωλητής δεν υποστηρίζει πλέον την παρούσα εφαρμογή ή επέκταση προγράμματος περιήγησης και δεν διαθέτει στην αγορά ενημερώσεις ή επιδιορθώσεις τρωτών σημείων.
Απόκρυψη μηχανισμών που χρησιμοποιούνται για το κλείσιμό τους	Σύμφωνα με την Kaspersky*, η εφαρμογή ή επέκταση προγράμματος περιήγησης κρύβει ή/και περιορίζει τους μηχανισμούς που ενδεχομένως χρησιμοποιείτε για να κλείσετε το παράθυρο της εφαρμογής, για να πραγματοποιήσετε έξοδο από την εφαρμογή ή για να καταργήσετε αυτήν την εφαρμογή από τον υπολογιστή σας.
Εγκατάσταση μαζί	Σύμφωνα με την Kaspersky, η εφαρμογή ή επέκταση

με άλλη εφαρμογή	προγράμματος περιήγησης εγκαταστάθηκε στον υπολογιστή σας μαζί με μια άλλη εφαρμογή. Η εφαρμογή ή επέκταση προγράμματος περιήγησης ίσως να εγκαταστάθηκε κατά λάθος ή μπορεί να μην δώσατε τη συγκατάθεσή σας για την εγκατάστασή της.
Χρησιμοποιείται	Σύμφωνα με την Kaspersky, δεν έχει εκκινηθεί η εφαρμογή εδώ και
σπάνια	περισσότερες από <n> ημέρες.</n>
Συλλογή και	Σύμφωνα με την Kaspersky, η εφαρμογή ή επέκταση
μετάδοση των	προγράμματος περιήγησης μπορεί να συλλέξει και να μεταδώσει
δεδομένων σας	τα δεδομένα σας χωρίς τη ρητή σας συναίνεση.
Ανακατεύθυνση ή αποκλεισμός κυκλοφορίας	Σύμφωνα με την Kaspersky, η εφαρμογή ή επέκταση προγράμματος περιήγησης μπορεί να ανακατευθύνει ή αποκλείσει κυκλοφορία δικτύου (π.χ. τα ερωτήματα αναζήτησης που υποβάλλεται στο web). Μπορεί επίσης να προσπελάσει δικτυακούς τόπους ή να τροποποιήσεις ιστοσελίδες δίχως να σας ενημερώσει.
Αλλαγή ρυθμίσεων προγράμματος περιήγησης/ΛΣ	Σύμφωνα με την Kaspersky, η εφαρμογή ή επέκταση προγράμματος περιήγησης μπορεί να τροποποιήσει ρυθμίσεις στο πρόγραμμα περιήγησης ή το λειτουργικό σύστημα (π.χ., την προτιμώμενη μηχανή αναζήτησης ή την αρχική σελίδα στο πρόγραμμα περιήγησης) χωρίς τη ρητή σας συναίνεση.
Περιορισμός	Σύμφωνα με την Kaspersky, η εφαρμογή ή επέκταση
δυνατότητων για	προγράμματος περιήγησης μπορεί να περιορίσει τις δυνατότητές
τροποποίηση	σας για προβολή και αλλαγή ρυθμίσεων στο πρόγραμμα
ρυθμίσεων	περιήγησης ή το λειτουργικό σύστημα.
Αλλαγή	Σύμφωνα με την Kaspersky, η εφαρμογή ή επέκταση
συμπεριφοράς	προγράμματος περιήγησης μπορεί να αλλάξει τη συμπεριφορά του
στο πρόγραμμα	προγράμματος περιήγησης όταν γίνεται εγκατάσταση, κατάργηση
περιήγησης	ή εκτέλεση, ή όταν είναι απενεργοποιούνται οι επεκτάσεις.

* Σύμφωνα με τις πληροφορίες που είναι διαθέσιμες στην Kaspersky, η εφαρμογή ή επέκταση προγράμματος περιήγησης εκτελεί τυπικά τις ενέργειες που περιγράφονται στον πίνακα. Η Kaspersky Total Security δεν ελέγχει εάν αυτές οι ενέργειες εκτελέστηκαν ή όχι στην πραγματικότητα στον υπολογιστή σας.

Προβολή της λίστας εντοπισμένων αντικειμένων

Για να δείτε τη λίστα που δημιουργείται με βάση τα αποτελέσματα της ανάλυσης αντικειμένων:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί Λεπτομέρειες που βρίσκεται στο πάνω μέρος του παραθύρου.
 Αυτό ανοίγει το παράθυρο Κέντρο ειδοποιήσεων.
- Στην ενότητα Συστάσεις, κάντε κλικ στο κουμπί Εμφάνιση στη γραμμή που περιέχει το μήνυμα σχετικά με τα εντοπισμένα αντικείμενα.

Αυτό ανοίγει ένα παράθυρο που περιέχει τη λίστα των εντοπισμένων εφαρμογών και επεκτάσεων προγραμμάτων περιήγησης. Στη λίστα εμφανίζονται οι εικαζόμενες αιτίες για την πιθανή κατάργηση ή επιδιόρθωση κάθε αντικειμένου στη λίστα.

- Εάν θέλετε να καταργήσετε μια εφαρμογή ή επέκταση προγράμματος περιήγησης από τον υπολογιστή σας, κάντε κλικ στο κουμπί Κατάργηση στη γραμμή που περιέχει περιγραφή της εφαρμογής ή της επέκτασης προγράμματος περιήγησης. Το Kaspersky Total Security θα ξεκινήσει τη διαδικασία κατάργησης.
- Εάν θέλετε να παραμείνει η εφαρμογή ή επέκταση προγράμματος περιήγησης στον υπολογιστή σας και να μην περιλαμβάνεται άλλο στα αποτελέσματα της ανάλυσης εντοπισμένων αντικειμένων, κάντε κλικ στο κουμπί Παράβλεψη στη γραμμή που περιέχει περιγραφή του αντικειμένου. Το αντικείμενο προστίθεται στη <u>λίστα</u>
 <u>εξαιρέσεων</u> και το Kaspersky Total Security παύει να το εμφανίζει στη λίστα εντοπισμένων αντικειμένων.

Προβολή της λίστας εξαιρέσεων

Οι εφαρμογές και επεκτάσεις που επιθυμείτε να διατηρήσετε μπορούν να προστεθούν στη λίστα εξαιρέσεων.

Για προβολή της λίστας εξαιρέσεων:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.
- 4. Επιλέξτε το στοιχείο Διαχείριση εφαρμογών.

Ανοίγει το παράθυρο **Ρυθμίσεις της Διαχείρισης εφαρμογών**.

5. Κάντε κλικ στη σύνδεση **Εξαιρέσεις** για να ανοίξετε το παράθυρο **Εξαιρέσεις**.

Το παράθυρο **Εξαιρέσεις** δείχνει τις εφαρμογές και επεκτάσεις προγράμματος περιήγησης που έχετε προσθέσει στη λίστα εξαιρέσεων κάνοντας κλικ στο κουμπί **Παράβλεψη** στη <u>λίστα αντικειμένων που εντοπίστηκαν</u>.

6. Για να καταργήσετε ένα αντικείμενο από τη λίστα εξαιρέσεων, κάντε κλικ στο κουμπί **Κατάργηση από τη λίστα**.

Τρόπος αποστολής δεδομένων σχετικά με παράθυρο εφαρμογής ή προγράμματος περιήγησης στην Kaspersky

Εάν αντιμετωπίσετε προβλήματα με παράθυρο εφαρμογής ή προγράμματος περιήγησης που είναι ανοικτό στον υπολογιστή σας, μπορείτε να αναφέρετε το παράθυρο στην Kaspersky μέσω του Kaspersky Total Security.

Για να αποστείλετε δεδομένα σχετικά με παράθυρο εφαρμογής ή προγράμματος περιήγησης στην Kaspersky:

- 1. Ανοίξτε το κύριο παράθυρο του Kaspersky Total Security.
- 2. Κάντε κλικ στο κουμπί **Περισσότερα εργαλεία**.
- 3. Επιλέξτε την ενότητα **Εκκαθάριση και βελτιστοποίηση**.
- 4. Κάντε κλικ στη σύνδεση **Εκκαθάριση υπολογιστή** για να ανοίξει το παράθυρο **Εκκαθάριση υπολογιστή**.
- 5. Κάντε κλικ στη σύνδεση **Αναφορά ενοχλητικής εφαρμογής**.

Ο δρομέας αλλάζει σε σταυρό.

- 6. Επισημάνετε με τον δρομέα το παράθυρο εφαρμογής ή προγράμματος περιήγησης που θέλετε να αναφέρετε στην Kaspersky.
- Κάντε αριστερό κλικ για να συγκεντρώσετε δεδομένα σχετικά με την εφαρμογή ή την τοποθεσία web που άνοιξε αυτό το παράθυρο.

Ανοίγει το παράθυρο Συλλογή δεδομένων για την εφαρμογή.

- 8. Στο παράθυρο **Συλλογή δεδομένων για την εφαρμογή** εκτελέστε τις ακόλουθες ενέργειες:
 - a. Για να προβάλετε δεδομένα σχετικά με το παράθυρο που επιλέχθηκε, κάντε κλικ στη σύνδεση Προβολή συλλεχθέντων δεδομένων.

Αυτό ανοίγει το παράθυρο **Προβολή δεδομένων για την εφαρμογή**, όπου μπορείτε να προβάλετε όλες τις συγκεντρωμένες πληροφορίες σχετικά με το επιλεγμένο παράθυρο.

b. Για να δείτε την εικόνα που αντιγράψατε, τοποθετήστε τον δείκτη του ποντικιού πάνω της και κάντε αριστερό κλικ.

Θα ανοίξει ο φάκελος στον οποίο αποθηκεύσατε την εικόνα.

- c. Κάνοντας κλικ στη σύνδεση **Δήλωση σχετικά με την επεξεργασία δεδομένων** μπορείτε να δείτε τη Δήλωση μας σχετικά με την επεξεργασία δεδομένων.
- d. Επιλέξτε το πλαίσιο ελέγχου **Έχω διαβάσει και συμφωνώ με τη Δήλωση τεχνικής** υποστήριξης.
- e. Κάντε κλικ στο κουμπί **Αποστολή**.

Δεδομένα σχετικά με το παράθυρο εφαρμογής ή προγράμματος περιήγησης θα αποσταλούν στην Kaspersky.

Καταστροφέας αρχείων

Η πρόσθετη προστασία των προσωπικών δεδομένων σας διασφαλίζεται μέσω της αποτροπής της μη εξουσιοδοτημένης ανάκτησης των πληροφοριών που διαγράφονται από χάκερ.

Το Kaspersky Total Security περιέχει ένα εργαλείο οριστικής διαγραφής δεδομένων, το οποίο καθιστά αδύνατη την ανάκτηση δεδομένων χρησιμοποιώντας τυπικά εργαλεία λογισμικού.

Το Kaspersky Total Security επιτρέπει τη διαγραφή δεδομένων από τα εξής μέσα αποθήκευσης χωρίς να υπάρχει δυνατότητα ανάκτησής τους:

- Τοπικές μονάδες δίσκου. Η διαγραφή είναι εφικτή εάν έχετε τα απαιτούμενα δικαιώματα εγγραφής και διαγραφής των δεδομένων.
- Αφαιρούμενη μονάδα δίσκου ή άλλες συσκευές που αναγνωρίζονται ως αφαιρούμενες μονάδες δίσκου (όπως δισκέτες, κάρτες μνήμης, δίσκοι USB ή κινητά τηλέφωνα). Τα δεδομένα μιας κάρτας μνήμης μπορούν να διαγραφούν εάν έχει απενεργοποιηθεί η μηχανική προστασία επανεγγραφής.

Έχετε τη δυνατότητα να διαγράψετε τα δεδομένα στα οποία μπορείτε να αποκτήσετε πρόσβαση με τον προσωπικό λογαριασμό σας. Πριν διαγράψετε τα δεδομένα, βεβαιωθείτε ότι δεν χρησιμοποιούνται από εφαρμογές που εκτελούνται εκείνη τη στιγμή.

Για να διαγράψετε δεδομένα οριστικά:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Περισσότερα εργαλεία** που βρίσκεται στο κάτω μέρος του κεντρικού παραθύρου για να ανοίξετε το παράθυρο **Εργαλεία**.
- 3. Μεταβείτε στην ενότητα **Προστασία δεδομένων**.
- 4. Κάντε κλικ στη σύνδεση **Καταστροφέας αρχείων** για να ανοίξετε το παράθυρο **Καταστροφέας Αρχείων** (βλ. την ακόλουθη εικόνα).

🔮 File Shredder	_		×
Delete data permanently			0
Use File Shredder to delete data permanently and avoid unauthorized	data	recovery	
File or folder to delete: Browse Data deletion method:			
Quick delete (recommended)			
We recommend using this method for data removal from SSD devices, USB device drives.	es, and	network	
Delete Siles deleted successfully.			
		Clos	e

Παράθυρο **Καταστροφέας αρχείων**

5. Κάντε κλικ στο κουμπί **Αναζήτηση** και στο παράθυρο **Επιλογή φακέλου** που θα εμφανιστεί, επιλέξτε τον φάκελο ή το αρχείο που θα διαγραφεί οριστικά.

Η διαγραφή αρχείων ή φακέλων του συστήματος μπορεί να προκαλέσει δυσλειτουργίες του λειτουργικού συστήματος.

6. Στην αναπτυσσόμενη λίστα **Μέθοδος διαγραφής δεδομένων**, επιλέξτε τον επιθυμητό αλγόριθμο διαγραφής δεδομένων.

Για τη διαγραφή δεδομένων από συσκευές SSD και USB, συνιστάται η εφαρμογή της **Γρήγορης διαγραφής** ή της μεθόδου **GOST R 50739-95, Ρωσία**. Οι υπόλοιπες μέθοδοι διαγραφής ενδέχεται να προκαλέσουν βλάβη στη συσκευή SSD ή USB.

- Γρήγορη διαγραφή (συνιστάται). Η διαδικασία διαγραφής αποτελείται από δύο κύκλους αντικατάστασης δεδομένων: εγγραφή μηδενικών και ψευδοτυχαίων αριθμών. Το βασικό πλεονέκτημα αυτού του αλγορίθμου είναι η απόδοσή του. Η γρήγορη διαγραφή αποτρέπει την ανάκτηση δεδομένων με τυπικά εργαλεία ανάκτησης.
- GOST R 50739-95, Ρωσία. Ο αλγόριθμος αυτός εκτελεί έναν κύκλο αντικατάστασης χρησιμοποιώντας ψευδοτυχαίους αριθμούς και προστατεύει τα δεδομένα από ανάκτηση μέσω των τυπικών εργαλείων. Ο αλγόριθμος αντιστοιχεί στην κατηγορία προστασίας 2 (από 6), σύμφωνα με το σύστημα ταξινόμησης της Κρατικής Τεχνικής Επιτροπής της Ρωσίας (Russian State Technical Commission).
- Αλγόριθμος Bruce Schneier. Η διαδικασία αποτελείται από επτά κύκλους αντικατάστασης. Η μέθοδος διαφέρει από το γερμανικό πρότυπο VSITR όσον αφορά την αλληλουχία αντικατάστασης που ακολουθεί. Αυτή η ενισχυμένη μέθοδος διαγραφής δεδομένων θεωρείται μία από τις πλέον αξιόπιστες.
- Πρότυπο VSITR, Γερμανία. Εκτελούνται επτά κύκλοι αντικατάστασης. Ο αλγόριθμος θεωρείται αξιόπιστος, αλλά απαιτείται μεγάλο χρονικό διάστημα για την εκτέλεσή του.
- Πρότυπο NAVSO P-5239-26 (MFM), ΗΠΑ και Πρότυπο NAVSO P-5239-26 (RLL), ΗΠΑ.
 Χρησιμοποιούνται τρεις κύκλοι αντικατάστασης. Τα πρότυπα αυτά διαφέρουν μεταξύ τους όσον αφορά την αλληλουχία με την οποία αντικαθιστούν τις πληροφορίες.
- Πρότυπο DoD 5250.22-Μ, ΗΠΑ. Ο αλγόριθμος εκτελεί τρεις κύκλους αντικατάστασης.
 Το πρότυπο αυτό χρησιμοποιείται από το Υπουργείο Άμυνας των Η.Π.Α.
- 7. Κάντε κλικ στο κουμπί **Κατάργηση**.

Τα αρχεία που χρησιμοποιούνται από μια εφαρμογή τρίτου μέρους δεν μπορούν να διαγραφούν.

Καθαρισμός μη χρησιμοποιούμενων δεδομένων

Αυτή η ενότητα περιέχει οδηγίες για την αφαίρεση προσωρινών και μη χρησιμοποιούμενων αρχείων.

Πληροφορίες για τον καθαρισμό μη χρησιμοποιούμενων δεδομένων

Το λειτουργικό σύστημα συγκεντρώνει προσωρινά ή μη χρησιμοποιούμενα αρχεία με την πάροδο του χρόνου. Αυτά τα αρχεία μπορεί να καταλαμβάνουν πολύ χώρο στον δίσκο, υποβαθμίζοντας την απόδοση του συστήματος, ενώ μπορούν να αποτελέσουν αντικείμενο εκμετάλλευσης από κακόβουλο λογισμικό.

Τα προσωρινά αρχεία δημιουργούνται κατά την εκκίνηση εφαρμογών ή λειτουργικών συστημάτων. Ορισμένα προσωρινά αρχεία μπορεί να μην διαγραφούν, ακόμη και όταν κλείσετε την εφαρμογή ή το λειτουργικό σύστημα. Το Kaspersky Total Security περιλαμβάνει τον Οδηγό εκκαθάρισης μη χρησιμοποιούμενων δεδομένων.

Ο Καθαρισμός μη χρησιμοποιούμενων δεδομένων εντοπίζει και αφαιρεί τα ακόλουθα αρχεία:

- Αρχεία καταγραφής συμβάντων συστήματος, όπου καταγράφονται οι ονομασίες όλων των ενεργών εφαρμογών
- Αρχεία καταγραφής συμβάντων διαφόρων εφαρμογών ή προγραμμάτων ενημέρωσης (όπως η Ενημέρωση Windows)
- Αρχεία καταγραφής συνδέσεων συστήματος
- Προσωρινά αρχεία προγραμμάτων περιήγησης (cookie)
- Προσωρινά αρχεία που παραμένουν μετά την εγκατάσταση / κατάργηση εγκατάστασης εφαρμογών
- Περιεχόμενα του κάδου ανακύκλωσης

• Αρχεία στον φάκελο Temp, ο όγκος των οποίων μπορεί να ανέλθει σε αρκετά gigabyte

Εκτός από την διαγραφή μη χρησιμοποιούμενων αρχείων από το σύστημα, ο οδηγός διαγράφει επίσης αρχεία που μπορεί να περιέχουν εμπιστευτικά δεδομένα (κωδικοί πρόσβασης, ονόματα χρηστών, δεδομένα φόρμας καταχώρισης). Ωστόσο, για την πλήρη διαγραφή αυτών των δεδομένων, συνιστάται η χρήση του Οδηγού εκκαθάρισης ιδιωτικού απορρήτου.

Καθαρισμός μη χρησιμοποιούμενων δεδομένων

Για να ξεκινήσετε τον Οδηγό εκκαθάρισης μη χρησιμοποιούμενων δεδομένων:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί Περισσότερα εργαλεία που βρίσκεται στο κάτω μέρος του κεντρικού παραθύρου για να ανοίξετε το παράθυρο Εργαλεία.
- 3. Στο παράθυρο **Εργαλεία**, μεταβείτε στην ενότητα **Εκκαθάριση και βελτιστοποίηση**.
- 4. Κάντε κλικ στη σύνδεση **Καθαρισμός μη χρησιμοποιούμενων δεδομένων** για να ξεκινήσετε τον Οδηγό καθαρισμού μη χρησιμοποιούμενων δεδομένων.

Ο Οδηγός αποτελείται από μια σειρά σελίδων (βήματα), στις οποίες μπορείτε να περιηγηθείτε με τα κουμπιά **Πίσω** και **Επόμενο**. Για να κλείσετε τον Οδηγό αφού ολοκληρωθεί, κάντε κλικ στο κουμπί **Ολοκληρώθηκε**. Για να διακόψετε τον Οδηγό σε οποιοδήποτε βήμα κι αν βρίσκεται, κάντε κλικ στο κουμπί **Άκυρο**.

Ας δούμε αναλυτικότερα τα βήματα του Οδηγού.

Έναρξη του Οδηγού

Η πρώτη σελίδα του Οδηγού εμφανίζει πληροφορίες για τον καθαρισμό μη χρησιμοποιούμενων δεδομένων.

Κάντε κλικ στο κουμπί **Επόμενο** για να ξεκινήσετε τον Οδηγό.

Αναζήτηση μη χρησιμοποιούμενων δεδομένων

Ο Οδηγός εκτελεί αναζήτηση μη χρησιμοποιούμενων δεδομένων στον υπολογιστή. Η αναζήτηση ενδέχεται να διαρκέσει αρκετή ώρα. Μόλις ολοκληρωθεί η αναζήτηση, ο Οδηγός θα συνεχίσει αυτόματα στο επόμενο βήμα.

Επιλογή ενεργειών για τη διαγραφή μη χρησιμοποιούμενων δεδομένων

Αφού ολοκληρωθεί η αναζήτηση μη χρησιμοποιούμενων δεδομένων, ανοίγει ένα παράθυρο που εμφανίζει τη λίστα ενεργειών.

Για να κάνετε τον Οδηγό να εκτελέσει μια συγκεκριμένη ενέργεια, επιλέξτε το αντίστοιχο πλαίσιο ελέγχου δίπλα στην ενέργεια. Από προεπιλογή, ο Οδηγός εκτελεί όλες τις συνιστώμενες και τις ιδιαίτερα συνιστώμενες ενέργειες. Εάν δεν επιθυμείτε να εκτελεστεί μια συγκεκριμένη ενέργεια, αποεπιλέξτε το πλαίσιο ελέγχου δίπλα της.

Δεν συνιστάται να αποεπιλέξετε τα πλαίσια ελέγχου που είναι επιλεγμένα από προεπιλογή. Κάτι τέτοιο ενδέχεται να προκαλέσει κινδύνους για την ασφάλεια του υπολογιστή σας.

Αφού ορίσετε το σύνολο των ενεργειών που θα εκτελέσει ο Οδηγός, κάντε κλικ στο κουμπί **Επόμενο**.

Καθαρισμός μη χρησιμοποιούμενων δεδομένων

Ο Οδηγός θα εκτελέσει τις ενέργειες που επιλέχθηκαν στο προηγούμενο βήμα. Ο καθαρισμός μη χρησιμοποιούμενων δεδομένων μπορεί να διαρκέσει αρκετή ώρα.

Αφού ολοκληρωθεί ο καθαρισμός μη χρησιμοποιούμενων δεδομένων, ο Οδηγός προχωρά αυτόματα στο επόμενο βήμα.

Ενώ εκτελείται ο Οδηγός, ορισμένα αρχεία (όπως το αρχείο καταγραφής των Microsoft Windows και το αρχείο καταγραφής συμβάντων του Microsoft Office) ενδέχεται να χρησιμοποιηθούν από το λειτουργικό σύστημα. Για την διαγραφή αυτών των αρχείων, ο οδηγός θα σας προτείνει επανεκκίνηση του λειτουργικού συστήματος.

Ολοκλήρωση Οδηγού

Κάντε κλικ στο κουμπί **Ολοκληρώθηκε** για έξοδο από τον Οδηγό.

Δημιουργία αντιγράφων ασφαλείας

Αυτή η ενότητα παρέχει πληροφορίες σχετικά με τη δημιουργία αντιγράφων ασφαλείας δεδομένων.

Σχετικά με τη δημιουργία αντιγράφων ασφαλείας

Η δημιουργία αντιγράφων ασφαλείας δεδομένων είναι απαραίτητη για την προστασία των δεδομένων σας από το ενδεχόμενο απώλειας σε περίπτωση δυσλειτουργίας ή κλοπής του υπολογιστή σας, ή ακούσιας διαγραφής ή καταστροφής τους από χάκερ.

Για να δημιουργήσετε αντίγραφα ασφαλείας των δεδομένων σας, <u>δημιουργήστε</u> και <u>ξεκινήστε</u> μια εργασία δημιουργίας αντιγράφου ασφαλείας. Η εργασία μπορεί να ξεκινά αυτόματα σύμφωνα με ένα χρονοδιάγραμμα ή χειροκίνητα. Η εφαρμογή σας δίνει επίσης τη δυνατότητα να δείτε πληροφορίες σχετικά με τις ολοκληρωμένες εργασίες δημιουργίας αντιγράφων ασφαλείας. Συνιστάται να αποθηκεύετε τα αντίγραφα ασφαλείας των δεδομένων σας σε αφαιρούμενες μονάδες δίσκου ή σε online χώρους αποθήκευσης.

Το Kaspersky Total Security δεν μπορεί να δημιουργήσει ένα πλήρες αντίγραφο μιας μονάδας δίσκου ενώ ένα λειτουργικό σύστημα Microsoft Windows είναι ενεργό στη μονάδα δίσκου.

Το Kaspersky Total Security σας δίνει τη δυνατότητα να χρησιμοποιήσετε τους εξής τύπους χώρων αποθήκευσης για τη δημιουργία αντιγράφων ασφαλείας:

- Τοπική μονάδα δίσκου
- Αφαιρούμενη μονάδα δίσκου (π.χ. εξωτερικός σκληρός δίσκος)
- Μονάδα δίσκου δικτύου
- <u>Online χώρος αποθήκευσης</u>

Δημιουργία εργασιών με βάση τα δικαιώματα πρόσβασης χρήστη

Οι εργασίες δημιουργίας αντιγράφων ασφαλείας δημιουργούνται με βάση τα δικαιώματα πρόσβασης χρήστη στα αρχεία του τοπικού υπολογιστή.

Αν δεν έχετε δικαιώματα τοπικού διαχειριστή στον υπολογιστή, μπορείτε να έχετε πρόσβαση μόνο σε εργασίες που δημιουργήσατε εσείς. Αν έχετε δικαιώματα τοπικού διαχειριστή στον υπολογιστή, βλέπετε όλες τις εργασίες δημιουργίας αντιγράφων ασφαλείας, αλλά δεν μπορείτε να τροποποιήσετε τις εργασίες που δημιουργήθηκαν από άλλους χρήστες.

Οι εργασίες δημιουργίας αντιγράφων ασφαλείας είχαν δημιουργηθεί προηγουμένως χωρίς να ληφθούν υπόψη τα δικαιώματα χρήστη είναι διαθέσιμες σε όλους τους χρήστες του υπολογιστή. Ωστόσο, αν τροποποιηθεί μια τέτοια εργασία, θα εκτελεστεί με βάση τα δικαιώματα του χρήστη που τροποποίησε την εργασία.

Επαναφορά εργασιών με βάση τα δικαιώματα πρόσβασης χρήστη

Αν δεν έχετε δικαιώματα τοπικού διαχειριστή στον υπολογιστή, μπορείτε να επαναφέρετε δεδομένα μόνο από εργασίες αντιγράφων ασφαλείας που δημιουργήσατε εσείς και μόνο σε φακέλους στους οποίους έχετε δικαιώματα πρόσβασης. Αν έχετε δικαιώματα τοπικού διαχειριστή στον υπολογιστή, μπορείτε να επαναφέρετε δεδομένα από οποιαδήποτε εργασία αντιγράφου ασφαλείας σε οποιονδήποτε φάκελο. Το συνολικό μέγεθος των αντιγραμμένων αρχείων σε έναν φάκελο μπορεί να υπερβαίνει το μέγεθος αυτού του φακέλου εάν περιέχει συνδέσεις σε άλλους φακέλους (για παράδειγμα, όταν αντιγράφετε τον φάκελο "Έγγραφα", οι φάκελοι "Η μουσική μου", "Οι εικόνες μου" και "Τα βίντεό μου" θα αντιγραφούν επίσης εάν ο φάκελος "Έγγραφα" περιέχει συνδέσεις σε αυτούς τους φακέλους).

Σχετικά με τη δημιουργία αντιγράφων ασφαλείας και την επαναφορά στο OneDrive

Κατά τη δημιουργία αντιγράφων ασφαλείας αρχείων σε φάκελο OneDrive στον υπολογιστή σας, το Kaspersky Total Security ενεργεί διαφορετικά ανάλογα με το εάν το αρχείο cloud έχει ληφθεί στον φάκελο OneDrive:

- Εάν το αρχείο βρίσκεται στο cloud και στον φάκελο OneDrive στον υπολογιστή σας, το Kaspersky Total Security δημιουργεί ένα αντίγραφο ασφαλείας αυτού του αρχείου.
- Εάν το αρχείο δεν βρίσκεται στο cloud, αλλά υπάρχει στο φάκελο OneDrive στον υπολογιστή σας, το Kaspersky Total Security δημιουργεί ένα αντίγραφο ασφαλείας αυτού του αρχείου.
- Εάν το αρχείο εμφανίζεται στον φάκελο OneDrive, αλλά είναι αποθηκευμένο μόνο στο cloud και όχι στον υπολογιστή σας, το Kaspersky Total Security δημιουργεί ένα αντίγραφο ασφαλείας αυτού του αρχείου.

Πώς να δημιουργήσετε μια εργασία δημιουργίας αντιγράφων ασφαλείας

Για να δημιουργήσετε μια εργασία δημιουργίας αντιγράφου ασφαλείας:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Δημιουργία αντιγράφων ασφαλείας**.
- 3. Στο παράθυρο Δημιουργία αντιγράφων ασφαλείας, πραγματοποιήστε μία από τις εξής ενέργειες:
 - Εάν δεν έχει δημιουργηθεί ακόμα εργασία δημιουργίας αντιγράφου ασφαλείας, κάνε κλικ στο κουμπί Επιλογή αρχείων για αντίγραφα ασφαλείας.

 Εάν έχετε ήδη μια υφιστάμενη εργασία δημιουργίας αντιγράφου ασφαλείας και επιθυμείτε να δημιουργήσετε νέα, κάντε κλικ στο κουμπί Δημιουργία αντιγράφων ασφαλείας άλλων αρχείων.

Εκκινείται ο Οδηγός δημιουργίας εργασίας αντιγράφων ασφαλείας.

Ο Οδηγός αποτελείται από μια σειρά σελίδων (βήματα), στις οποίες μπορείτε να περιηγηθείτε με τα κουμπιά **Πίσω** και **Επόμενο**. Για να κλείσετε τον Οδηγό αφού ολοκληρωθεί, κάντε κλικ στο κουμπί **Ολοκληρώθηκε**. Για να διακόψετε τον Οδηγό σε οποιοδήποτε βήμα κι αν βρίσκεται, κάντε κλικ στο κουμπί **Άκυρο**.

Ας δούμε αναλυτικότερα τα βήματα του Οδηγού.

Βήμα 1. Επιλογή αρχείων

Σε αυτό το βήμα του Οδηγού, επιλέξτε τον τύπο των αρχείων ή προσδιορίστε τους φακέλους για τους οποίους επιθυμείτε να δημιουργήσετε αντίγραφα ασφαλείας:

 Επιλέξτε έναν από τους προκαθορισμένους τύπους αρχείων (αρχεία από τους φακέλους Τα έγγραφά μου και την Επιφάνεια εργασίας, φωτογραφίες και εικόνες, ταινίες και βίντεο, αρχεία μουσικής) για να εκτελέσετε τη γρήγορη ρύθμιση παραμέτρων. Αν επιβεβαιώσετε αυτήν την επιλογή, ο οδηγός θα σας μεταφέρει απευθείας στο βήμα 4 "Επιλογή χώρου αποθήκευσης αντιγράφων ασφαλείας".

Το Kaspersky Total Security δεν δημιουργεί αντίγραφα ασφαλείας των αρχείων που βρίσκονται στους φακέλους "Επιφάνεια εργασίας" και "Τα έγγραφά μου", εάν οι φάκελοι αυτοί βρίσκονται σε μονάδα δίσκου δικτύου.

 Επιλέξτε Δημιουργία αντιγράφων ασφαλείας αρχείων από καθορισμένους φακέλους για να προσδιορίσετε χειροκίνητα τους φακέλους για τους οποίους επιθυμείτε να δημιουργήσετε αντίγραφα ασφαλείας.

Βήμα 2. Επιλογή φακέλων για δημιουργία αντιγράφων ασφαλείας

Εάν επιλέξατε **Δημιουργία αντιγράφων ασφαλείας αρχείων από καθορισμένους φακέλους** στο προηγούμενο βήμα του Οδηγού, κάντε κλικ στο κουμπί **Προσθήκη φακέλου** και επιλέξτε έναν φάκελο στο παράθυρο **Επιλογή φακέλου για αντίγραφα ασφαλείας** που εμφανίζεται ή σύρετε τον φάκελο και αποθέστε τον εντός του παραθύρου της εφαρμογής. Επιλέξτε το πλαίσιο ελέγχου **Περιορισμός αντιγράφων ασφαλείας ανά τύπο αρχείου** εάν θέλετε να ορίσετε τις κατηγορίες αρχείων για τις οποίες θα δημιουργηθούν αντίγραφα ασφαλείας στους φακέλους που έχετε επιλέξει.

Βήμα 3. Επιλογή τύπων αρχείων για δημιουργία αντιγράφων ασφαλείας

Εάν επιλέξατε το πλαίσιο ελέγχου **Περιορισμός αντιγράφων ασφαλείας ανά τύπο αρχείου** στο προηγούμενο βήμα του Οδηγού, σε αυτό το βήμα του Οδηγού, επιλέξτε τα πλαίσια ελέγχου απέναντι από τους τύπους αρχείων για τα οποία θέλετε να δημιουργηθούν αντίγραφα ασφαλείας.

Βήμα 4. Επιλογή χώρου αποθήκευσης αντιγράφων ασφαλείας

Σε αυτό το βήμα μπορείτε να επιλέξετε έναν χώρο αποθήκευσης των αντιγράφων ασφαλείας:

- Online χώρος αποθήκευσης Ορίστε αυτήν την επιλογή εάν θέλετε να αποθηκεύετε τα αντίγραφα ασφαλείας στον online χώρο αποθήκευσης Dropbox. Η επιλογή <u>Online χώρος αποθήκευσης</u> πρέπει να έχει ενεργοποιηθεί για να είναι δυνατή η χρήση του. Όταν δημιουργείτε αντίγραφα ασφαλείας δεδομένων σε online χώρο αποθήκευσης, το Kaspersky Total Security δεν δημιουργεί αντίγραφα ασφαλείας στου Dropbox.
- Τοπική μονάδα δίσκου. Εάν θέλετε να αποθηκεύσετε τα αντίγραφα ασφαλείας σε μια τοπική μονάδα δίσκου, επιλέξτε την αντίστοιχη τοπική μονάδα δίσκου από τη λίστα.
- Μονάδα δίσκου δικτύου. Εάν θέλετε να αποθηκεύσετε τα αντίγραφα ασφαλείας σε μια μονάδα δίσκου δικτύου, επιλέξτε την αντίστοιχη μονάδα δίσκου δικτύου από τη λίστα.
- Αφαιρούμενη μονάδα δίσκου. Εάν θέλετε να αποθηκεύσετε τα αντίγραφα ασφαλείας σε μια αφαιρούμενη μονάδα δίσκου, επιλέξτε την αντίστοιχη αφαιρούμενη μονάδα δίσκου από τη λίστα.

Για να διασφαλιστεί η προστασία των δεδομένων, συνιστούμε τη χρήση του online χώρου αποθήκευσης ή τη δημιουργία χώρων αποθήκευσης αντιγράφων ασφαλείας σε αφαιρούμενες μονάδες δίσκου.

<u>Πώς να προσθέσετε χώρο αποθήκευσης δικτύου</u> ?

Για να προσθέσετε έναν χώρο αποθήκευσης δικτύου:

- 1. Κάντε κλικ στη σύνδεση **Προσθήκη χώρου δικτύου** για να ανοίξετε το παράθυρο **Προσθήκη χώρου δικτύου** και να επιλέξετε τον χώρο αποθήκευσης δικτύου.
- Προσδιορίστε τα δεδομένα που απαιτούνται για τη σύνδεση στον χώρο αποθήκευσης δικτύου.
- 3. Κάντε κλικ στο **ΟΚ**.

<u>Πώς να προσθέσετε μια αφαιρούμενη μονάδα δίσκου ως χώρο αποθήκευσης</u> 🕑

Για να προσθέσετε μια αφαιρούμενη μονάδα δίσκου ως χώρο αποθήκευσης αντιγράφων ασφαλείας:

- Κάντε κλικ στη σύνδεση Σύνδεση υφιστάμενου χώρου για να ανοίξετε το παράθυρο Σύνδεση χώρου αποθήκευσης.
- 2. Επιλέξτε την ενότητα **Αφαιρούμενη μονάδα δίσκου**.
- Κάντε κλικ στο κουμπί Αναζήτηση και στο παράθυρο που θα εμφανιστεί, προσδιορίστε την αφαιρούμενη μονάδα δίσκου στην οποία θέλετε να αποθηκεύσετε τα αντίγραφα ασφαλείας των αρχείων.

Επιλέξτε το πλαίσιο ελέγχου **Χρήση προηγμένων ρυθμίσεων αποθήκευσης** για να διαμορφώσετε τις ρυθμίσεις του χώρου αποθήκευσης αρχείων, όπως τον αριθμό των εκδόσεων των αντιγράφων ασφαλείας των αρχείων που θα αποθηκεύονται και τη διάρκεια αποθήκευσης των αντιγράφων ασφαλείας.

Βήμα 5. Δημιουργία χρονοδιαγράμματος δημιουργίας αντιγράφων ασφαλείας

Σε αυτό το βήμα του Οδηγού, πραγματοποιήστε μία από τις εξής ενέργειες:

- Προσδιορίστε το χρονοδιάγραμμα της εργασίας δημιουργίας αντιγράφου ασφαλείας, εάν θέλετε να ξεκινά αυτόματα η εργασία δημιουργίας αντιγράφων ασφαλείας.
 - a. Από την αναπτυσσόμενη λίστα Εκτέλεση δημιουργίας αντιγράφων ασφαλείας,
 επιλέξτε ένα χρονικό διάστημα για την εκτέλεση της εργασίας (για παράδειγμα,
 καθημερινά) και καθορίστε τον χρόνο εκτέλεσης της εργασίας στο πεδίο Στις.

- b. Στην ενότητα **Λογαριασμός χρήστη**, καθορίστε το όνομα και τον κωδικό πρόσβασης χρήστη του λογαριασμού σας σε αυτόν τον υπολογιστή. Τα δεδομένα του λογαριασμού σας απαιτούνται για την πρόσβαση στα αρχεία κατά τη διάρκεια της δημιουργίας αντιγράφων ασφαλείας.
- c. Επιλέξτε το πλαίσιο ελέγχου Εκτέλεση προγραμματισμένης δημιουργίας αντιγράφου ασφαλείας κατά την εκκίνηση του υπολογιστή εάν αυτός απενεργοποιήθηκε στον καθορισμένο χρόνο αν θέλετε να εκτελεστεί η δημιουργία αντιγράφου ασφαλείας αμέσως μόλις είναι δυνατό μετά την επανεκκίνηση της εφαρμογής. Για παράδειγμα, η δημιουργία αντιγράφων ασφαλείας έχει προγραμματιστεί να πραγματοποιείται κάθε σαββατοκύριακο. Εάν ο υπολογιστής ήταν απενεργοποιηθεί μόλις ενεργοποιηθεί ο υπολογιστής σε μια εργάσιμη ημέρα. Εάν αυτό το πλαίσιο ελέγχου είναι αποεπιλεγμένο, η δημιουργία αντιγράφων ασφαλείας πραγματοποιείται σύμφωνα με το χρονοδιάγραμμα χωρίς να επιχειρείται εκ νέου μετά από αποτυχημένη απόπειρα.
- Στη λίστα Εκτέλεση δημιουργίας αντιγράφων ασφαλείας, επιλέξτε κατ' απαίτηση εάν θέλετε να ξεκινήσετε χειροκίνητα την εργασία.

Όταν εργάζεστε με εργασίες δημιουργίας αντιγράφων ασφαλείας, λάβετε υπόψη τα ακόλουθα:

- Αν δημιουργήσετε μια εργασία προγραμματισμένης δημιουργίας αντιγράφου ασφαλείας,
 θα πρέπει να καθορίσετε τα δεδομένα του λογαριασμού σας σε αυτόν τον υπολογιστή.
- Αν δημιουργήσετε μια εργασία κατ' απαίτηση δημιουργίας αντιγράφου ασφαλείας, θα πρέπει να καθορίσετε τα δεδομένα του λογαριασμού σας σε αυτόν τον υπολογιστή.
- Αν μετατρέψετε μια κατ' απαίτηση εργασία σε προγραμματισμένη εργασία, θα πρέπει να καθορίσετε τα δεδομένα του λογαριασμού σας σε αυτόν τον υπολογιστή.

Βήμα 6. Ρύθμιση κωδικού πρόσβασης για την προστασία των αντιγράφων ασφαλείας

Επιλέξτε το πλαίσιο ελέγχου **Ενεργοποίηση προστασίας με κωδικό πρόσβασης** και συμπληρώστε τα πεδία **Κωδικός πρόσβασης στα αντίγραφα ασφαλείας** και **Επιβεβαίωση κωδικού πρόσβασης** για να προστατεύσετε την πρόσβαση στα αντίγραφα ασφαλείας με κωδικό πρόσβασης.

Απαιτείται ο κωδικός πρόσβασης για την προστασία του χώρου αποθήκευσης αντιγράφων ασφαλείας έναντι μη εξουσιοδοτημένης πρόσβασης. Το πρόγραμμα θα σας ζητήσει να πληκτρολογήσετε κωδικό πρόσβασης στις παρακάτω περιπτώσεις:

Όταν δημιουργήσετε για πρώτη φορά έναν χώρο αποθήκευσης αντιγράφων ασφαλείας σε μια τοπική ή αφαιρούμενη μονάδα δίσκου (όπως μια μονάδα flash). Κατά τη δημιουργία επόμενων εργασιών δημιουργίας αντιγράφων ασφαλείας σε μια τοπική μονάδα δίσκου ή σε αυτή την αφαιρούμενη μονάδα δίσκου, το πρόγραμμα δεν θα σας ζητά πλέον να πληκτρολογείτε κωδικό πρόσβασης. Θα χρησιμοποιείται ο κωδικός πρόσβασης που πληκτρολογήσατε προηγουμένως.

Αν αντιγράψετε τον τοπικό χώρο αποθήκευσης αντιγράφων ασφαλείας σε μια αφαιρούμενη μονάδα δίσκου και συνδέσετε αυτή την αφαιρούμενη μονάδα δίσκου σε άλλον υπολογιστή, το πρόγραμμα θα σας ζητήσει να πληκτρολογήσετε κωδικό πρόσβασης για να αντιγράψετε ή να επαναφέρετε δεδομένα από αυτόν τον χώρο αποθήκευσης.

 Όταν συνδέετε μια αφαιρούμενη μονάδα δίσκου στον υπολογιστή σας. Το πρόγραμμα ελέγχει την αφαιρούμενη μονάδα δίσκου και σας ζητά να πληκτρολογήσετε κωδικό πρόσβασης αν εντοπίσει χώρο αποθήκευσης αντιγράφων ασφαλείας σε αυτή την αφαιρούμενη μονάδα δίσκου.

Βήμα 7. Ρυθμίσεις χώρου αποθήκευσης εκδόσεων αρχείων

Το βήμα αυτό είναι διαθέσιμο εάν έχετε επιλέξει το πλαίσιο ελέγχου **Χρήση προηγμένων ρυθμίσεων αποθήκευσης** στο βήμα 4 "Επιλογή χώρου αποθήκευσης αντιγράφων ασφαλείας".

Καθορισμός ρυθμίσεων χώρου αποθήκευσης αρχείων:

- Επιλέξτε το πλαίσιο ελέγχου Περιορισμός του αριθμού των εκδόσεων αντιγράφων ασφαλείας και ορίστε τον αριθμό των εκδόσεων των αντιγράφων ασφαλείας των αρχείων που θα αποθηκεύονται στο πεδίο Εκδόσεις αντιγράφων ασφαλείας αρχείου για αποθήκευση.
- Επιλέξτε το πλαίσιο ελέγχου Περιορισμός στην περίοδο αποθήκευσης των εκδόσεων αντιγράφων ασφαλείας και ορίστε τον αριθμό ημερών που θα αποθηκεύεται κάθε έκδοση αντιγράφου ασφαλείας ενός αρχείου στο πεδίο Διατήρηση παλαιών εκδόσεων αντιγράφων ασφαλείας για.

Βήμα 8. Εισαγωγή ονόματα εργασίας δημιουργίας αντιγράφων ασφαλείας

Σε αυτό το βήμα πραγματοποιήστε την εξής ενέργεια:

- Εισαγάγετε το όνομα της εργασίας δημιουργίας αντιγράφων ασφαλείας.
- Επιλέξτε το πλαίσιο ελέγχου Εκτέλεση δημιουργίας αντιγράφου ασφαλείας μετά την ολοκλήρωση του οδηγού για να ξεκινήσει αυτόματα η διαδικασία δημιουργίας αντιγράφων ασφαλείας μόλις ολοκληρωθεί ο οδηγός.

Βήμα 9. Ολοκλήρωση Οδηγού

Το παράθυρο αυτό εμφανίζει τη διαδικασία ρύθμισης παραμέτρων του χώρου αποθήκευσης αντιγράφων ασφαλείας. Η διαδικασία ρύθμισης παραμέτρων μπορεί να διαρκέσει αρκετή ώρα.

Όταν ολοκληρωθεί η ρύθμιση των παραμέτρων, κάντε κλικ στην επιλογή **Ολοκληρώθηκε**.

Δημιουργείται μια εργασία δημιουργίας αντιγράφων ασφαλείας. Η εργασία που δημιουργήσατε εμφανίζεται στο παράθυρο **Δημιουργία αντιγράφων ασφαλείας**.

Πώς να ξεκινήσετε μια εργασία δημιουργίας αντιγράφων ασφαλείας

Για να ξεκινήσετε μια εργασία δημιουργίας αντιγράφων ασφαλείας:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Δημιουργία αντιγράφων ασφαλείας**.
- Στο παράθυρο Δημιουργία αντιγράφων ασφαλείας που εμφανίζεται, επιλέξτε μια εργασία δημιουργίας αντιγράφων ασφαλείας και κάντε κλικ στο κουμπί Εκτέλεση.

Ξεκινά η εργασία δημιουργίας αντιγράφων ασφαλείας.

Επαναφορά δεδομένων από αντίγραφο ασφαλείας

Για να επαναφέρετε δεδομένα από αντίγραφο ασφαλείας:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Δημιουργία αντιγράφων ασφαλείας**.
- 3. Πραγματοποιήστε μία από τις εξής ενέργειες:

- Κάντε κλικ στο κουμπί Επαναφορά αρχείων απέναντι από την αντίστοιχη εργασία δημιουργίας αντιγράφων ασφαλείας.
- Κάντε κλικ στο κουμπί Διαχείριση χώρων αποθήκευσης και στο παράθυρο που εμφανίζεται κάντε κλικ στο κουμπί Επαναφορά αρχείων απέναντι από τον αντίστοιχο χώρο αποθήκευσης αντιγράφων ασφαλείας.
- 4. Αν ορίστηκε κωδικός πρόσβασης κατά τη δημιουργία του αντιγράφου ασφαλείας, πληκτρολογήστε αυτόν τον κωδικό στο παράθυρο Εισαγάγετε τον κωδικό πρόσβασής σας για να αποκτήσετε πρόσβαση στον χώρο αποθήκευσης.
- 5. Στην αναπτυσσόμενη λίστα **Ημερομηνία/ώρα αντιγράφου ασφαλείας**, επιλέξτε την ημερομηνία και την ώρα δημιουργίας του αντιγράφου ασφαλείας.
- 6. Πραγματοποιήστε μία από τις εξής ενέργειες:
 - Εάν θέλετε να επαναφέρετε όλα τα δεδομένα, επιλέξτε το πλαίσιο ελέγχου Όλα τα δεδομένα.
 - Αν θέλετε να επαναφέρετε μόνο ορισμένους φακέλους, επιλέξτε τα πλαίσια ελέγχου που βρίσκονται δίπλα στους σχετικούς φακέλους.
 - Αν θέλετε να επαναφέρετε μόνο ορισμένα αρχεία, επιλέξτε τα πλαίσια ελέγχου που βρίσκονται δίπλα στους σχετικούς φακέλους στη στήλη Όνομα.
- Για να επαναφέρετε μόνο συγκεκριμένους τύπους αρχείων, επιλέξτε αυτούς τους τύπους αρχείων στην αναπτυσσόμενη λίστα Τύπος αρχείου.
- 8. Κάντε κλικ στο κουμπί **Ανάκτηση επιλεγμένων αρχείων**.

Εμφανίζεται το παράθυρο Επαναφορά αρχείων από αντίγραφα ασφαλείας.

- 9. Επιλέξτε μία από τις δύο επιλογές:
 - Αρχικός φάκελος. Εάν επιλεγεί αυτή η δυνατότητα, η εφαρμογή επαναφέρει τα δεδομένα στον αρχικό φάκελο.
 - Καθορισμένος φάκελος. Εάν επιλεγεί αυτή η δυνατότητα, η εφαρμογή επαναφέρει τα δεδομένα στον καθορισμένο φάκελο. Κάντε κλικ στο κουμπί Αναζήτηση για να επιλέξετε τον φάκελο στον οποίο θέλετε να επαναφέρετε δεδομένα.
- Στην αναπτυσσόμενη λίστα Σε περίπτωση διένεξης ονομάτων, επιλέξτε την ενέργεια που θα πραγματοποιείται από την εφαρμογή όταν το όνομα του αρχείου που

επαναφέρετε είναι ίδιο με το όνομα ενός αρχείου που υπάρχει ήδη στον φάκελο προορισμού:

- Προτροπή χρήστη όταν υπάρχει διένεξη ονομάτων αρχείων, η εφαρμογή σας ειδοποιεί να επιλέξετε μία από τις εξής εναλλακτικές: αντικατάσταση του αρχείου με το αντίγραφο ασφαλείας, αποθήκευση και των δύο αρχείων ή να μην εκτελεστεί επαναφορά αυτού του αρχείου.
- αντικατάσταση αρχείου με αντίγραφο ασφαλείας Το Kaspersky Total Security διαγράφει το υπάρχον αρχείο και το αντικαθιστά με το αρχείο που επανέρχεται από το αντίγραφο ασφαλείας.
- αποθήκευση και των δύο αρχείων Το Kaspersky Total Security αφήνει το υπάρχον αρχείο αμετάβλητο και αποθηκεύει το αρχείο που επανέρχεται από το αντίγραφο ασφαλείας με νέο όνομα στον ίδιο φάκελο.
- να μην γίνει επαναφορά αυτού του αρχείου Το Kaspersky Total Security αφήνει το υπάρχον αρχείο αμετάβλητο και δεν εκτελεί επαναφορά του αρχείου με το ίδιο όνομα από το αντίγραφο ασφαλείας.
- 11. Κάντε κλικ στο κουμπί **Επαναφορά**.

Εκτελείται επαναφορά των επιλεγμένων αρχείων από το αντίγραφο ασφαλείας και αποθήκευσή τους στον καθορισμένο φάκελο.

Επαναφορά δεδομένων από τον χώρο αποθήκευσης FTP

Η τρέχουσα έκδοση της εφαρμογής δεν υποστηρίζει δημιουργία αντιγράφων ασφαλείας και επαναφορά μέσω FTP. Για να επαναφέρετε αντίγραφα ασφαλείας που δημιουργήθηκαν σε παλαιότερες εκδόσεις εφαρμογών από χώρο αποθήκευσης FTP, ακολουθήστε τις παρακάτω οδηγίες.

Για να επαναφέρετε αντίγραφα ασφαλείας από τον χώρο αποθήκευσης FTP:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Δημιουργία αντιγράφων ασφαλείας**.
- 3. Κάντε κλικ στη σύνδεση **Διαχείριση χώρων αποθήκευσης** για να ανοίξετε το παράθυρο **Χώροι αποθήκευσης**.
- 4. Κάντε κλικ στον σύνδεσμο **Μετάβαση στον διακομιστή FTP** για να ανοίξετε τον φάκελο αποθήκευσης FTP στην Εξερεύνηση των Windows.

- 5. Αντιγράψτε τα δεδομένα (συμπεριλαμβανομένου του αρχείου storage.xml) σε μια τοπική μονάδα δίσκου (για παράδειγμα, C: \<όνομα φακέλου>).
- 6. Στο παράθυρο **Διαχείριση χώρων αποθήκευσης** δίπλα στον χώρο αποθήκευσης FTP, κάντε κλικ στο κουμπί **Διαγραφή**.
- 7. Στο παράθυρο επιβεβαίωσης της διαγραφής, επιλέξτε **Κατάργηση**.

Ο χώρος αποθήκευσης έχει πλέον διαγραφεί.

- 8. Στο παράθυρο **Διαχείριση χώρων αποθήκευσης**, κάντε κλικ στο κουμπί **Σύνδεση** υφιστάμενου χώρου.
- 9. Στο παράθυρο Σύνδεση χώρου αποθήκευσης, επιλέξτε την ενότητα Τοπική μονάδα δίσκου και χρησιμοποιήστε το κουμπί Αναζήτηση για να καθορίσετε τη διαδρομή προς τον φάκελο που περιέχει τα αντίγραφα ασφαλείας που αντιγράψατε στην τοπική μονάδα δίσκου από χώρο αποθήκευσης FTP.
- Στο παράθυρο Χώροι αποθήκευσης, δίπλα στον συνδεδεμένο χώρο αποθήκευσης, κάντε κλικ στο κουμπί Επαναφορά.
- 11. Ακολουθήστε την <u>τυπική διαδικασία επαναφοράς</u>.

Επαναφορά δεδομένων από αντίγραφο ασφαλείας με χρήση του Kaspersky Restore Utility

Το Kaspersky Restore Utility σάς δίνει τη δυνατότητα να διαχειριστείτε τα δεδομένα του χώρου αποθήκευσης αντιγράφων ασφαλείας σε έναν υπολογιστή όπου μια εφαρμογή της Kaspersky έχει καταστραφεί ή καταργηθεί. Από προεπιλογή, μετά την εγκατάσταση της εφαρμογής, το βοηθητικό πρόγραμμα βρίσκεται στον φάκελο του Kaspersky Restore Utility που βρίσκεται στον φάκελο ρύθμισης της εφαρμογής. Για να χρησιμοποιήσετε το βοηθητικό πρόγραμμα σε υπολογιστή στον οποίο δεν είναι εγκατεστημένη ή είναι κατεστραμμένη η εφαρμογή της Kaspersky, αντιγράψτε το βοηθητικό πρόγραμμα σε μια αφαιρούμενη μονάδα δίσκου.

Για να ξεκινήσετε το Kaspersky Restore Utility, χρειάζεστε δικαιώματα τοπικού διαχειριστή.

<u>Πώς να ξεκινήσετε το Βοηθητικό Πρόγραμμα Επαναφοράς 🖻</u>

Για να ξεκινήσετε το Βοηθητικό Πρόγραμμα Επαναφοράς:

- Ανοίξτε την αφαιρούμενη μονάδα δίσκου στην οποία έχετε αντιγράψει το βοηθητικό πρόγραμμα.
- 2. Εκτελέστε το αρχείο kasperskylab.pure.restoretool στον φάκελο του Kaspersky Restore Utility.

Εμφανίζεται το κύριο παράθυρο του Restore Utility. Το παράθυρο εμφανίζει τον προεπιλεγμένο χώρο αποθήκευσης που έχει διαμορφωθεί στην εφαρμογή. Μπορείτε να καθορίσετε τη διαδρομή προς κάποιον άλλο χώρο αποθήκευσης.

<u>Πώς να ανοίξετε έναν χώρο αποθήκευσης χρησιμοποιώντας το Restore Utility</u> 🕑

Για να ανοίξετε έναν χώρο αποθήκευσης αντιγράφων ασφαλείας χρησιμοποιώντας το Restore Utility:

1. Ξεκινήστε το Restore Utility.

Το βοηθητικό πρόγραμμα εντοπίζει αυτόματα τη διαδρομή προς τον χώρο αποθήκευσης αντιγράφων ασφαλείας εάν αυτός δημιουργήθηκε στην τοπική μονάδα δίσκου C:\.

- Εάν ο χώρος αποθήκευσης αντιγράφων ασφαλείας βρίσκεται σε άλλη μονάδα δίσκου, κάντε κλικ στο κουμπί Καθορισμός χώρου αποθήκευσης στο κύριο παράθυρο του Restore Utility.
- 3. Στο παράθυρο που ανοίγει, κάντε κλικ στο κουμπί **Αναζήτηση** και προσδιορίστε τη διαδρομή προς τον χώρο αποθήκευσης αντιγράφων ασφαλείας.
- 4. Κάντε κλικ στο κουμπί **Επιλογή χώρου αποθήκευσης**.

Πώς να επαναφέρετε δεδομένα από αντίγραφο ασφαλείας 💿

Για να επαναφέρετε δεδομένα από αντίγραφο ασφαλείας:

- 1. Ξεκινήστε το Restore Utility.
- 2. Πραγματοποιήστε τις εξής ενέργειες από το κύριο παράθυρο του Restore Utility:
 - a. Στην αναπτυσσόμενη λίστα Εργασία δημιουργίας αντιγράφου ασφαλείας,
 επιλέξτε την εργασία που οδήγησε στη δημιουργία των επιθυμητών
 αντιγράφων ασφαλείας.

- b. Στην αναπτυσσόμενη λίστα **Ημερομηνία/ώρα αντιγράφου ασφαλείας**, επιλέξτε την ημερομηνία και την ώρα που δημιουργήθηκαν τα αντίστοιχα αντίγραφα ασφαλείας.
- Επιλέξτε τα αρχεία που θέλετε να επαναφέρετε. Για να το κάνετε αυτό, επιλέξτε τα πλαίσια ελέγχου δίπλα από τους σχετικούς φακέλους στη λίστα.

Χρησιμοποιήστε δίπλα στο πεδίο **Αναζήτηση** για εναλλαγή ανάμεσα στο δέντρο φακέλων και τη λίστα αρχείων.

4. Κάντε κλικ στο κουμπί **Επαναφορά επιλεγμένων δεδομένων**.

Ανοίγει το παράθυρο **Επιλέξτε πού θέλετε να τοποθετηθούν τα αρχεία μετά την επαναφορά**.

- 5. Στο παράθυρο που εμφανίζεται, επιλέξτε τη θέση για την αποθήκευση των αρχείων που θα επανέλθουν.
 - Αρχικός φάκελος. Επιλέξτε αυτή τη δυνατότητα για να επαναφέρετε δεδομένα στον αρχικό φάκελο.
 - Καθορισμένος φάκελος. Ενεργοποιήστε αυτήν την επιλογή για να επιλέξετε τον φάκελο στον οποίο θα πραγματοποιηθεί επαναφορά των δεδομένων. Για να επιλέξετε τον φάκελο στον οποίο θα πραγματοποιηθεί επαναφορά των δεδομένων, κάντε κλικ στο κουμπί Αναζήτηση.
- 6. Στην αναπτυσσόμενη λίστα **Σε περίπτωση διένεξης ονομάτων**, επιλέξτε την ενέργεια που θα πραγματοποιείται από την εφαρμογή όταν στον φάκελο προορισμού για την επαναφορά του αρχείου, υπάρχει ήδη αρχείο με το ίδιο όνομα:
 - Προτροπή χρήστη όταν υπάρχει διένεξη ονομάτων αρχείων, η εφαρμογή σας ειδοποιεί να επιλέξετε μία από τις εξής εναλλακτικές: αντικατάσταση του αρχείου με το αντίγραφο ασφαλείας, αποθήκευση και των δύο αρχείων ή να μην εκτελεστεί επαναφορά αυτού του αρχείου.
 - αντικατάσταση αρχείου με αντίγραφο ασφαλείας Το Kaspersky Total Security διαγράφει το υπάρχον αρχείο και το αντικαθιστά με το αρχείο που επανέρχεται από το αντίγραφο ασφαλείας.
 - αποθήκευση και των δύο αρχείων Το Kaspersky Total Security αφήνει το υπάρχον αρχείο αμετάβλητο και αποθηκεύει το αρχείο που επανέρχεται από το αντίγραφο ασφαλείας με νέο όνομα στον ίδιο φάκελο.
 - να μην γίνει επαναφορά αυτού του αρχείου Το Kaspersky Total Security αφήνει το υπάρχον αρχείο αμετάβλητο και δεν εκτελεί επαναφορά του αρχείου

με το ίδιο όνομα από το αντίγραφο ασφαλείας.

7. Κάντε κλικ στο κουμπί **Επαναφορά**.

Θα ανοίξει το παράθυρο **Επαναφορά αρχείων**. Το παράθυρο δείχνει την πρόοδο της επαναφοράς του αρχείου από αντίγραφα ασφαλείας. Μπορείτε να διακόψετε τη διεργασία επαναφοράς χρησιμοποιώντας το κουμπί **Διακοπή**.

Γίνεται επαναφορά των απαιτούμενων αντιγράφων ασφαλείας των επιλεγμένων αρχείων.

Σχετικά με τον online χώρο αποθήκευσης

Το Kaspersky Total Security σας δίνει τη δυνατότητα να αποθηκεύετε τα αντίγραφα ασφαλείας των δεδομένων σας σε online χώρο αποθήκευσης σε έναν απομακρυσμένο διακομιστή μέσω της υπηρεσίας Dropbox.

Για να χρησιμοποιήσετε τον online χώρο αποθήκευσης:

- Βεβαιωθείτε ότι ο υπολογιστής είναι συνδεδεμένος στο Διαδίκτυο.
- Δημιουργήστε λογαριασμό στον δικτυακό τόπο του παρόχου υπηρεσιών online αποθήκευσης δεδομένων.
- Ενεργοποιήστε τον online χώρο αποθήκευσης.

Μπορείτε να χρησιμοποιήσετε έναν μεμονωμένο λογαριασμό Dropbox για τη δημιουργία αντιγράφου ασφαλείας από διαφορετικές συσκευές με εγκατεστημένο το Kaspersky Total Security σε έναν μεμονωμένο online χώρο αποθήκευσης.

To μέγεθος του online χώρου αποθήκευσης καθορίζεται από τον πάροχο της υπηρεσίας του online χώρου αποθήκευσης, δηλ. της υπηρεσίας web Dropbox. Συμβουλευτείτε τον διαδικτυακό τόπο του Dropbox ^Δ για περισσότερες λεπτομέρειες σχετικά με τους όρους χρήσης της υπηρεσίας web.

Κατά την αντιγραφή αρχείων στο Dropbox, το Kaspersky Total Security δεν κάνει διάκριση μεταξύ κεφαλαίων και πεζών γραμμάτων στο όνομα ενός αρχείου ή/και στο όνομα μιας διαδρομής προς το αρχείο. Επομένως, κατά την προσπάθεια δημιουργίας αντιγράφων ασφαλείας των αρχείων των οποίων τα ονόματα ή/και οι διαδρομές διαφέρουν μόνο ως προς τα πεζά ή τα κεφαλαία γράμματα, το Kaspersky Total Security δημιουργεί μόνο ένα αντίγραφο ασφαλείας επειδή προκύπτει διένεξη στο Dropbox.

Πώς να ενεργοποιήσετε τον online χώρο αποθήκευσης

Για να ενεργοποιήσετε τον online χώρο αποθήκευσης:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί **Δημιουργία αντιγράφων ασφαλείας**.
- 3. Πραγματοποιήστε μία από τις εξής ενέργειες:
 - Εάν δεν έχει δημιουργηθεί ακόμα εργασία δημιουργίας αντιγράφου ασφαλείας, κάνε κλικ στο κουμπί Επιλογή αρχείων για αντίγραφα ασφαλείας.
 - Εάν έχετε ήδη μια εργασία δημιουργίας αντιγράφου ασφαλείας, κάντε κλικ στο κουμπί Δημιουργία αντιγράφων ασφαλείας άλλων αρχείων.

Εκκινείται ο <u>Οδηγός δημιουργίας εργασίας αντιγράφων ασφαλείας</u>.

- 4. Στο παράθυρο επιλογής τύπου δεδομένων, επιλέξτε την κατηγορία δεδομένων ή προσδιορίστε χειροκίνητα τα αρχεία για τα οποία θέλετε να δημιουργήσετε αντίγραφα ασφαλείας.
- 5. Στο παράθυρο επιλογής χώρου αποθήκευσης, επιλέξτε **Online χώρος αποθήκευσης** και κάντε κλικ στο κουμπί **Ενεργοποίηση**.

Απαιτείται σύνδεση στο Διαδίκτυο για τη δημιουργία online χώρου αποθήκευσης.

Ανοίγει ένα παράθυρο διαλόγου σύνδεσης στον λογαριασμό Dropbox.

- 6. Στο παράθυρο που εμφανίζεται, πραγματοποιήστε μία από τις εξής ενέργειες:
 - Ολοκληρώστε την εγγραφή εάν δεν είστε ήδη εγγεγραμμένος χρήστης του Dropbox.
 - Εάν είστε εγγεγραμμένος χρήστης του Dropbox, συνδεθείτε στον λογαριασμό σας στο Dropbox.
- 7. Για να ολοκληρώσετε την ενεργοποίηση του online χώρου αποθήκευσης, επιβεβαιώστε ότι το Kaspersky Total Security επιτρέπεται να χρησιμοποιήσει τον λογαριασμό σας στο Dropbox για τη δημιουργία αντιγράφων ασφαλείας των δεδομένων σας. Το Kaspersky Total Security τοποθετεί τα αντίγραφα ασφαλείας των αποθηκευμένων δεδομένων σε

ξεχωριστό φάκελο που δημιουργείται στον φάκελο αποθήκευσης του Dropbox για εφαρμογές.

Μόλις ολοκληρωθεί η ενεργοποίηση του online χώρου αποθήκευσης, εμφανίζεται το παράθυρο επιλογής χώρου αποθήκευσης. Περιέχει μια λίστα με online χώρους αποθήκευσης για να επιλέξετε. Για τον ενεργοποιημένο online χώρο αποθήκευσης, η εφαρμογή εμφανίζει το ποσοστό του κατειλημμένου χώρου και του διαθέσιμου ελεύθερου χώρου για αποθήκευση δεδομένων.

Αποθήκευση δεδομένων σε θαλάμους δεδομένων

Η ενότητα αυτή περιγράφει την προστασία των δεδομένων χρησιμοποιώντας θαλάμους δεδομένων.

Σχετικά με τον θάλαμο δεδομένων

Οι θάλαμοι δεδομένων έχουν σχεδιαστεί για την προστασία των εμπιστευτικών δεδομένων σας από τη μη εξουσιοδοτημένη πρόσβαση. *Θάλαμος δεδομένων* είναι ένας χώρος αποθήκευσης δεδομένων στον υπολογιστή σας, τον οποίο μπορείτε να κλειδώσετε ή να ξεκλειδώσετε χρησιμοποιώντας έναν κωδικό πρόσβασης που γνωρίζετε μόνο εσείς. Για να τροποποιήσετε τα αρχεία που είναι αποθηκευμένα σε έναν κλειδωμένο θάλαμο δεδομένων, πρέπει να συμπληρώσετε τον κωδικό πρόσβασης. Εάν εισαγάγατε έναν μη έγκυρο κωδικό πρόσβασης 10 συνεχόμενες φορές, η πρόσβαση στο θάλαμο δεδομένων αποκλείεται για μία ώρα.

Εάν χάσετε ή ξεχάσετε τον κωδικό πρόσβασης, δεν θα έχετε τη δυνατότητα να ανακτήσετε τα δεδομένα σας.

Για τη δημιουργία θαλάμων δεδομένων, το Kaspersky Total Security χρησιμοποιεί τον αλγόριθμο κρυπτογράφησης δεδομένων AES XTS με μήκος κλειδιού 56 bit.

Εάν στον υπολογιστή σας χρησιμοποιείται το σύστημα αρχείων FAT32, μπορείτε να δημιουργήσετε θαλάμους δεδομένων σε μέγεθος όχι μεγαλύτερο από 4 GB.

Πώς να μετακινήσετε αρχεία στο θάλαμο δεδομένων

Για να τοποθετήσετε αρχεία σε έναν θάλαμο δεδομένων:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Στο κάτω μέρος του κύριου παραθύρου, κάντε κλικ στο κουμπί **Περισσότερα εργαλεία**.
Ανοίγει το παράθυρο Εργαλεία.

- 3. Μεταβείτε στην ενότητα **Προστασία δεδομένων**.
- 4. Κάντε κλικ στη σύνδεση **Κρυπτογράφηση δεδομένων** για να ανοίξει το παράθυρο **Κρυπτογράφηση δεδομένων**.
- 5. Στο παράθυρο **Κρυπτογράφηση δεδομένων**, πραγματοποιήστε μία από τις εξής ενέργειες:
 - Εάν δεν διαθέτετε ακόμα θάλαμο δεδομένων, κάντε κλικ στο κουμπί δημιουργία νέου θαλάμου δεδομένων.
 - Εάν έχετε προηγούμενα δημιουργήσει θάλαμο δεδομένων, κάντε κλικ στο κουμπί
 Δημιουργία θαλάμου δεδομένων.
- 6. Κάντε κλικ στο κουμπί **Προσθήκη** για να ανοίξετε την Εξερεύνηση και να προσδιορίσετε τα αρχεία που θέλετε να τοποθετήσετε στον θάλαμο δεδομένων.

Τα επιλεγμένα αρχεία εμφανίζονται στο παράθυρο **Κρυπτογράφηση δεδομένων**.

- 7. Κάντε κλικ στο κουμπί **Συνέχεια**.
- 8. Εισαγάγετε το όνομα του θαλάμου δεδομένων και προσδιορίστε τη θέση του ή χρησιμοποιήστε τις προεπιλεγμένες τιμές αυτών των ρυθμίσεων.
- Για να έχετε τη δυνατότητα γρήγορης πρόσβασης στον θάλαμο δεδομένων, επιλέξτε το πλαίσιο ελέγχου Δημιουργία συντόμευσης στην επιφάνεια εργασίας για τον θάλαμο δεδομένων.
- 10. Κάντε κλικ στο κουμπί **Συνέχεια**.
- 11. Συμπληρώστε τα πεδία **Κωδικός πρόσβασης θαλάμου δεδομένων** και **Επιβεβαίωση** κωδικού πρόσβασης και κάντε κλικ στη Συνέχεια.
- 12. Επιλέξτε ποια ενέργεια θα πραγματοποιείται με τα αντίγραφα προέλευσης των αρχείων που βρίσκονται εκτός του θαλάμου δεδομένων:
 - Για τη διαγραφή των αντιγράφων προέλευσης που βρίσκονται εκτός του θαλάμου δεδομένων, κάντε κλικ στην Διαγραφή.
 - Για τη διατήρηση των αντιγράφων προέλευσης που βρίσκονται εκτός του θαλάμου δεδομένων, κάντε κλικ στην Παράλειψη.

13. Κάντε κλικ στο κουμπί **Ολοκληρώθηκε**.

Ο θάλαμος δεδομένων που έχετε δημιουργήσει, εμφανίζεται στη λίστα θαλάμων δεδομένων.

14. Για να κλειδώσετε τον θάλαμο δεδομένων, κάντε κλικ στο κουμπί **Κλείδωμα**.

Τα δεδομένα σε έναν κλειδωμένο θάλαμο δεδομένων καθίστανται διαθέσιμα μόνο μετά την εισαγωγή του κατάλληλου κωδικού πρόσβασης.

Κατά την προσθήκη στον θάλαμο αρχείων με το ίδιο όνομα που είναι εγγεγραμμένα σε διαφορετικά μητρώα, ένα από αυτά τα αρχεία μπορεί να μην είναι διαθέσιμο όταν επιχειρήσετε να ανοίξετε τον θάλαμο. Για να αποφύγετε την απώλεια δεδομένων, σας συνιστούμε να προσθέσετε αυτά τα αρχεία σε διαφορετικούς θαλάμους ή να αλλάξετε τα ονόματα των αρχείων, έτσι ώστε αυτά να είναι μοναδικά.

Πώς να αποκτήσετε πρόσβαση στα αρχεία που είναι αποθηκευμένα σε θάλαμο δεδομένων

Για να αποκτήσετε πρόσβαση στα δεδομένα εντός του θαλάμου δεδομένων:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Στο κάτω μέρος του κύριου παραθύρου, κάντε κλικ στο κουμπί Περισσότερα εργαλεία.
 Ανοίγει το παράθυρο Εργαλεία.
- 3. Μεταβείτε στην ενότητα **Προστασία δεδομένων**.
- 4. Κάντε κλικ στη σύνδεση **Κρυπτογράφηση δεδομένων** για να ανοίξει το παράθυρο **Κρυπτογράφηση δεδομένων**.
- 5. Κάντε κλικ στο κουμπί **Άνοιγμα** δίπλα στον επιθυμητό θάλαμο δεδομένων.
- 6. Εισαγάγετε τον κωδικό πρόσβασης και κάντε κλικ στο κουμπί **Άνοιγμα στην Εξερεύνηση**.

Τα αρχεία που είναι αποθηκευμένα στον θάλαμο δεδομένων εμφανίζονται στο παράθυρο της Εξερεύνησης. Μπορείτε να πραγματοποιήσετε τις απαραίτητες αλλαγές στα αρχεία και να κλειδώσετε ξανά τον θάλαμο δεδομένων. Ξεκινώντας με το Kaspersky Total Security 2021, όταν μετονομάσετε έναν θάλαμο, εμφανίζεται σφάλμα αν προσπαθήσετε να τον ανοίξετε. Για να το αποφύγετε, σας συνιστούμε να ανοίξετε τον θάλαμο που θέλετε να μετονομάσετε, να εξαγάγετε τα δεδομένα σας και να δημιουργήσετε έναν νέο θάλαμο με αυτά τα δεδομένα, με διαφορετικό όνομα.

Για να ξεκλειδώσετε θαλάμους δεδομένων που έχουν δημιουργηθεί χρησιμοποιώντας προηγούμενη έκδοση της εφαρμογής, πρέπει να μετατρέψετε τους θαλάμους δεδομένων από την παλιά στη νέα μορφή. Η εφαρμογή θα εμφανίσει μια ειδοποίηση σχετικά με τη μετατροπή όταν επιχειρήσετε να ανοίξετε έναν θάλαμο δεδομένων στο Kaspersky Total Security.

Η μετατροπή του θαλάμου δεδομένων στη νέα μορφή μπορεί να διαρκέσει αρκετή ώρα ανάλογα με το μέγεθος του θαλάμου.

Εάν δεν έχετε εγκαταστήσει την πλέον πρόσφατη ενημέρωση για το Kaspersky Total Security, όταν θα κάνετε αναβάθμιση σε μια νέα έκδοση, οι θάλαμοι δεδομένων που δημιουργήσατε στην προηγούμενη έκδοση της εφαρμογής <u>ενδέχεται να καταστούν μη διαθέσιμοι</u> 🖬 .

Τρόπος δέσμευσης πόρων του λειτουργικού συστήματος για παιχνίδια υπολογιστή

Όταν το Kaspersky Total Security εκτελείται σε λειτουργία πλήρους οθόνης ταυτόχρονα με ορισμένες άλλες εφαρμογές (ειδικά αν πρόκειται για παιχνίδια για υπολογιστές), ενδέχεται να προκύψουν τα παρακάτω προβλήματα:

- Μειωμένη απόδοση της εφαρμογής ή του παιχνιδιού λόγω έλλειψης πόρων συστήματος
- Τα παράθυρα ειδοποιήσεων του Kaspersky Total Security αποσπούν τον χρήστη από το παιχνίδι

Για να αποφύγετε τη χειροκίνητη αλλαγή των ρυθμίσεων του Kaspersky Total Security κάθε φορά που περνάτε σε λειτουργία πλήρους οθόνης, μπορείτε να χρησιμοποιήσετε την Κατάσταση παιχνιδιών. Εάν χρησιμοποιείται η Κατάσταση παιχνιδιών και παίζετε ή εργάζεστε με εφαρμογές σε λειτουργία πλήρους οθόνης, το Kaspersky Total Security δεν εκτελεί εργασίες σάρωσης και ενημέρωσης, και δεν εμφανίζει ειδοποιήσεις.

Για να ενεργοποιήσετε την Κατάσταση παιχνιδιών:

1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.

- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Γενικά**.
- 4. Στον αποκλεισμό των ρυθμίσεων **Απόδοση**, επιλέξτε το πλαίσιο ελέγχου **Χρήση της λειτουργίας παιχνιδιών**.

Πώς να βελτιστοποιήσετε το φορτίο στο λειτουργικό σύστημα λόγω της εκτέλεσης εργασιών του Kaspersky Total Security

Όταν εκτελείτε σάρωση υπολογιστή χρησιμοποιώντας το Kaspersky Total Security, αυτό μπορεί να καταναλώνει σημαντικούς πόρους συστήματος. Για να βελτιστοποιήσετε το φορτίο στο σύστημα, μπορείτε να διαμορφώσετε το Kaspersky Total Security έτσι ώστε να εκτελεί εργασίες σάρωσης (για μνήμη συστήματος, διαμέρισμα συστήματος και αντικείμενα εκκίνησης) και να ενημερώνει βάσεις δεδομένων όταν ο υπολογιστής είναι κλειδωμένος ή ενεργοποιείται η προφύλαξη οθόνης. Αυτή η πρόσθετη ρύθμιση σας επιτρέπει να βελτιώσετε την ασφάλεια του υπολογιστή σας χωρίς να υποβαθμίζεται η απόδοσή του κατά τη χρήση.

Εάν ο υπολογιστής λειτουργεί με μπαταρία, το Kaspersky Total Security δεν θα εκτελεί εργασίες όταν ο υπολογιστής είναι σε αδράνεια, για την παράταση της διάρκειας ζωής της μπαταρίας.

Για να βελτιστοποιήσετε το φορτίο στο λειτουργικό σύστημα, εκτελέστε τις ακόλουθες ενέργειες:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί 🧔 που βρίσκεται στο κάτω μέρος του παραθύρου.

Ανοίγει το παράθυρο **Ρυθμίσεις**.

3. Επιλέξτε την ενότητα Γενικά και, στην ενότητα Απόδοση, επιλέξτε το πλαίσιο ελέγχου Παραχώρηση πόρων σε άλλες εφαρμογές για να αναβάλετε τις εργασίες σάρωσης για ιούς όταν ο επεξεργαστής (CPU) και τα υποσυστήματα δίσκου βρίσκονται υπό υψηλό φορτίο.

Τρόπος κατάργησης ιχνών δραστηριότητας στον υπολογιστή

Οι ενέργειες του χρήστη σε έναν υπολογιστή καταγράφονται στο λειτουργικό σύστημα. Αποθηκεύονται οι ακόλουθες πληροφορίες:

- Λεπτομέρειες για ερωτήματα αναζήτησης που έχουν εισαχθεί από τους χρήστες και τους δικτυακούς τόπους στους οποίους έχει γίνει επίσκεψη
- Πληροφορίες σχετικά με τις εφαρμογές που έχουν εκκινηθεί, καθώς και για τα ανοικτά και αποθηκευμένα αρχεία
- Καταχωρήσεις στο μητρώο καταγραφής συμβάντων των Microsoft Windows
- Άλλες πληροφορίες σχετικά με τη δραστηριότητα του χρήστη

Οι εισβολείς και άλλα μη εξουσιοδοτημένα άτομα ενδέχεται να αποκτήσουν πρόσβαση στα εμπιστευτικά δεδομένα που περιέχονται στις πληροφορίες προηγούμενων ενεργειών του χρήστη.

Το Kaspersky Total Security περιλαμβάνει τον Οδηγό εκκαθάρισης ιδιωτικού απορρήτου, ο οποίος εκκαθαρίζει τα ίχνη της δραστηριότητας του χρήστη στο λειτουργικό σύστημα.

Για να εκτελέσετε τον Οδηγό εκκαθάρισης ιδιωτικού απορρήτου:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Στο κάτω μέρος του κύριου παραθύρου, κάντε κλικ στο κουμπί Περισσότερα εργαλεία.
 Ανοίγει το παράθυρο Εργαλεία.
- 3. Μεταβείτε στην ενότητα **Εκκαθάριση και βελτιστοποίηση**.
- 4. Κάντε κλικ στη σύνδεση **Εκκαθάριση ιδιωτικού απορρήτου** για να εκτελέσετε τον Οδηγό εκκαθάρισης ιδιωτικού απορρήτου.

Ο Οδηγός αποτελείται από μια σειρά σελίδων (βήματα), στις οποίες μπορείτε να περιηγηθείτε με τα κουμπιά **Πίσω** και **Επόμενο**. Για να κλείσετε τον Οδηγό αφού ολοκληρωθεί, κάντε κλικ στο κουμπί **Ολοκληρώθηκε**. Για να διακόψετε τον Οδηγό σε οποιοδήποτε στάδιο κι αν βρίσκεται, κάντε κλικ στο κουμπί **Άκυρο**.

Ας δούμε αναλυτικότερα τα βήματα του Οδηγού.

Έναρξη του Οδηγού

a. Επιλέξτε μία από τις δύο επιλογές για τη λειτουργία του Οδηγού:

 Αναζήτηση για ίχνη δραστηριότητας χρήστη. Ο Οδηγός θα αναζητήσει ίχνη της δραστηριότητάς σας στον υπολογιστή.

- Επαναφορά αλλαγών. Ο Οδηγός θα επαναφέρει τις αλλαγές που είχαν γίνει προηγούμενα από τον Οδηγό εκκαθάρισης ιδιωτικού απορρήτου. Αυτή η επιλογή είναι διαθέσιμη εάν καταργήθηκαν ίχνη δραστηριότητας από τον Οδηγό σε προγενέστερο χρόνο.
- b. Κάντε κλικ στο κουμπί **Επόμενο** για να ξεκινήσετε τον Οδηγό.

Αναζήτηση για ίχνη δραστηριότητας

Εάν ορίσατε την επιλογή **Αναζήτηση για ίχνη δραστηριότητας χρήστη**, ο Οδηγός εκτελεί αναζήτηση για ίχνη δραστηριότητας στον υπολογιστή σας. Η αναζήτηση ενδέχεται να διαρκέσει αρκετή ώρα. Όταν ολοκληρωθεί η αναζήτηση, ο Οδηγός θα συνεχίσει αυτόματα στο επόμενο βήμα.

Επιλογή των ενεργειών του Προγράμματος εκκαθάρισης ιδιωτικού απορρήτου

Όταν ολοκληρωθεί η αναζήτηση, ο Οδηγός σάς ενημερώνει για τα <u>ίχνη δραστηριότητας</u> που εντόπισε και σας ρωτά για τις ενέργειες που θέλετε να πραγματοποιηθούν για να διαγραφούν αυτά τα ίχνη δραστηριότητας.

Για να προβάλετε τις ενέργειες που περιλαμβάνονται σε μια ομάδα, αναπτύξτε τη λίστα της επιλεγμένης ομάδας.

Για να κάνετε τον Οδηγό να εκτελέσει μια συγκεκριμένη ενέργεια, επιλέξτε το αντίστοιχο πλαίσιο ελέγχου δίπλα στην ενέργεια. Από προεπιλογή, ο Οδηγός εκτελεί όλες τις συνιστώμενες και τις ιδιαίτερα συνιστώμενες ενέργειες. Εάν δεν επιθυμείτε να εκτελεστεί μια συγκεκριμένη ενέργεια, αποεπιλέξτε το πλαίσιο ελέγχου δίπλα της.

Συνιστάται ιδιαίτερα να μην αποεπιλέξετε τα πλαίσια ελέγχου που είναι επιλεγμένα από προεπιλογή, καθώς κάτι τέτοιο θα αφήσει τον υπολογιστή σας ευάλωτο στις απειλές.

Αφού ορίσετε το σύνολο των ενεργειών που θα εκτελέσει ο Οδηγός, κάντε κλικ στο κουμπί **Επόμενο**.

Εκκαθάριση ιδιωτικού απορρήτου

Ο Οδηγός θα εκτελέσει τις ενέργειες που επιλέχθηκαν στο προηγούμενο βήμα. Η εξάλειψη των ιχνών δραστηριότητας μπορεί να διαρκέσει αρκετή ώρα. Για να καθαρίσετε τα ίχνη ορισμένων δραστηριοτήτων, μπορεί να είναι απαραίτητο να κάνετε επανεκκίνηση του υπολογιστή. Εάν ισχύει αυτό, ο οδηγός σάς ειδοποιεί.

Μόλις ολοκληρωθεί η εκκαθάριση, ο Οδηγός θα συνεχίσει αυτόματα στο επόμενο βήμα.

Ολοκλήρωση Οδηγού

Κάντε κλικ στο κουμπί **Ολοκληρώθηκε** για έξοδο από τον Οδηγό.

Τρόπος παύσης και συνέχισης της προστασίας του υπολογιστή

Παύση προστασίας σημαίνει την προσωρινή απενεργοποίηση όλων των στοιχείων προστασίας για κάποιο χρονικό διάστημα.

Όταν η προστασία είναι σε παύση ή το Kaspersky Total Security δεν εκτελείται, η δραστηριότητα των εφαρμογών που εκτελούνται στον υπολογιστή σας παρακολουθείται. Οι πληροφορίες σχετικά με τα αποτελέσματα της παρακολούθησης της δραστηριότητας των εφαρμογών αποθηκεύονται στο λειτουργικό σύστημα. Όταν εκκινείται ξανά το Kaspersky Total Security ή επανενεργοποιείται η προστασία, η εφαρμογή χρησιμοποιεί αυτές τις πληροφορίες για να προστατεύσει τον υπολογιστή σας από κακόβουλες ενέργειες που μπορεί να έχουν εκτελεστεί όταν ήταν σε παύση η προστασία σας ή όταν το Kaspersky Total Security ήταν εκτός λειτουργίας. Οι πληροφορίες σχετικά με τα αποτελέσματα της παρακολούθησης της δραστηριότητας των εφαρμογών αποθηκεύονται επ' αόριστον. Οι πληροφορίες αυτές διαγράφονται σε περίπτωση κατάργησης του Kaspersky Total Security από τον υπολογιστή σας.

Για να θέσετε σε παύση την προστασία του υπολογιστή σας:

1. Στο μενού περιβάλλοντος του εικονιδίου της εφαρμογής που βρίσκεται στην περιοχή ειδοποιήσεων της γραμμής εργασιών, επιλέξτε το στοιχείο **Παύση προστασίας**.

Ανοίγει το παράθυρο **Παύση προστασίας** (βλ. παρακάτω εικόνα).

Pause protection —	\times
 Pause protection Pause for 1 minute ~ Pause until application restart 	0
O Pause	
Pause protection Cancel	



- Στο παράθυρο Παύση προστασίας, επιλέξτε το χρονικό διάστημα μετά από το οποίο θα συνεχιστεί η προστασία:
 - Παύση για η προστασία θα ενεργοποιηθεί όταν παρέλθει το χρονικό διάστημα που θα επιλεγεί από την αναπτυσσόμενη λίστα.
 - Παύση μέχρι επανεκκίνηση της εφαρμογής η προστασία θα ενεργοποιηθεί μετά από την επανεκκίνηση της εφαρμογής ή του λειτουργικού συστήματος (εφόσον η εφαρμογή εκτελείται αυτομάτως κατά την εκκίνηση).

- Παύση η προστασία θα ενεργοποιηθεί μόνο όταν εσείς αποφασίσετε να την συνεχίσετε.
- Κάντε κλικ στο κουμπί Παύση προστασίας για να επιβεβαιώσετε την επιλογή σας στο παράθυρο που θα εμφανιστεί.

<u>Συνέχιση της προστασίας του υπολογιστή </u>

Για να συνεχίσετε την προστασία του υπολογιστή:

Στην περιοχή ειδοποιήσεων της γραμμής εργασιών, στο μενού περιβάλλοντος του εικονιδίου της εφαρμογής, επιλέξτε **Συνέχιση προστασίας**.

Τρόπος επαναφοράς των προεπιλεγμένων ρυθμίσεων της εφαρμογής

Μπορείτε να επαναφέρετε οποιαδήποτε στιγμή τις προεπιλεγμένες ρυθμίσεις της εφαρμογής που συνιστώνται από την Kaspersky για το Kaspersky Total Security. Όταν γίνεται επαναφορά των ρυθμίσεων, ορίζεται για όλα τα στοιχεία προστασίας το επίπεδο ασφάλειας **Συνιστάται**.

Για να επαναφέρετε τις προεπιλεγμένες ρυθμίσεις λειτουργίας της εφαρμογής:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Διαχείριση ρυθμίσεων**.
- 4. Κάντε κλικ στη σύνδεση **Επαναφορά** για να εκτελέσετε τον Οδηγό επαναφοράς ρυθμίσεων.
- 5. Κάντε κλικ στο κουμπί **Επόμενο**.

Το παράθυρο του Οδηγού δείχνει την πρόοδο στην επαναφορά των προεπιλεγμένων ρυθμίσεων εφαρμογής που είχαν ορίσει οι ειδικοί της Kaspersky.

6. Αφού ολοκληρωθεί η διαδικασία επαναφοράς των προεπιλεγμένων ρυθμίσεων της εφαρμογής, κάντε κλικ στο κουμπί **Ολοκληρώθηκε**.

Τρόπος προβολής της αναφοράς λειτουργίας της εφαρμογής

To Kaspersky Total Security διατηρεί αναφορές λειτουργίας για κάθε ένα από τα στοιχεία προστασίας. Με τις αναφορές, μπορείτε να αποκτήσετε στατιστικές πληροφορίες σχετικά με τη λειτουργία της εφαρμογής (για παράδειγμα, για να ανακαλύψετε πόσα κακόβουλα αντικείμενα εντοπίστηκαν και εξουδετερώθηκαν στη διάρκεια μιας καθορισμένης χρονικής περιόδου, πόσες φορές ενημερώθηκαν οι βάσεις δεδομένων και οι λειτουργικές μονάδες της εφαρμογής κατά την ίδια περίοδο, πόσα μηνύματα spam διαγράφηκαν και πολλά άλλα).

Για να προβάλετε την αναφορά λειτουργίας της εφαρμογής:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Στο κάτω μέρος του κύριου παραθύρου, κάντε κλικ στο κουμπί Περισσότερα εργαλεία.
 Ανοίγει το παράθυρο Εργαλεία.
- Στο παράθυρο Εργαλεία, κάντε κλικ στη σύνδεση Αναφορές για να μεταβείτε στο παράθυρο Αναφορές.

Το παράθυρο **Αναφορές** εμφανίζει δεδομένα με τη μορφή πίνακα. Για μια πιο εύχρηστη προβολή των αναφορών, μπορείτε να ορίσετε διάφορες επιλογές φιλτραρίσματος.

Τρόπος εφαρμογής των ρυθμίσεων εφαρμογών σε άλλο υπολογιστή

Αφού ρυθμίσετε τις παραμέτρους της εφαρμογής, μπορείτε να εφαρμόσετε τις ρυθμίσεις του σε κάποια άλλη εγκατάσταση του Kaspersky Total Security σε άλλον υπολογιστή. Ως αποτέλεσμα, η εφαρμογή μπορεί να ρυθμιστεί πανομοιότυπα και στους δύο υπολογιστές.

Οι ρυθμίσεις της εφαρμογής αποθηκεύονται σε ένα αρχείο ρύθμισης παραμέτρων, το οποίο μπορείτε να μεταφέρετε από τον έναν υπολογιστή στον άλλον.

Η μεταφορά των ρυθμίσεων του Kaspersky Total Security από τον έναν υπολογιστή στον άλλον γίνεται με τα εξής τρία βήματα:

- 1. Αποθήκευση των ρυθμίσεων της εφαρμογής σε ένα αρχείο ρύθμισης παραμέτρων.
- Μεταφορά του αρχείου ρύθμισης παραμέτρων στον άλλο υπολογιστή (για παράδειγμα, μέσω μηνύματος email ή σε αφαιρούμενη μονάδα δίσκου).
- Εισαγωγή των ρυθμίσεων από το αρχείο ρύθμισης παραμέτρων στην εφαρμογή που είναι εγκατεστημένη στον δεύτερο υπολογιστή.

<u>Τρόπος εξαγωγής των ρυθμίσεων της εφαρμογής ?</u>

Για την εξαγωγή των ρυθμίσεων της εφαρμογής:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Στο παράθυρο **Ρυθμίσεις**, επιλέξτε την ενότητα **Διαχείριση ρυθμίσεων**.
- 4. Επιλέξτε **Εξαγωγή**.
- 5. Ανοίγει το παράθυρο **Αποθήκευση**.
- 6. Ορίστε ένα όνομα για το αρχείο ρύθμισης παραμέτρων και κάντε κλικ στο κουμπί **Αποθήκευση**.

Οι ρυθμίσεις της εφαρμογής έχουν αποθηκευτεί στο αρχείο ρύθμισης παραμέτρων.

Μπορείτε επίσης να εξάγετε τις ρυθμίσεις της εφαρμογής από τη γραμμή εντολών, χρησιμοποιώντας την ακόλουθη εντολή: avp.com EXPORT <file_name>.

<u>Τρόπος εισαγωγής των ρυθμίσεων της εφαρμογής</u> ?

Για την εισαγωγή των ρυθμίσεων σε μια εγκατάσταση της εφαρμογής σε άλλον υπολογιστή:

- 1. Στον δεύτερο υπολογιστή, ανοίξτε το κύριο παράθυρο του Kaspersky Total Security.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Στο παράθυρο **Ρυθμίσεις**, επιλέξτε την ενότητα **Διαχείριση ρυθμίσεων**.
- 4. Επιλέξτε **Εισαγωγή**.

Θα ανοίξει το παράθυρο Άνοιγμα.

5. Καθορίστε το αρχείο ρύθμισης παραμέτρων και κάντε κλικ στο κουμπί **Άνοιγμα**.

Οι ρυθμίσεις εισάγονται στην εφαρμογή που είναι εγκατεστημένη στον άλλο υπολογιστή.

Συμμετοχή στο Kaspersky Security Network

Το Kaspersky Total Security χρησιμοποιεί την προστασία cloud για να παρέχει αποτελεσματικότερη προστασία στον υπολογιστή σας. Η προστασία cloud παρέχεται με τη χρήση της υποδομής Kaspersky Security Network που χρησιμοποιεί δεδομένα τα οποία λαμβάνονται από χρήστες από όλο τον κόσμο.

To Kaspersky Security Network (KSN) είναι η γνωσιακή βάση της Kaspersky που βασίζεται σε cloud με πληροφορίες σχετικά με την αξιοπιστία των εφαρμογών και των δικτυακών τόπων. Η χρήση δεδομένων από το Kaspersky Security Network διασφαλίζει την ταχύτερη απόκριση του Kaspersky Total Security όταν εμφανίζονται νέοι τύποι απειλών, βελτιώνει την απόδοση ορισμένων στοιχείων προστασίας και μειώνει την πιθανότητα εμφάνισης ψευδών θετικών αποτελεσμάτων.

Χάρη στους χρήστες που συμμετέχουν στο Kaspersky Security Network, η Kaspersky είναι σε θέση να συγκεντρώνει άμεσα πληροφορίες σχετικά με τους τύπους και τις προελεύσεις νέων απειλών, να αναπτύσσει λύσεις για την εξουδετέρωσή τους και να ελαχιστοποιεί τον αριθμό των ψευδών θετικών αποτελεσμάτων. Συμμετέχοντας στο Kaspersky Security Network αποκτάτε τη δυνατότητα πρόσβασης σε στατιστικά στοιχεία σχετικά με την αξιοπιστία εφαρμογών και δικτυακών τόπων.

Εάν συμμετέχετε στο Kaspersky Security Network, αποστέλλετε αυτομάτως <u>στην</u> <u>Kaspersky πληροφορίες σχετικά με τη ρύθμιση παραμέτρων του λειτουργικού</u> <u>συστήματός σας, καθώς την ώρα έναρξης και ολοκλήρωσης των διαδικασιών του</u> <u>Kaspersky Total Security</u>.

Πώς να ενεργοποιήσετε ή να απενεργοποιήσετε τη συμμετοχή στο Kaspersky Security Network

Η συμμετοχή στο Kaspersky Security Network είναι εθελοντική. Μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε τη χρήση του Kaspersky Security Network (KSN) κατά την εγκατάσταση του Kaspersky Total Security και/ή οποιαδήποτε στιγμή μετά από την εγκατάσταση της εφαρμογής.

Για να ενεργοποιήσετε ή να απενεργοποιήσετε τη συμμετοχή στο Kaspersky Security Network:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Κάντε κλικ στο κουμπί 🧔 που βρίσκεται στο κάτω μέρος του παραθύρου.

Ανοίγει το παράθυρο Ρυθμίσεις.

3. Στην ενότητα **Προστασία**, επιλέξτε τον αποκλεισμό **Kaspersky Security Network**.

Ανοίγει το παράθυρο **Kaspersky Security Network** με λεπτομέρειες για το Kaspersky Security Network και τις ρυθμίσεις συμμετοχής στο Kaspersky Security Network.

- 4. Ενεργοποιήστε ή απενεργοποιήστε τη συμμετοχή στο Kaspersky Security Network χρησιμοποιώντας τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου:
 - Εάν θέλετε να συμμετάσχετε στο Kaspersky Security Network, κάντε κλικ στον διακόπτη εναλλαγής Ενεργό.

Εμφανίζεται ένα παράθυρο με το κείμενο της δήλωσης του Kaspersky Security Network. Εάν αποδέχεστε τους όρους της δήλωσης, κάντε κλικ στο κουμπί **Συμφωνώ**.

 Εάν δεν θέλετε να συμμετάσχετε στο Kaspersky Security Network, κάντε κλικ στον διακόπτη εναλλαγής Ανενεργό.

Σε <u>ορισμένες εκδόσεις της εφαρμογής</u>, το παράθυρο **Kaspersky Security Network** εμφανίζει την ενότητα **Δήλωση για το Kaspersky Security Network** αντί για τις πληροφορίες σχετικά με το Kaspersky Security Network.

Για να αποδεχτείτε τη Δήλωση για το Kaspersky Security Network:

1. Κάντε κλικ στο κουμπί **Αποδοχή** στην ενότητα **Δήλωση για το Kaspersky Security Network**.

Ανοίγει η Δήλωση για το Kaspersky Security Network. Αυτή η δήλωση επιτρέπει στους ειδικούς της Kaspersky να λάβουν άμεσα πληροφορίες σχετικά με απειλές που εντοπίζονται στον υπολογιστή σας, με εφαρμογές που εκτελούνται και υπογεγραμμένες εφαρμογές που έχουν ληφθεί, καθώς και πληροφορίες σχετικά με το λειτουργικό σύστημα για τη βελτίωση της προστασίας σας.

2. Εάν αποδέχεστε τους όρους της δήλωσης, κάντε κλικ στο κουμπί **Αποδοχή**.

Για να απορρίψετε τη Δήλωση για το Kaspersky Security Network,

κάντε κλικ στο κουμπί **Άρνηση** στην ενότητα **Δήλωση για το Kaspersky Security Network**.

Πώς να ελέγξετε τη σύνδεση με το Kaspersky Security Network

Η σύνδεσή σας με το Kaspersky Security Network μπορεί να χαθεί για τις ακόλουθες αιτίες:

- Δεν συμμετέχετε στο Kaspersky Security Network.
- Ο υπολογιστής σας δεν είναι συνδεδεμένος στο Διαδίκτυο.
- Η τρέχουσα κατάσταση του κλειδιού δεν επιτρέπει τη σύνδεση με το Kaspersky Security Network. Για παράδειγμα, μια σύνδεση με το KSN ενδέχεται να μην είναι διαθέσιμη για τους ακόλουθους λόγους:
 - Η εφαρμογή δεν είναι ενεργοποιημένη.
 - Η άδεια ή η συνδρομή έχει λήξει.
 - Έχουν εντοπιστεί ζητήματα κλειδιών άδειας χρήσης (για παράδειγμα, το κλειδί έχει προστεθεί στη λίστα μη επιτρεπόμενων στοιχείων).

Η τρέχουσα κατάσταση του κλειδιού εμφανίζεται στο παράθυρο **Εκχώρηση άδειας χρήσης**.

Για να δοκιμάσετε τη σύνδεση με το Kaspersky Security Network:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Στο κάτω μέρος του κύριου παραθύρου, κάντε κλικ στο κουμπί Περισσότερα εργαλεία.
 Ανοίγει το παράθυρο Εργαλεία.
- 3. Στο παράθυρο **Εργαλεία**, μεταβείτε στην ενότητα **Ασφάλεια**.

Στο παράθυρο **Ασφάλεια**, κάντε κλικ στη σύνδεση **Προστασία cloud** για να ανοίξετε το παράθυρο **Προστασία cloud**. Το παράθυρο **Προστασία cloud** εμφανίζει την κατάσταση της σύνδεσής σας με το Kaspersky Security Network.

Σε ορισμένες περιπτώσεις, η Kaspersky μπορεί να επιβάλει προσωρινούς περιορισμούς στις αιτήσεις προς το Kaspersky Security Network για την αξιοπιστία αρχείων. Όταν επιβάλλονται προσωρινοί περιορισμοί στις αιτήσεις παροχής πληροφοριών προς το Kaspersky Security Network, εμφανίζεται η αντίστοιχη ειδοποίηση.

Προστασία με χρήση λειτουργίας αναπαράστασης υλικού

Σε αυτή την ενότητα θα μάθετε πώς μπορείτε να προστατεύσετε τον υπολογιστή σας, χρησιμοποιώντας την αναπαράσταση υλικού.

Σχετικά με την προστασία κατά τη χρήση εικονικοποίησης υλικού

Όταν το Kaspersky Total Security είναι εγκατεστημένο σε υπολογιστή που λειτουργεί με έκδοση 64-bit των Microsoft Windows 8, Microsoft Windows 8.1 ή Microsoft Windows 10, χρησιμοποιεί τεχνολογία <u>hypervisor</u> (2) για πρόσθετη προστασία απέναντι σε προηγμένο κακόβουλο λογισμικό που μπορεί να υποκλέψει προσωπικά δεδομένα με χρήση του προχείρου ή phishing.

Η προστασία με χρήση εικονικοποίησης υλικού είναι ενεργοποιημένη από προεπιλογή. Εάν η εν λόγω προστασία έχει απενεργοποιηθεί χειροκίνητα, μπορείτε να την <u>ενεργοποιήσετε ξανά</u> <u>από το παράθυρο ρυθμίσεων της εφαρμογής</u>.

Σε υπολογιστές που λειτουργούν με έκδοση 64-bit των Microsoft Windows 8, Microsoft Windows 8.1 ή Microsoft Windows 10, η προστασία που παρέχεται από την εικονικοποίηση υλικού του Kaspersky Total Security έχει τους εξής περιορισμούς:

- Αυτή η δυνατότητα δεν είναι διαθέσιμη όταν εκτελείται ένα hypervisor τρίτου προμηθευτή, όπως το hypervisor εικονικοποίησης VMware. Αφού τερματίσετε το hypervisor τρίτου προμηθευτή, η προστασία ενάντια στα στιγμιότυπα οθόνης θα ενεργοποιηθεί ξανά.
- Η δυνατότητα αυτή δεν είναι διαθέσιμη εάν η CPU του υπολογιστή σας δεν υποστηρίζει την τεχνολογία εικονικοποίησης υλικού. Για περισσότερες λεπτομέρειες σχετικά με το κατά πόσον η CPU σας υποστηρίζει την εικονικοποίηση υλικού, ανατρέξτε στην τεκμηρίωση του υπολογιστή σας ή στον δικτυακό τόπο του κατασκευαστή της CPU.
- Η δυνατότητα αυτή δεν είναι διαθέσιμη εάν εκτελείται το hypervisor ενός τρίτου προμηθευτή (όπως το hypervisor VMware) κατά την εκκίνηση του Προστατευμένου προγράμματος περιήγησης.
- Η δυνατότητα δεν είναι διαθέσιμη εάν η εικονικοποίηση υλικού είναι απενεργοποιημένη στον υπολογιστή σας. Για λεπτομέρειες σχετικά με τον τρόπο ενεργοποίησης της εικονικοποίησης υλικού στον υπολογιστή σας, ανατρέξτε στην τεχνική τεκμηρίωση του υπολογιστή σας ή επισκεφτείτε τον δικτυακό τόπο του κατασκευαστή του επεξεργαστή σας.
- Η λειτουργία δεν είναι διαθέσιμη εάν το Device Guard είναι ενεργοποιημένο στο λειτουργικό σύστημα Microsoft Windows 10.

 Η λειτουργία δεν είναι διαθέσιμη εάν η ασφάλεια με βάση τη λειτουργία αναπαράστασης είναι ενεργοποιημένη στο λειτουργικό σύστημα Microsoft Windows 10.

Πώς να ενεργοποιήσετε την προστασία με χρήση εικονικοποίησης υλικού

Για να ενεργοποιήσετε την προστασία με χρήση εικονικοποίησης υλικού:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🥶 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Πρόσθετα**.
- 4. Επιλέξτε το πλαίσιο ελέγχου Χρήση λειτουργίας αναπαράστασης υλικού εάν είναι διαθέσιμη. Αυτό το πλαίσιο ελέγχου εμφανίζεται όταν η εφαρμογή εγκαθίσταται σε έκδοση 64-bit των Windows 8, Windows 8.1 και Windows 10.
- 5. Επιλέξτε το πλαίσιο ελέγχου **Χρήση λειτουργίας αναπαράστασης υλικού για προχωρημένους**, αν θέλετε να ενεργοποιείται η αναπαράσταση υλικού κατά την εκκίνηση του λειτουργικού συστήματος.

Εάν η εικονικοποίηση υλικού είναι απενεργοποιημένη στον υπολογιστή σας, θα απενεργοποιηθεί και η προστασία με χρήση εικονικοποίησης υλικού.

Προστασία χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface (AMSI)

Αυτή η ενότητα σας ενημερώνει ότι εφαρμογές τρίτων όπως το Microsoft Office μπορούν να στείλουν δέσμες ενεργειών στο Kaspersky Total Security για σάρωση χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface (AMSI) και περιγράφει τον τρόπο απενεργοποίησης της προστασίας χρησιμοποιώντας τη λειτουργία AMSI στο Kaspersky Total Security.

Σχετικά με την προστασία χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface

Η λειτουργία Antimalware Scan Interface (AMSI) επιτρέπει σε μια εφαρμογή τρίτων που υποστηρίζει AMSI να στέλνει αντικείμενα (για παράδειγμα, δέσμες ενεργειών PowerShell) στο Kaspersky Total Security για επιπλέον σάρωση και να λαμβάνει τα αποτελέσματα σάρωσης για τα συγκεκριμένα αντικείμενα. Για παράδειγμα, οι εφαρμογές του Microsoft Office μπορεί να αποτελούν εφαρμογές τρίτων. Για περισσότερες πληροφορίες σχετικά με τη διεπαφή AMSI, ανατρέξτε στην <u>τεκμηρίωση της Microsoft</u>

Η λειτουργία Antimalware Scan Interface επιτρέπει μόνο τον εντοπισμό μιας απειλής και την ειδοποίηση μιας εφαρμογής τρίτων σχετικά με την απειλή που εντοπίστηκε. Μετά τη λήψη της ειδοποίησης απειλής, η εφαρμογή τρίτου μέρους αποτρέπει κακόβουλες ενέργειες (για παράδειγμα, τερματίζεται).

Το Kaspersky Total Security ενδέχεται να απορρίψει ένα αίτημα από μια εφαρμογή τρίτων εάν, για παράδειγμα, η εφαρμογή αυτή υπερβαίνει τον μέγιστο επιτρεπόμενο αριθμό αιτημάτων για μια περίοδο. Σε αυτήν την περίπτωση, το Kaspersky Total Security εμφανίζει μια ειδοποίηση σχετικά με το αίτημα που απορρίφθηκε. Εάν λάβετε μια τέτοια ειδοποίηση, δεν χρειάζεται να εκτελέσετε καμία ενέργεια.

Η προστασία με χρήση της λειτουργίας Antimalware Scan Interface διατίθεται στα λειτουργικά συστήματα Windows 10 Home/Pro/Education/Enterprise.

Πώς να ενεργοποιήσετε την προστασία χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface

Για να ενεργοποιήσετε την προστασία χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Στην ενότητα **Προστασία**, επιλέξτε **Προστασία AMSI**.
- 4. Ρυθμίστε τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου σε **Ενεργό**.

Πώς να εξαιρέσετε μια δέσμη ενεργειών από τη σάρωση χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface Για να εξαιρέσετε μια δέσμη ενεργειών από τη σάρωση χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί ο που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- 3. Επιλέξτε την ενότητα **Προστασία**.
- 4. Επιλέξτε το στοιχείο Προστασία αρχείων από ιούς.Ανοίγει το παράθυρο Ρυθμίσεις της Προστασίας αρχείων από ιούς.
- 5. Κάντε κλικ στη σύνδεση **Ρυθμίσεις για προχωρημένους** για να μεταβείτε στο παράθυρο **Ρυθμίσεις προστασίας αρχείων από ιούς για προχωρημένους**.
- 6. Στην ενότητα **Σαρωτής δέσμης ενεργειών**, επιλέξτε το πλαίσιο ελέγχου Πραγματοποιήστε σάρωση των δεσμών ενεργειών χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface (AMSI).
- Κάντε κλικ στη σύνδεση Διαχείριση εξαιρέσεων για να μεταβείτε στο παράθυρο Εξαιρέσεις.
- 8. Στο παράθυρο **Εξαιρέσεις**, κάντε κλικ στο κουμπί **Προσθήκη**.

Ανοίγει το παράθυρο Προσθήκη νέας εξαίρεσης.

- 9. Στο πεδίο **Αρχείο ή φάκελος**, καθορίστε τον φάκελο με τη δέσμη ενεργειών.
- 10. Στο πεδίο **Αντικείμενο**, καθορίστε το όνομα της δέσμης ενεργειών.

Μπορείτε επίσης να προσθέσετε πολλά αρχεία του ίδιου τύπου στις εξαιρέσεις χρησιμοποιώντας μια μάσκα.

- Στην ενότητα Στοιχεία προστασίας, επιλέξτε το πλαίσιο ελέγχου δίπλα στο στοιχείο Προστασία αρχείων από ιούς.
- 12. Επιλέξτε την κατάσταση **Ενεργό**.

Το καθορισμένο αντικείμενο δεν θα σαρωθεί χρησιμοποιώντας τη λειτουργία Antimalware Scan Interface.

Χρήση της εφαρμογής από τη γραμμή εντολών

Μπορείτε να χρησιμοποιήσετε το Kaspersky Total Security στη γραμμή εντολών.

Σύνταξη γραμμής εντολών:

avp.com <εντολή> [settings]

Για να εμφανιστεί η βοήθεια σχετικά με τη σύνταξη στη γραμμή εντολών, εισαγάγετε την εξής εντολή:

avp.com [/? | HELP]

Με αυτήν την εντολή θα αποκτήσετε πρόσβαση στην πλήρη λίστα με τις εντολές που είναι διαθέσιμες για τη διαχείριση του Kaspersky Total Security μέσω της γραμμής εντολών.

Για να αποκτήσετε πρόσβαση στη βοήθεια σχετικά με μια συγκεκριμένη εντολή, μπορείτε να εισαγάγετε μία από τις παρακάτω εντολές:

avp.com <εντολή> /? avp.com HELP <εντολή>

Στη γραμμή εντολών, μπορείτε να ανατρέξετε στην εφαρμογή είτε από τον φάκελο εγκατάστασης της εφαρμογής είτε ορίζοντας την πλήρη διαδρομή προς το avp.com.

Μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε την καταγραφή συμβάντων εφαρμογής (δημιουργώντας αρχεία ιχνών) από τη γραμμή εντολών αν έχετε ορίσει προηγουμένως <u>έναν</u> <u>κωδικό πρόσβασης</u> για την προστασία της πρόσβασης στη διαχείριση του Kaspersky Total Security στο παράθυρο ρυθμίσεων της εφαρμογής.

Αν δεν έχετε ορίσει κωδικό πρόσβασης στο παράθυρο ρυθμίσεων της εφαρμογής, δεν μπορείτε να δημιουργήσετε κωδικό πρόσβασης και να ενεργοποιήσετε την καταγραφή συμβάντων εφαρμογής από τη γραμμή εντολών.

Ορισμένες εντολές μπορούν να εκτελεστούν μόνο από τον λογαριασμό διαχειριστή.

Αξιολόγηση του Kaspersky Total Security

Μπορείτε να αξιολογήσετε το Kaspersky Total Security και να στείλετε τη βαθμολογία σας στην Kaspersky. Κάποια στιγμή μετά την εγκατάσταση, η εφαρμογή σας δίνει την ευκαιρία να αξιολογήσετε τη λειτουργία της.

Για την αξιολόγηση του Kaspersky Total Security:

- 1. Στο παράθυρο **Εκτιμούμε τη γνώμη σας**, κάντε ένα από τα εξής:
 - Εάν είστε έτοιμοι να αξιολογήσετε το Kaspersky Total Security, κατατάξτε την εφαρμογή σε μια κλίμακα 10 σημείων.
 - Εάν δεν θέλετε να αξιολογήσετε το Kaspersky Total Security, κάντε κλικ στο κουμπί ×, για να κλείσει το παράθυρο αξιολόγησης.
- 2. Κάντε κλικ στο κουμπί **Αποστολή**.
- 3. Κάντε κλικ στο κουμπί **Κλείσιμο**, για να κλείσετε τον παράθυρο.

Επικοινωνία με την Τεχνική υποστήριξη

Η ενότητα αυτή περιγράφει τους τρόπους με τους οποίους μπορείτε να λάβετε τεχνική υποστήριξη και τους όρους με τους οποίους διατίθεται αυτή η υποστήριξη.

Τρόπος λήψης τεχνικής υποστήριξης

Εάν δεν μπορείτε να βρείτε μια λύση για το ζήτημά σας στο κείμενο Βοήθειας της εφαρμογής ή σε κάποια από τις πηγές ενημέρωσης σχετικά με την εφαρμογή, συνιστάται να επικοινωνήσετε με την Τεχνική υποστήριξη της Kaspersky. Οι ειδικοί της Τεχνικής υποστήριξης θα απαντήσουν σε οποιαδήποτε ερώτηση έχετε σχετικά με την εγκατάσταση και τη χρήση της εφαρμογής.

Προτού επικοινωνήσετε με την Υπηρεσία τεχνικής υποστήριξης, διαβάστε τους <u>κανόνες</u> <u>υποστήριξης</u> .

Μπορείτε να επικοινωνήσετε με την Τεχνική υποστήριξη με έναν από τους ακόλουθους τρόπους:

- Μέσω τηλεφώνου. Με τη μέθοδο αυτή, μπορείτε να συμβουλευτείτε τους ειδικούς μας από τη ρωσόφωνη ή την αγγλόφωνη Τεχνική υποστήριξη.
- Να στείλετε το αίτημά σας μέσω της τοποθεσίας web My Kaspersky. Με τη μέθοδο αυτή, μπορείτε να επικοινωνήσετε με τους ειδικούς μας χρησιμοποιώντας τη φόρμα

ερωτήματος.

Η τεχνική υποστήριξη είναι διαθέσιμη μόνο στους χρήστες που έχουν αγοράσει άδεια χρήσης για την εφαρμογή. Δεν παρέχεται τεχνική υποστήριξη σε χρήστες δοκιμαστικών εκδόσεων.

Τεχνική υποστήριξη μέσω τηλεφώνου

Μπορείτε να καλέσετε την Τεχνική υποστήριξη από τις περισσότερες περιοχές του κόσμου. Θα βρείτε πληροφορίες σχετικά με τη λήψη τεχνικής υποστήριξης στην περιοχή σας και τα αντίστοιχα στοιχεία επικοινωνίας στον <u>δικτυακό τόπο της Υπηρεσίας τεχνικής υποστήριξης</u> της Kaspersky 2.

Προτού επικοινωνήσετε με την Υπηρεσία τεχνικής υποστήριξης, διαβάστε τους <u>κανόνες</u> <u>υποστήριξης</u> .

Τεχνική υποστήριξη μέσω του My Kaspersky

To <u>My Kaspersky</u> I^{II} είναι μια υπηρεσία μίας στάσης για τη διαχείριση της προστασίας των συσκευών σας και των κωδικών ενεργοποίησής σας για τις εφαρμογές της Kaspersky, καθώς και για την αναζήτηση τεχνικής υποστήριξης.

Για να αποκτήσετε πρόσβαση στην τοποθεσία web My Kaspersky, πρέπει να εγγραφείτε. Για να το κάνετε αυτό, εισαγάγετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σας και δημιουργήστε έναν κωδικό πρόσβασης.

Μπορείτε να λάβετε τεχνική υποστήριξη μέσω της τοποθεσίας web My Kaspersky με τους εξής τρόπους:

- Αποστολή αιτημάτων μέσω email στην Τεχνική υποστήριξη
- Επικοινωνία με την Τεχνική υποστήριξη χωρίς τη χρήση email
- Παρακολούθηση της κατάστασης των αιτημάτων σας σε πραγματικό χρόνο

Μπορείτε επίσης να δείτε το πλήρες ιστορικό των αιτημάτων τεχνικής υποστήριξής σας.

Αίτημα μέσω ηλεκτρονικού ταχυδρομείου στην Υπηρεσία τεχνικής υποστήριξης

Το μήνυμά σας προς την Υπηρεσία τεχνικής υποστήριξης πρέπει να περιέχει τις εξής πληροφορίες:

- Θέμα μηνύματος
- Όνομα εφαρμογής και αριθμός έκδοσης
- Όνομα και αριθμός έκδοσης λειτουργικού συστήματος
- Περιγραφή προβλήματος

Ένας ειδικός της Τεχνικής υποστήριξης θα απαντήσει στο ερώτημά σας μέσω μηνύματος στην τοποθεσία web My Kaspersky και στη διεύθυνση email που προσδιορίσατε κατά την εγγραφή.

Συλλογή πληροφοριών για τεχνική υποστήριξη

Αφού ειδοποιήσετε τους ειδικούς της Τεχνικής υποστήριξης για κάποιο πρόβλημα, οι ειδικοί μας μπορεί να σας ζητήσουν να δημιουργήσετε μια αναφορά που περιέχει πληροφορίες σχετικά με το λειτουργικό σας σύστημα και να την στείλετε στην Τεχνική υποστήριξη. Οι ειδικοί της Υπηρεσίας τεχνικής υποστήριξης μπορεί να σας ζητήσουν να δημιουργήσετε ένα αρχείο ιχνών. Το αρχείο ιχνών επιτρέπει την ιχνηλάτηση βήμα-βήμα της διαδικασίας εκτέλεσης των εντολών της εφαρμογής και τον εντοπισμό του σταδίου της λειτουργίας της εφαρμογής και το σφάλμα.

Για καλύτερη υποστήριξη σε ζητήματα που σχετίζονται με τη λειτουργία της εφαρμογής, οι ειδικοί Τεχνικής υποστήριξης μπορεί να σας ζητήσουν να αλλάξετε προσωρινά τις ρυθμίσεις της εφαρμογής για τους σκοπούς του εντοπισμού σφαλμάτων, όσο βρίσκονται σε εξέλιξη οι διαγνωστικοί έλεγχοι. Για να το κάνετε αυτό, μπορεί να χρειαστεί να εκτελέσετε τις εξής ενέργειες:

- Να συλλέξετε εκτεταμένες διαγνωστικές πληροφορίες
- Να ρυθμίσετε τις παραμέτρους μεμονωμένων στοιχείων της εφαρμογής αλλάζοντας ειδικές ρυθμίσεις που είναι προσβάσιμες μέσω του τυπικού περιβάλλοντος εργασίας χρήστη
- Να ρυθμίσετε εκ νέου τις παραμέτρους αποθήκευσης και αποστολής των διαγνωστικών πληροφοριών που συλλέγονται
- Να ρυθμίσετε την καταγραφή της κυκλοφορίας δικτύου και την αποθήκευσή της σε ένα αρχείο

Οι ειδικοί Τεχνικής υποστήριξης θα σας δώσουν όλες τις απαραίτητες πληροφορίες για την εκτέλεση αυτών των ενεργειών (οδηγίες βήμα-βήμα, ρυθμίσεις που πρέπει να τροποποιηθούν, δέσμες ενεργειών, πρόσθετες λειτουργίες γραμμής εντολών, λειτουργικές μονάδες εντοπισμού σφαλμάτων, ειδικά βοηθητικά προγράμματα κτλ.) και θα σας ενημερώσουν σχετικά με το ποια δεδομένα πρόκειται να συλλεχθούν για τους σκοπούς το εντοπισμού σφαλμάτων. Μόλις ολοκληρωθεί η συλλογή των εκτεταμένων διαγνωστικών πληροφοριών, αυτές αποθηκεύονται στον υπολογιστή του χρήστη. Τα δεδομένα που συλλέγονται δεν αποστέλλονται αυτόματα στην Kaspersky.

Σας συνιστούμε να εκτελέσετε τις προαναφερόμενες ενέργειες μόνο αν σας ζητηθεί από έναν ειδικό Τεχνικής υποστήριξης και ακολουθώντας τις οδηγίες του. Αν επιχειρήσετε να αλλάξετε τις ρυθμίσεις της εφαρμογής μόνος σας και με τρόπους που δεν περιγράφονται στη Βοήθεια ή δεν συνιστώνται από τους ειδικούς Τεχνικής υποστήριξης, ενδεχομένως να προκληθεί επιβράδυνση της λειτουργίας ή σφάλμα στο λειτουργικό σύστημα, να μειωθεί το επίπεδο προστασίας του υπολογιστή σας και να διαταραχθεί η διαθεσιμότητα και ακεραιότητα των πληροφοριών που υποβάλλονται σε επεξεργασία.

Σχετικά με τα περιεχόμενα και την αποθήκευση των αρχείων δεδομένων υπηρεσίας

Τα αρχεία ιχνών και τα αρχεία ένδειξης σφαλμάτων αποθηκεύονται στον υπολογιστή σας σε μη κρυπτογραφημένη μορφή για περίοδο επτά ημερών μετά την απενεργοποίηση της καταγραφής δεδομένων. Τα αρχεία ιχνών και τα αρχεία ένδειξης σφαλμάτων διαγράφονται οριστικά μετά από επτά ημέρες.

Τα αρχεία ιχνών αποθηκεύονται στον φάκελο ProgramData\Kaspersky Lab.

H μορφή των ονομάτων των αρχείων ιχνών έχει ως εξής: KAV<version number_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log.

Τα αρχεία ιχνών μπορούν να περιέχουν εμπιστευτικά δεδομένα. Μπορείτε να δείτε τα περιεχόμενα ενός αρχείου ιχνών ανοίγοντάς το σε ένα πρόγραμμα επεξεργασίας κειμένου (όπως το Σημειωματάριο).

Μπορείτε να δείτε αρχεία ιχνών απόδοσης χρησιμοποιώντας το βοηθητικό πρόγραμμα Windows Performance Analyzer. Μπορείτε να πραγματοποιήσετε λήψη αυτού του βοηθητικού προγράμματος από την τοποθεσία web της Microsoft.

Πώς να ενεργοποιήσετε την ιχνηλάτηση

Βεβαιωθείτε ότι έχετε ρυθμίσει τις παραμέτρους της ιχνηλάτησης μόνο υπό την καθοδήγηση ενός ειδικού τεχνικής υποστήριξης της Kaspersky.

Για να ενεργοποιήσετε τα ίχνη εφαρμογών και τα ίχνη απόδοσης:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🗔 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Υποστήριξη.
- Κάντε κλικ στη σύνδεση Εργαλεία υποστήριξης για να ανοίξει το παράθυρο Εργαλεία υποστήριξης.
- 4. Ενεργοποιήστε και ρυθμίστε τις παραμέτρους των ιχνών εφαρμογών και των ιχνών απόδοσης σύμφωνα με τις οδηγίες ενός ειδικού τεχνικής υποστήριξης της Kaspersky.

Περιορισμοί και προειδοποιήσεις

Το Kaspersky Total Security έχει μια σειρά από περιορισμούς που δεν επηρεάζουν σε σημαντικό βαθμό τη λειτουργία της εφαρμογής.

Περιορισμοί στη λειτουργία συγκεκριμένων στοιχείων και την αυτόματη επεξεργασία αρχείων

Τα μολυσμένα αρχεία και οι κακόβουλες συνδέσεις υποβάλλονται σε επεξεργασία αυτόματα σύμφωνα με τους κανόνες που έχουν δημιουργήσει οι ειδικοί της Kaspersky. Δεν μπορείτε να τροποποιήσετε αυτούς τους κανόνες χειροκίνητα. Οι κανόνες μπορούν να ενημερωθούν κατόπιν ενημέρωσης των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής. Οι κανόνες για το Τείχος προστασίας, την Προστασία της Webcam, τη Διαχείριση εφαρμογών την Εκκαθάριση λογισμικού και τον Έλεγχο εφαρμογών ενημερώνονται επίσης αυτόματα.

Εάν μια σάρωση συσκευής εκκινηθεί από το My Kaspersky, τα αρχεία θα υποβληθούν αυτόματα σε επεξεργασία με βάση τους κανόνες που έχουν καθοριστεί στην εφαρμογή. Τα αρχεία που εντοπίζονται σε μια συσκευή μπορούν να υποβληθούν αυτόματα σε επεξεργασία κατόπιν αιτήματος από το My Kaspersky χωρίς την επιβεβαίωσή σας.

Περιορισμοί κατά τη σύνδεση με το Kaspersky Security Network

Κατά τη διάρκεια της λειτουργίας της, η εφαρμογή μπορεί να υποβάλλει ερωτήματα στο Kaspersky Security Network για πληροφορίες. Εάν δεν είναι δυνατή η ανάκτηση δεδομένων από το Kaspersky Security Network, η εφαρμογή λαμβάνει αποφάσεις με βάση τις τοπικές βάσεις δεδομένων προστασίας από ιούς.

Περιορισμοί της λειτουργίας Παρακολούθησης συστημάτων

Η προστασία από cryptor (κακόβουλο λογισμικό που κρυπτογραφεί τα αρχεία χρηστών) έχει τους ακόλουθους περιορισμούς:

- Για την υποστήριξη της λειτουργίας χρησιμοποιείται ο φάκελος συστήματος Temp. Αν η μονάδα δίσκου του συστήματος με τον φάκελο Temp δεν διαθέτει επαρκή χώρο στον σκληρό δίσκο για τη δημιουργία προσωρινών αρχείων, δεν παρέχεται προστασία από τα cryptor. Σε αυτήν την περίπτωση, η εφαρμογή δεν εμφανίζει ειδοποίηση σχετικά με την αδυναμία δημιουργίας αντιγράφων ασφαλείας των αρχείων (δεν παρέχεται προστασία).
- Τα προσωρινά αρχεία διαγράφονται αυτόματα όταν κλείνετε το Kaspersky Total Security ή απενεργοποιείτε το στοιχείο Παρακολούθηση συστημάτων.
- Σε περίπτωση έκτακτου τερματισμού του Kaspersky Total Security, τα προσωρινά αρχεία δεν διαγράφονται αυτόματα. Για να διαγράψετε τα προσωρινά αρχεία, διαγράψτε χειροκίνητα το περιεχόμενο του φακέλου Temp. Για να το κάνετε, ανοίξτε το παράθυρο Εκτέλεση και στο πεδίο Άνοιγμα πληκτρολογήστε %ΤΕΜΡ%. Κάντε κλικ στο ΟΚ.
- Προστασία από μονάδες κρυπτογράφησης παρέχεται μόνο για αρχεία που βρίσκονται τοποθετημένα σε μονάδες δίσκου δεδομένων, οι οποίες έχουν μορφοποιηθεί με το σύστημα αρχείων NTFS.
- Ο αριθμός των αρχείων που μπορούν να ανακτηθούν δεν μπορεί να υπερβαίνει τα 50 ανά μία διεργασία κρυπτογράφησης.
- Ο συνολικός όγκος τροποποιήσεων σε αρχεία δεν μπορεί να υπερβαίνει τα 100 MB.
 Αρχεία με τροποποιήσεις που υπερβαίνουν αυτό το όριο δεν μπορούν να ανακτηθούν.
- Τροποποιήσεις αρχείων που εκκινούνται μέσω διασύνδεσης δικτύου δεν παρακολουθούνται.
- Αρχεία που έχουν κρυπτογραφηθεί με EFS δεν υποστηρίζονται.
- Πρέπει να επανεκκινήσετε τον υπολογιστή σας για να ενεργοποιήσετε την προστασία από μονάδες κρυπτογράφησης μετά την εγκατάσταση του Kaspersky Total Security.

Περιορισμοί σάρωσης κρυπτογραφημένων συνδέσεων

Εξαιτίας των τεχνικών περιορισμών της υλοποίησης των αλγορίθμων σάρωσης, η σάρωση των κρυπτογραφημένων συνδέσεων δεν υποστηρίζει συγκεκριμένες επεκτάσεις του πρωτοκόλλου TLS 1.0 και μεταγενέστερες εκδόσεις (ειδικά τις NPN και ALPN). Οι συνδέσεις μέσω αυτών των πρωτοκόλλων μπορεί να είναι περιορισμένες. Τα προγράμματα περιήγησης με υποστήριξη SPDY, χρησιμοποιούν το πρωτόκολλο HTTP over TLS αντί του SPDY ακόμη και αν ο διακομιστής με τον οποίο γίνεται η σύνδεση υποστηρίζει το SPDY. Αυτό δεν επηρεάζει το επίπεδο ασφάλειας της σύνδεσης. Εάν ο διακομιστής υποστηρίζει μόνο το πρωτόκολλο SPDY και δεν είναι δυνατή η δημιουργία σύνδεσης μέσω του πρωτοκόλλου HTTPS, η εφαρμογή δεν θα παρακολουθεί τη σύνδεση που δημιουργείται.

Το Kaspersky Total Security δεν υποστηρίζει την επεξεργασία της κυκλοφορίας του διακομιστή μεσολάβησης HTTPS/2. Η εφαρμογή δεν υποστηρίζει την κυκλοφορία που λαμβάνει χώρα μέσω των επεκτάσεων του πρωτοκόλλου HTTP/2.

To Kaspersky Total Security αποτρέπει την ανταλλαγή δεδομένων μέσω του πρωτοκόλλου QUIC. Τα προγράμματα περιήγησης χρησιμοποιούν ένα τυπικό πρωτόκολλο μεταφοράς (TLS ή SSL) ανεξάρτητα από το αν είναι ενεργοποιημένη ή δεν είναι ενεργοποιημένη η υποστήριξη του πρωτοκόλλου QUIC στο πρόγραμμα περιήγησης.

To Kaspersky Total Security παρακολουθεί μόνο τις προστατευμένες συνδέσεις που έχει τη δυνατότητα να αποκρυπτογραφήσει. Η εφαρμογή δεν παρακολουθεί τις συνδέσεις που προστίθενται στη λίστα εξαιρέσεων (σύνδεσμος **Τοποθεσίες web** στο παράθυρο **Ρυθμίσεις** δικτύου).

Τα παρακάτω στοιχεία εκτελούν αποκρυπτογράφηση και σάρωση της κρυπτογραφημένης κίνησης από προεπιλογή:

- Προστασία από ιούς στο Web
- Ασφαλείς τραπεζικές συναλλαγές
- Σύμβουλος URL
- Γονικός έλεγχος

Το Kaspersky Total Security αποκρυπτογραφεί την κρυπτογραφημένη κίνηση καθώς ο χρήστης χρησιμοποιεί το πρόγραμμα περιήγησης Google Chrome, εάν η επέκταση Kaspersky Protection είναι απενεργοποιημένη σε αυτό το πρόγραμμα περιήγησης. To Kaspersky Total Security δεν παρακολουθεί την κυκλοφορία σχετικά με το αν το πρόγραμμα περιήγησης φορτώνει μια ιστοσελίδα ή τα στοιχεία της από μια τοπική κρυφή μνήμη (cache) αντί από το Διαδίκτυο.

Περιορισμοί στη σάρωση των κρυπτογραφημένων συνδέσεων του προγράμματος πελάτη The Bat

Δεδομένου ότι το πρόγραμμα πελάτης ηλεκτρονικού ταχυδρομείου The Bat χρησιμοποιεί το δικό του κατάστημα πιστοποιητικών, το Kaspersky Total Security αναγνωρίζει το πιστοποιητικό που χρησιμοποιήθηκε για τη δημιουργία σύνδεσης HTTPS μεταξύ αυτού του προγράμματος πελάτη και του διακομιστή ως μη αξιόπιστο. Για να αποτρέψετε αυτή την κατάσταση, ρυθμίστε τις παραμέτρους του προγράμματος πελάτη ηλεκτρονικού ταχυδρομείου The Bat, έτσι ώστε να συνεργάζεται με τον τοπικό χώρο αποθήκευσης πιστοποιητικών των Windows.

Περιορισμοί σχετικά με εξαιρέσεις σάρωσης κρυπτογραφημένων συνδέσεων

Όταν εκτελείται σάρωση κρυπτογραφημένων συνδέσεων με δικτυακούς τόπους που έχουν προστεθεί στις εξαιρέσεις, συγκεκριμένα στοιχεία, όπως το Πρόγραμμα Anti-Banner, ο Σύμβουλος URL και η Ιδιωτική περιήγηση ενδέχεται να συνεχίσουν να σαρώνουν τις κρυπτογραφημένες συνδέσεις. Τα στοιχεία Ασφαλείς τραπεζικές συναλλαγές, Γονικός Έλεγχος και Προστασία από ιούς στο Web δεν σαρώνουν δικτυακούς τόπους που έχουν προστεθεί στις εξαιρέσεις.

Περιορισμοί Δημιουργίας αντιγράφων ασφαλείας

Στη λειτουργία Δημιουργία αντιγράφων ασφαλείας ισχύουν οι παρακάτω περιορισμοί:

- Ο online χώρος αποθήκευσης των αντιγράφων ασφαλείας καθίσταται μη διαθέσιμος όταν αντικαθίσταται ο σκληρός δίσκος ή ο υπολογιστής. Επισκεφθείτε την τοποθεσία web τεχνικής υποστήριξης της Kaspersky για πληροφορίες σχετικά με την επαναφορά της σύνδεσης στον online χώρο αποθήκευσης μετά την αντικατάσταση του υλικού σας.
- Η επεξεργασία των αρχείων υπηρεσίας του χώρου αποθήκευσης αντιγράφων ασφαλείας μπορεί να οδηγήσει σε απώλεια της δυνατότητας πρόσβασης στον χώρο αποθήκευσης αντιγράφων ασφαλείας και αδυναμία επαναφοράς των δεδομένων σας.
- Εφόσον η εφαρμογή δημιουργεί αντίγραφα ασφαλείας μέσω της υπηρεσίας σκιώδους αντιγράφου του συστήματος, το offline αρχείο δεδομένων του Outlook (.ost) δεν

περιλαμβάνεται στο σύνολο αντιγράφων ασφαλείας, επειδή δεν έχει σχεδιαστεί για δημιουργία αντιγράφων ασφαλείας.

Περιορισμοί της λειτουργίας Κρυπτογράφησης δεδομένων

Όταν δημιουργείται ένας θάλαμος δεδομένων σε σύστημα αρχείων FAT32, το μέγεθος του αρχείου του θαλάμου δεδομένων στη μονάδα δίσκου δεν πρέπει να υπερβαίνει τα 4 GB.

Ειδικά ζητήματα σχετικά με τη σάρωση μνήμης kernel για rootkit στη λειτουργία Προστατευμένου προγράμματος περιήγησης

Όταν εντοπίζεται μια μη αξιόπιστη λειτουργική μονάδα στη λειτουργία Προστατευμένου προγράμματος περιήγησης, ανοίγει μια νέα καρτέλα του προγράμματος περιήγησης με μια ειδοποίηση σχετικά με τον εντοπισμό κακόβουλου λογισμικού. Εάν συμβεί αυτό, συνιστούμε να εξέλθετε από το πρόγραμμα περιήγησης και να εκτελέσετε Πλήρη σάρωση του υπολογιστή σας.

Ειδικά ζητήματα σχετικά με την προστασία των δεδομένων προχείρου

Το Kaspersky Total Security επιτρέπει σε μια εφαρμογή την πρόσβαση στο πρόχειρο στις εξής περιπτώσεις:

- Μια εφαρμογή στο ενεργό παράθυρο επιχειρεί να τοποθετήσει δεδομένα στο πρόχειρο.
 Ενεργό παράθυρο είναι αυτό που χρησιμοποιείτε εκείνη τη στιγμή.
- Μια αξιόπιστη διεργασία μιας εφαρμογής επιχειρεί να τοποθετήσει δεδομένα στο πρόχειρο.
- Μια αξιόπιστη διεργασία μιας εφαρμογής ή μια διεργασία στο ενεργό παράθυρο επιχειρεί να λάβει δεδομένα από το πρόχειρο.
- Μια διεργασία εφαρμογής που τοποθέτησε προηγουμένως δεδομένα στο πρόχειρο, επιχειρεί να λάβει αυτά τα δεδομένα από το πρόχειρο.

Λεπτομέρειες σχετικά με την επεξεργασία των μολυσμένων αρχείων από τα στοιχεία της εφαρμογής

Από προεπιλογή, η εφαρμογή μπορεί να διαγράψει τα μολυσμένα αρχεία που δεν μπορούν να απολυμανθούν. Η αφαίρεση από προεπιλογή μπορεί να εκτελεστεί κατά την επεξεργασία των αρχείων από στοιχεία όπως τα Έλεγχος εφαρμογών, Προστασία email από ιούς, Προστασία αρχείων από ιούς, κατά τη διάρκεια εργασιών σάρωσης ή όταν η Παρακολούθηση συστημάτων εντοπίσει κακόβουλη δραστηριότητα ή εφαρμογή.

Περιορισμοί που ισχύουν σε συγκεκριμένα στοιχεία σε περίπτωση εγκατάστασης της εφαρμογής μαζί με το Kaspersky Fraud Prevention for Endpoints

Η λειτουργία των παρακάτω στοιχείων του Kaspersky Total Security είναι περιορισμένη στο Προστατευμένο πρόγραμμα περιήγησης όταν η εφαρμογή έχει εγκατασταθεί μαζί με το Kaspersky Fraud Prevention for Endpoints:

- Προστασία από ιούς στο web, εκτός του προγράμματος κατά του phishing
- Γονικός έλεγχος
- Σύμβουλος URL
- Πρόγραμμα Anti-Banner

Λεπτομέρειες λειτουργίας της διεργασίας αυτόματης εκτέλεσης

Η διεργασία αυτόματης εκτέλεσης καταγράφει τα αποτελέσματα της λειτουργίας της. Τα δεδομένα καταγράφονται σε αρχεία κειμένου με την ονομασία "kl-autorun-<ημερομηνία> <ώρα>.log". Για να δείτε τα δεδομένα, ανοίξτε το παράθυρο **Εκτέλεση** και, στο πεδίο **Άνοιγμα**, πληκτρολογήστε %ΤΕΜΡ% και κάντε κλικ στο **ΟΚ**.

Όλα τα αρχεία ιχνών αποθηκεύονται στη διαδρομή των αρχείων εγκατάστασης που ελήφθησαν κατά τη διάρκεια της λειτουργίας της διεργασίας αυτόματης εκτέλεσης. Τα δεδομένα αποθηκεύονται για όσο διαρκεί η λειτουργία της διεργασίας αυτόματης εκτέλεσης και διαγράφονται οριστικά όταν η εργασία αυτή τερματίζεται. Τα δεδομένα δεν αποστέλλονται πουθενά.

Περιορισμοί του Kaspersky Total Security στα Microsoft Windows 10 RS4 με τη λειτουργία Device Guard ενεργοποιημένη:

Η χρήση των παρακάτω δυνατοτήτων είναι μερικώς περιορισμένη:

- Προστασία προχείρου
- Προστασία προγράμματος περιήγησης από προσομοιωτές εισόδου πληκτρολογίου και ποντικιού (πλαστογράφηση εισόδου)
- Προστασία από εφαρμογές απομακρυσμένης διαχείρισης
- Προστασία προγράμματος περιήγησης (διαχείριση μέσω API, προστασία από επιθέσεις που χρησιμοποιούν επικίνδυνα μηνύματα σε παράθυρα του προγράμματος περιήγησης, προστασία από διαχείριση ουράς μηνυμάτων)
- Ευρετική ανάλυση (προσομοίωση εκκίνησης κακόβουλων εφαρμογών)

Αν η λειτουργία UMCI είναι ενεργοποιημένη στα Windows, το Kaspersky Total Security δεν εντοπίζει κακόβουλα προγράμματα κλειδώματος οθόνης.

Πληροφορίες για την καταγραφή συμβάντων στο αρχείο καταγραφής συμβάντων των Windows τα οποία σχετίζονται με την Άδεια Χρήσης Τελικού Χρήστη και το Kaspersky Security Network

Συμβάντα που αφορούν την αποδοχή και άρνηση των όρων της Άδειας Χρήσης Τελικού Χρήστη, καθώς επίσης και την αποδοχή και άρνηση συμμετοχής στο Kaspersky Security Network, καταγράφονται στο αρχείο καταγραφής των Windows.

Περιορισμοί σε ελέγχους αξιοπιστίας τοπικών διευθύνσεων στο Kaspersky Security Network

Στο Kaspersky Security Network οι συνδέσεις σε τοπικούς πόρους δεν σαρώνονται.

Προειδοποίηση για εφαρμογές που συλλέγουν πληροφορίες

Εάν εγκατασταθεί στον υπολογιστή σας μια εφαρμογή που συλλέγει πληροφορίες και τις αποστέλλει αλλού προς επεξεργασία, το Kaspersky Total Security ενδέχεται να ταξινομήσει αυτήν την εφαρμογή ως κακόβουλο λογισμικό. Για να αποφύγετε κάτι τέτοιο, μπορείτε να εξαιρέσετε την εφαρμογή από τη σάρωση με το να ρυθμίσετε τις παραμέτρους του Kaspersky Total Security όπως περιγράφεται στο παρόν έγγραφο.

Προειδοποίηση σχετικά με τη δημιουργία μιας αναφοράς εγκατάστασης της εφαρμογής

Όταν γίνεται εγκατάσταση της εφαρμογής σε έναν υπολογιστή, δημιουργείται ένα αρχείο αναφοράς εγκατάστασης. Εάν η εγκατάσταση της εφαρμογής ολοκληρωθεί με σφάλμα, ένα αρχείο αναφοράς εγκατάστασης αποθηκεύεται και αποστέλλεται στην Τεχνική Υποστήριξη της Kaspersky. Μπορείτε να δείτε τα περιεχόμενα του αρχείου αναφοράς εγκατάστασης κάνοντας κλικ στη σύνδεση στο παράθυρο της εφαρμογής. Εάν η εγκατάσταση της εφαρμογής ολοκληρωθεί με επιτυχία, το αρχείο αναφοράς εγκατάστασης εφαρμογής διαγράφεται αμέσως από τον υπολογιστή σας.

Περιορισμοί στον έλεγχο της Webcam στο λειτουργικό σύστημα της επετειακής ενημέρωσης των Microsoft Windows 10 (RedStone 1)

Μετά από εγκατάσταση της εφαρμογής στο λειτουργικό σύστημα της επετειακής ενημέρωσης των Microsoft Windows 10 (RedStone 1), ο έλεγχος της πρόσβασης στην Webcam δεν εγγυάται μέχρι να γίνει επανεκκίνηση του υπολογιστή.

Περιορισμοί στη δημιουργία αντιγράφων ασφαλείας στο διαδίκτυο και στην επαναφορά δεδομένων από αντίγραφα ασφαλείας

Δεν είναι δυνατή η ταυτόχρονη εκτέλεση μιας εργασίας δημιουργίας αντιγράφου ασφαλείας του Kaspersky Total Security και μιας εργασίας ανάκτησης δεδομένων του Kaspersky Restore Utility στον ίδιο υπολογιστή.

Περιορισμοί του Τείχους προστασίας

Το Τείχος προστασίας δεν ελέγχει τις τοπικές συνδέσεις που εγκαθίστανται από ελεγχόμενες εφαρμογές.

Περιορισμοί Ελέγχου εφαρμογών

Εάν το VeraCrypt είναι εγκατεστημένο στον υπολογιστή σας, το Kaspersky Total Security ενδέχεται να τερματιστεί κατά την εργασία με το στοιχείο Έλεγχος εφαρμογών. Για να επιλύσετε αυτό το ζήτημα, αναβαθμίστε το VeraCrypt στην έκδοση 1.19 ή σε νεότερη έκδοση.

Περιορισμοί όταν η εφαρμογή εκκινείται για πρώτη φορά μετά από αναβάθμιση από Microsoft Windows 7 σε Microsoft Windows 10 Εάν πραγματοποιήσατε αναβάθμιση από τα Microsoft Windows 7 στα Microsoft Windows 8 / 8.1 ή Microsoft Windows 10 / RS1 / RS2, το Kaspersky Total Security λειτουργεί με τους ακόλουθους περιορισμούς όταν εκκινείται για πρώτη φορά:

- Μόνο η Προστασία αρχείων από ιούς (προστασία πραγματικού χρόνου) εκτελείται. Άλλα στοιχεία της εφαρμογής δεν εκτελούνται.
- Η Αυτοάμυνα αρχείων και το μητρώο συστήματος εκτελείται. Η Αυτοάμυνα διεργασιών δεν εκτελείται.
- Το περιβάλλον εργασίας της εφαρμογής δεν είναι διαθέσιμο μέχρι να επανεκκινήσετε τον υπολογιστή. Η εφαρμογή εμφανίζει μια ειδοποίηση που δηλώνει ότι μερικά στοιχεία της εφαρμογής δεν εκτελούνται και ότι ο υπολογιστής πρέπει να επανεκκινηθεί μετά από την ολοκλήρωση της προσαρμογής στο καινούριο λειτουργικό σύστημα.
- Μόνο η επιλογή Έξοδος είναι διαθέσιμη στο μενού περιβάλλοντος του εικονιδίου της εφαρμογής στην περιοχή ειδοποιήσεων.
- Η εφαρμογή δεν εμφανίζει ειδοποιήσεις και επιλέγει αυτόματα την συνιστώμενη ενέργεια.

Προειδοποίηση σχετικά με σφάλμα στην προσαρμογή των προγραμμάτων οδήγησης εφαρμογής κατά την αναβάθμιση του λειτουργικού συστήματος από Windows 7 σε Windows 10

Η αναβάθμιση από Windows 7 σε Windows 10 μπορεί να οδηγήσει σε σφάλμα κατά την προσαρμογή των προγραμμάτων οδήγησης του Kaspersky Total Security. Τα προγράμματα οδήγησης προσαρμόζονται στο παρασκήνιο, το οποίο σημαίνει ότι δεν λαμβάνετε ειδοποιήσεις για την πρόοδο της διαδικασίας.

Εάν υπάρξει σφάλμα στην προσαρμογή των προγραμμάτων οδήγησης, δεν θα μπορείτε να χρησιμοποιείτε τις ακόλουθες δυνατότητες της εφαρμογής:

- Τείχος προστασίας
- Εντοπισμός απειλών την ώρα που φορτώνει το λειτουργικό σύστημα
- Προστασία των διαδικασιών εφαρμογής χρησιμοποιώντας την τεχνολογία Protected Process Light (PPL) της Microsoft Corporation

Μπορείτε να χρησιμοποιήσετε τις ακόλουθες μεθόδους για να διορθώσετε το σφάλμα:

- Επανεκκινήστε τον υπολογιστή και επίσης την προσαρμογή της εφαρμογής από την ειδοποίηση στο Κέντρο ειδοποιήσεων.
- Απεγκαταστήστε την εφαρμογή και εγκαταστήστε την ξανά.

Περιορισμοί κατά τη σάρωση κυκλοφορίας που στέλνεται μέσω HTTPS στο πρόγραμμα περιήγησης Mozilla Firefox

Στο Mozilla Firefox 58.x και σε μεταγενέστερες εκδόσεις, η εφαρμογή δεν σαρώνει κυκλοφορία που μεταδίδεται μέσω του πρωτοκόλλου HTTPS, εάν η τροποποίηση των ρυθμίσεων του προγράμματος περιήγησης προστατεύεται από τον Κύριο κωδικό πρόσβασης. Όταν εντοπιστεί Κύριος κωδικός πρόσβασης στο πρόγραμμα περιήγησης, η εφαρμογή εμφανίζει μια ειδοποίηση, η οποία περιέχει σύνδεση για ένα άρθρο στη Γνωσιακή βάση. Το άρθρο περιέχει οδηγίες για την επίλυση αυτού του προβλήματος.

Εάν η κυκλοφορία HTTPS δεν παρακολουθείτε, η λειτουργία των ακόλουθων στοιχείων είναι περιορισμένη:

- Προστασία από ιούς στο Web
- Κατά του phishing
- Γονικός έλεγχος
- Ιδιωτική προστασία
- Πρόγραμμα Anti-Banner
- Ασφαλής καταχώρηση δεδομένων
- Ασφαλείς τραπεζικές συναλλαγές

Περιορισμοί της επέκτασης Kaspersky Protection στο Google Chrome και το Mozilla Firefox

Η επέκταση Kaspersky Protection δεν λειτουργεί στο Google Chrome και το Mozilla Firefox, αν είναι εγκατεστημένο το Malwarebytes για Windows στον υπολογιστή σας.

Ειδικές συνθήκες κατά την εγκατάσταση της εφαρμογής σε Microsoft Windows 7 Service Pack 0 και Service Pack 1 Όταν εγκαθιστάτε την εφαρμογή σε ένα λειτουργικό σύστημα που δεν υποστηρίζει πιστοποιητικά με ψηφιακή υπογραφή SHA256, η εφαρμογή εγκαθιστά το δικό της αξιόπιστο πιστοποιητικό.

Άλλες πηγές ενημέρωσης σχετικά με την εφαρμογή

Σελίδα Kaspersky Total Security στη Γνωσιακή βάση

Η Γνωσιακή βάση είναι μια ενότητα του δικτυακού τόπου Τεχνικής υποστήριξης.

Στη <u>σελίδα του Kaspersky Total Security στη Γνωσιακή βάση</u> ^Δ, μπορείτε να διαβάσετε άρθρα με χρήσιμες πληροφορίες, συστάσεις και απαντήσεις σε συχνές ερωτήσεις σχετικά με τον τρόπο αγοράς, εγκατάστασης και χρήσης της εφαρμογής.

Τα άρθρα στη Γνωσιακή βάση ενδέχεται να παρέχουν απαντήσεις σε ερωτήσεις που σχετίζονται με το Kaspersky Total Security, αλλά και με άλλες εφαρμογές της Kaspersky. Τα άρθρα στη Γνωσιακή βάση μπορεί επίσης να περιέχουν νέα από την Τεχνική υποστήριξη.

Συζητήσεις για τις εφαρμογές της Kaspersky στην Κοινότητά μας

Εάν η ερώτησή σας δεν απαιτεί άμεση απάντηση, μπορείτε να τη συζητήσετε με τους ειδικούς της Kaspersky και άλλους χρήστες στην <u>Κοινότητά μας</u> .

Στην Κοινότητα μπορείτε να δείτε υπάρχοντα θέματα, να υποβάλετε τα σχόλιά σας και να δημιουργήσετε νέα θέματα συζήτησης.

Γλωσσάριο

Hypervisor

Εφαρμογή που υποστηρίζει την παράλληλη λειτουργία πολλών λειτουργικών συστημάτων σε έναν υπολογιστή.

Kaspersky Security Network (KSN)

Η γνωσιακή βάση της Kaspersky που βασίζεται σε cloud με πληροφορίες σχετικά με την αξιοπιστία των εφαρμογών και των δικτυακών τόπων. Η χρήση δεδομένων από το Kaspersky Security Network διασφαλίζει την ταχύτερη απόκριση των εφαρμογών της Kaspersky όταν εμφανίζονται απειλές, βελτιώνει την απόδοση ορισμένων στοιχείων προστασίας και μειώνει την πιθανότητα εμφάνισης ψευδών θετικών αποτελεσμάτων.

Phishing

Ένα είδος διαδικτυακής απάτης που έχει ως στόχο την απόκτηση μη εξουσιοδοτημένης πρόσβασης στα εμπιστευτικά δεδομένα των χρηστών.

Rootkit

Πρόγραμμα ή σύνολο προγραμμάτων με στόχο την απόκρυψη των ιχνών ενός εισβολέα ή κακόβουλου λογισμικού στο λειτουργικό σύστημα.

Στα συστήματα που βασίζονται σε Windows, ο όρος "rootkit" αναφέρεται συνήθως σε ένα πρόγραμμα που διεισδύει στο λειτουργικό σύστημα και υποκλέπτει λειτουργίες του συστήματος (API Windows). Η αναχαίτιση και τροποποίηση των λειτουργιών API χαμηλού επιπέδου είναι οι βασικές μέθοδοι που επιτρέπουν σε αυτά τα προγράμματα να καμουφλάρουν αρκετά αποτελεσματικά την παρουσία τους στο λειτουργικό σύστημα. Ένα rootkit είναι συνήθως σε θέση να καμουφλάρει την παρουσία διεργασιών, φακέλων και αρχείων που έχουν αποθηκευτεί σε μια μονάδα δίσκου, καθώς και κλειδιών μητρώου, εφόσον περιγράφονται στη ρύθμιση παραμέτρων του rootkit. Πολλά rootkit εγκαθιστούν δικά τους προγράμματα οδήγησης και υπηρεσίες στο λειτουργικό σύστημα (είναι επίσης "αόρατα").

Spam (ανεπιθύμητη αλληλογραφία)

Αυτόκλητες μαζικές αποστολές μηνυμάτων ηλ. αλληλογραφίας που περιλαμβάνουν συνήθως διαφημίσεις.

Άγνωστος ιός

Ένας νέος ιός για τον οποίο δεν υπάρχουν πληροφορίες στις βάσεις δεδομένων. Σε γενικές γραμμές, οι άγνωστοι ιοί εντοπίζονται από την εφαρμογή σε αντικείμενα όταν γίνεται χρήση της ευρετικής ανάλυσης. Αυτά τα αντικείμενα κατατάσσονται ως πιθανώς μολυσμένα.

Αντικείμενα εκκίνησης

Το σύνολο προγραμμάτων που απαιτούνται για την εκκίνηση και σωστή λειτουργία του λειτουργικού συστήματος και των προγραμμάτων λογισμικού που είναι εγκατεστημένα στον υπολογιστή σας. Αυτά τα αντικείμενα εκτελούνται κάθε φορά που εκκινείται το λειτουργικό σύστημα. Υπάρχουν ιοί ικανοί να μολύνουν ειδικά αντικείμενα αυτόματης εκτέλεσης, γεγονός που μπορεί να οδηγήσει, για παράδειγμα, στο να αποκλειστεί η έναρξη του λειτουργικού συστήματος.

Αξιόπιστη διεργασία

Μια διεργασία λογισμικού, της οποίας οι λειτουργίες αρχείου δεν περιορίζονται από την εφαρμογή της Kaspersky στη λειτουργία προστασίας πραγματικού χρόνου. Αν εντοπιστεί ύποπτη δραστηριότητα σε αξιόπιστη διεργασία, το Kaspersky Total Security καταργεί τη διεργασία από τη λίστα με τις αξιόπιστες διεργασίες και δεν της επιτρέπει να εκτελεί ενέργειες.

Αποκλεισμός αντικειμένου

Άρνηση της πρόσβασης σε ένα αντικείμενο από εξωτερικές εφαρμογές. Ένα αποκλεισμένο αντικείμενο δεν είναι δυνατόν να αναγνωσθεί, εκτελεστεί, τροποποιηθεί ή διαγραφεί.

Βάσεις δεδομένων προστασίας από ιούς

Βάσεις δεδομένων που περιέχουν πληροφορίες σχετικά με τις απειλές για την ασφάλεια του υπολογιστή που είναι γνωστές στην Kaspersky τη χρονική στιγμή της κυκλοφορίας των βάσεων δεδομένων προστασίας από ιούς. Οι καταχωρήσεις που περιέχονται στις βάσεις δεδομένων προστασίας από ιούς επιτρέπουν τον εντοπισμό κακόβουλου κώδικα στα αντικείμενα που ελέγχονται. Οι βάσεις δεδομένων προστασίας από ιούς δημιουργούνται από τους ειδικούς της Kaspersky και ενημερώνονται κάθε μία ώρα.

Βάση δεδομένων κακόβουλων διευθύνσεων ιστού

Μια λίστα διευθύνσεων ιστού το περιεχόμενο των οποίων μπορεί να θεωρηθεί επικίνδυνο. Η λίστα αυτή δημιουργείται από τους ειδικούς της Kaspersky, ενημερώνεται τακτικά και αποτελεί μέρος του πακέτου εφαρμογών της Kaspersky.

Βάση δεδομένων των διευθύνσεων ιστού phishing

Λίστα διευθύνσεων ιστού που ορίζονται ως διευθύνσεις phishing web από τους ειδικούς της Kaspersky. Η βάση δεδομένων ενημερώνεται τακτικά και αποτελεί μέρος του πακέτου εφαρμογών της Kaspersky.

Δέσμη ενεργειών

Μικρό πρόγραμμα υπολογιστή ή ανεξάρτητο τμήμα προγράμματος (λειτουργία) το οποίο έχει αναπτυχθεί, κατά κανόνα, για εκτέλεση μιας συγκεκριμένης εργασίας. Η πιο συχνή του χρήση είναι με προγράμματα που είναι ενσωματωμένα σε υπερκείμενο. Για παράδειγμα, εκτελούνται δέσμες ενεργειών όταν ανοίγετε συγκεκριμένους δικτυακούς τόπους.

Εάν έχει ενεργοποιηθεί η προστασία πραγματικού χρόνου, η εφαρμογή παρακολουθεί την εκτέλεση δεσμών ενεργειών, τις αναχαιτίζει και τις σαρώνει για ιούς. Ανάλογα με τα αποτελέσματα της σάρωσης, μπορείτε να αποκλείσετε ή να επιτρέψετε την εκτέλεση μιας δέσμης ενεργειών.

Δημιουργία αντιγράφων ασφαλείας

Δημιουργεί αντίγραφα ασφαλείας των δεδομένων που είναι αποθηκευμένα στον υπολογιστή. Τα αντίγραφα ασφαλείας δημιουργούνται για την αποφυγή της απώλειας δεδομένων σε περίπτωση κλοπής, σφαλμάτων υλικού ή επιθέσεων από χάκερ.

Διακομιστές ενημέρωσης της Kaspersky

Διακομιστές HTTP της Kaspersky από τους οποίους λαμβάνονται οι ενημερώσεις των βάσεων δεδομένων και των μονάδων λογισμικού.

Διάρκεια ισχύος της άδειας χρήσης

Μια χρονική περίοδος κατά την οποία έχετε πρόσβαση στις λειτουργίες της εφαρμογής και δικαίωμα χρήσης πρόσθετων υπηρεσιών.

Ενεργοποίηση της εφαρμογής

Η μετάβαση της εφαρμογής σε κατάσταση πλήρους λειτουργίας. Η ενεργοποίηση της εφαρμογής γίνεται από τον χρήστη κατά τη διάρκεια της εγκατάστασής της ή μετά από αυτήν. Για να ενεργοποιήσει την εφαρμογή, ο χρήστης πρέπει να έχει έναν κωδικό ενεργοποίησης.

Ενημέρωση

Η διαδικασία αντικατάστασης/προσθήκης νέων αρχείων (βάσεις δεδομένων ή μονάδες εφαρμογές) που ανακτώνται από τους διακομιστές ενημέρωσης της Kaspersky.

Επίπεδο απειλών

Δείκτης που εκφράζει την πιθανότητα μια εφαρμογή να αποτελεί απειλή για το λειτουργικό σύστημα. Το επίπεδο απειλών υπολογίζεται χρησιμοποιώντας την ευρετική ανάλυση, βάσει δύο τύπων κριτηρίων:

- Στατικά (όπως πληροφορίες για το εκτελέσιμο αρχείο μιας εφαρμογής: μέγεθος, ημερομηνία δημιουργίας, κλπ.)
- Δυναμικά, τα οποία χρησιμοποιούνται ενώ προσομοιώνεται η λειτουργία της εφαρμογής σε εικονικό περιβάλλον (ανάλυση των κλήσεων της εφαρμογής προς τις λειτουργίες του συστήματος)

Το επίπεδο απειλών επιτρέπει τον εντοπισμό συμπεριφορών που είναι χαρακτηριστικές του κακόβουλου λογισμικού. Όσο χαμηλότερο είναι το επίπεδο απειλών, τόσο περισσότερες ενέργειες θα επιτρέπεται να εκτελεί η εφαρμογή στο λειτουργικό σύστημα.
Επίπεδο ασφαλείας

Το επίπεδο ασφάλειας ορίζεται ως μια προκαθορισμένη συλλογή ρυθμίσεων για ένα στοιχείο της εφαρμογής.

Εργασία

Οι λειτουργίες της εφαρμογής Kaspersky εφαρμόζονται με τη μορφή εργασιών, όπως: εργασία Πλήρους σάρωσης ή εργασία Ενημέρωσης.

Θάλαμος δεδομένων

Θάλαμος δεδομένων είναι ένας ειδικός χώρος αποθήκευσης δεδομένων, στον οποίο τα αρχεία αποθηκεύονται σε κρυπτογραφημένη μορφή. Η πρόσβαση σε αυτά τα αρχεία γίνεται μόνο με κωδικό πρόσβασης. Οι θάλαμοι δεδομένων έχουν ως σκοπό την αποτροπή της μη εξουσιοδοτημένης πρόσβασης στα δεδομένα του χρήστη.

Ιός

Πρόγραμμα που μολύνει άλλα προγράμματα προσθέτοντας τον κώδικά του σε αυτά, με σκοπό να ελέγξει το πότε θα εκτελεστούν τα μολυσμένα αρχεία. Αυτός ο απλός ορισμός κάνει σαφή την κύρια ενέργεια που εκτελεί κάθε ιός, δηλαδή τη μόλυνση.

Ίχνη

Εκτέλεση της εφαρμογής στη λειτουργία εντοπισμού σφαλμάτων. Μετά από την εκτέλεση κάθε εντολής, η εφαρμογή διακόπτεται και προβάλλεται το αποτέλεσμα αυτού του βήματος.

Καραντίνα

Ένας χώρος αποθήκευσης ειδικά σχεδιασμένος για την αποθήκευση αντιγράφων ασφαλείας των αρχείων που διαγράφονται ή τροποποιούνται κατά τη διεργασία απολύμανσης. Τα αντίγραφα των αρχείων αποθηκεύονται σε μια ειδική μορφή, η οποία δεν αποτελεί απειλή για τον υπολογιστή.

Καταγραφέας πληκτρολόγησης (keylogger)

Πρόγραμμα σχεδιασμένο για εν κρυπτώ καταγραφή πληροφοριών σχετικά με τα πλήκτρα που πατάει ο χρήστης. Οι καταγραφείς πληκτρολόγησης (keylogger)λειτουργούν ως υποκλοπείς των δεδομένων που εισάγονται μέσω του πληκτρολογίου.

Κωδικός ενεργοποίησης

Ένας κωδικός που λαμβάνετε μετά από την αγορά της εμπορικής άδειας χρήσης για το Kaspersky Total Security. Αυτός ο κωδικός απαιτείται για την ενεργοποίηση της εφαρμογής.

Ο κωδικός ενεργοποίησης είναι μια μοναδική ακολουθία είκοσι αλφαριθμητικών χαρακτήρων, με τη μορφή xxxxx-xxxxx-xxxxx.

Μάσκα αρχείου

Αναπαράσταση ονόματος αρχείου χρησιμοποιώντας χαρακτήρες μπαλαντέρ. Οι τυπικοί χαρακτήρες μπαλαντέρ που χρησιμοποιούνται σε μάσκες αρχείων είναι * και ?, όπου το σύμβολο * αναπαριστά οποιονδήποτε αριθμό χαρακτήρων, ενώ το σύμβολο ? υποκαθιστά οποιονδήποτε μεμονωμένο χαρακτήρα.

Μη συμβατή εφαρμογή

Μια εφαρμογή προστασίας από ιούς προερχόμενη από τρίτο δημιουργό ή μια εφαρμογή της Kaspersky που δεν υποστηρίζει διαχείριση μέσω του Kaspersky Total Security.

Μολυσμένο αντικείμενο

Αντικείμενο με κώδικα τμήμα του οποίου αντιστοιχεί επακριβώς με τον κώδικα γνωστού κακόβουλου λογισμικού. Η Kaspersky δεν συνιστά τη χρήση τέτοιων αντικειμένων.

Μονάδες της εφαρμογής

Αρχεία που περιλαμβάνονται στο πακέτο εγκατάστασης της Kaspersky και που είναι υπεύθυνα για την εκτέλεση των κύριων εργασιών της αντίστοιχης εφαρμογής. Μία συγκεκριμένη μονάδα εφαρμογής αντιστοιχεί σε κάθε τύπο εργασίας που εκτελείται από την εφαρμογή (μονάδες προστασίας, σάρωσης, ενημερώσεων βάσεων δεδομένων και λειτουργικών μονάδων της εφαρμογής).

Ομάδα αξιοπιστίας

Μια ομάδα στην οποία το Kaspersky Total Security κατατάσσει μια εφαρμογή ή διαδικασία, ανάλογα με τα ακόλουθα κριτήρια: την παρουσία μιας ψηφιακής υπογραφής, αξιοπιστία στο Kaspersky Security Network, επίπεδο αξιοπιστίας στην πηγής της εφαρμογής, και πιθανός κίνδυνος από ενέργειες που εκτελούνται από την εφαρμογή ή τη διαδικασία. Με βάση την ομάδα αξιοπιστίας στην οποία ανήκει η εφαρμογή, το Kaspersky Total Security μπορεί να περιορίσει τις ενέργειες που μπορεί να εκτελέσει η εφαρμογή στο λειτουργικό σύστημα.

Στο Kaspersky Total Security, οι εφαρμογές ανήκουν σε μία από τις ακόλουθες ομάδες αξιοπιστίας: Αξιόπιστη, χαμηλού περιορισμού, Υψηλού περιορισμού, ή Μη αξιόπιστη.

Πακέτο ενημέρωσης

Ένα πακέτο αρχείων σχεδιασμένο για την ενημέρωση των βάσεων δεδομένων και των μονάδων της εφαρμογής. Η εφαρμογή της Kaspersky αντιγράφει τα πακέτα ενημέρωσης από τους διακομιστές ενημέρωσης της Kaspersky και εγκαθιστά και εφαρμόζει αυτόματα αυτά τα πακέτα.

Πιθανό μήνυμα spam

Μήνυμα που δεν μπορεί να θεωρηθεί αναμφισβήτητα spam, αλλά διαθέτει αρκετά χαρακτηριστικά spam (π.χ. συγκεκριμένοι τύποι αποστολών ηλεκτρονικής αλληλογραφίας και διαφημιστικών μηνυμάτων).

Πιθανώς μολυσμένο αντικείμενο

Ένα αντικείμενο που περιέχει στον κώδικά του μέρη τροποποιημένου κώδικα από μια γνωστή απειλή ή ένα αντικείμενο που συμπεριφέρεται με παρόμοιο τρόπο με μία απειλή.

Πρόγραμμα εκμετάλλευσης

Κώδικας λογισμικού που χρησιμοποιεί ένα τρωτό σημείο στο σύστημα ή στο λογισμικό. Οι εκμεταλλεύσεις χρησιμοποιούνται συχνά για την εγκατάσταση κακόβουλου λογισμικού στον υπολογιστή, χωρίς να το γνωρίζει ο χρήστης.

Πρόγραμμα ευρετικής ανάλυσης

Τεχνολογία για τον εντοπισμό απειλών, για τις οποίες δεν έχουν προστεθεί ακόμα πληροφορίες στις βάσεις δεδομένων της Kaspersky. Η λειτουργία ευρετικής ανάλυσης εντοπίζει αντικείμενα που η συμπεριφορά τους στο λειτουργικό σύστημα μπορεί να αποτελέσει απειλή ασφαλείας. Τα αντικείμενα που εντοπίζονται από το πρόγραμμα ευρετικής ανάλυσης θεωρούνται πιθανώς μολυσμένα. Για παράδειγμα, ένα αντικείμενο μπορεί να θεωρηθεί πιθανώς μολυσμένο αν περιέχει ακολουθίες εντολών που είναι χαρακτηριστικές σε κακόβουλα αντικείμενα (άνοιγμα αρχείου, εγγραφή σε αρχείο).

Προστατευμένο πρόγραμμα περιήγησης

Μια ειδική κατάσταση λειτουργίας ενός τυπικού προγράμματος περιήγησης, η οποία είναι σχεδιασμένη για οικονομικές συναλλαγές και διαδικτυακές αγορές. Η χρήση του Προστατευμένου προγράμματος περιήγησης διασφαλίζει την προστασία των εμπιστευτικών δεδομένων που εισάγετε στους δικτυακούς τόπους τραπεζών και συστημάτων πληρωμής, όπως αριθμοί πιστωτικών καρτών ή κωδικοί πρόσβασης που χρησιμοποιούνται για τραπεζικές συναλλαγές στο Διαδίκτυο, και επίσης αποτρέπει την κλοπή δεδομένων πληρωμής όταν πραγματοποιείτε ηλεκτρονικές πληρωμές.

Πρωτόκολλο

Σαφώς ορισμένο και τυποποιημένο σύνολο κανόνων που διέπουν την αλληλεπίδραση μεταξύ προγράμματος-πελάτη και διακομιστή. Στα γνωστά πρωτόκολλα και στις υπηρεσίες που συσχετίζονται με αυτά περιλαμβάνονται τα HTTP, FTP και NNTP.

Ρυθμίσεις εργασιών

Ρυθμίσεις εφαρμογής ειδικές για κάθε τύπο εργασίας.

Σάρωση κυκλοφορίας δικτύου

Σάρωση σε πραγματικό χρόνο που χρησιμοποιεί πληροφορίες από την τρέχουσα (τελευταία) έκδοση των βάσεων δεδομένων για αντικείμενα που μεταφέρονται μέσω όλων των πρωτοκόλλων (για παράδειγμα, HTTP, FTP και άλλα πρωτόκολλα).

Στοιχεία προστασίας

Δομικά ενσωματωμένα τμήματα του Kaspersky Total Security που προορίζονται για την προστασία από συγκεκριμένους τύπους απειλών (π.χ. Πρόγραμμα Anti-Spam και Κατά του phishing). Κάθε ένα από τα στοιχεία είναι σχετικά ανεξάρτητο από τα άλλα και μπορεί να απενεργοποιηθεί ή να διαμορφωθεί μεμονωμένα.

Συμπιεσμένο αρχείο

Ένα συμπιεσμένο εκτελέσιμο αρχείο που περιέχει ένα πρόγραμμα αποσυμπίεσης και οδηγίες εκτέλεσης για το λειτουργικό σύστημα.

Τεχνολογία iChecker

Μια τεχνολογία που αυξάνει την ταχύτητα της σάρωσης προστασίας από ιούς εξαιρώντας αντικείμενα που παρέμειναν αμετάβλητα από την τελευταία σάρωση, υπό την προϋπόθεση ότι οι παράμετροι σάρωσης (η βάση δεδομένων και οι ρυθμίσεις) δεν έχουν αλλάξει. Οι πληροφορίες για κάθε αρχείο αποθηκεύονται σε μια ειδική βάση δεδομένων. Αυτή η τεχνολογία χρησιμοποιείται τόσο στην προστασία σε πραγματικό χρόνο όσο και στις λειτουργίες σάρωσης κατόπιν απαίτησης.

Για παράδειγμα, έστω ότι έχετε ένα αρχείο αρχειοθέτησης που σαρώθηκε από μια εφαρμογή της Kaspersky και στο αρχείο έχει εκχωρηθεί η κατάσταση *μη μολυσμένο*. Την επόμενη φορά, η εφαρμογή θα παραλείψει αυτό το αρχείο αρχειοθέτησης, εκτός αν το αρχείο έχει τροποποιηθεί ή έχουν αλλάξει οι ρυθμίσεις σάρωσης. Εάν έχετε αλλάξει το περιεχόμενο του αρχείου αρχειοθέτησης (π.χ. προσθέτοντας ένα νέο αρχείο μέσα σε αυτό), έχετε τροποποιήσει τις ρυθμίσεις σάρωσης ή έχετε ενημερώσει τις βάσεις δεδομένων εφαρμογών, το αρχείο αρχειοθέτησης θα υποβληθεί εκ νέου σε σάρωση.

Περιορισμοί της τεχνολογίας iChecker:

- Αυτή η τεχνολογία δεν λειτουργεί με αρχεία μεγάλου μεγέθους, καθώς είναι ταχύτερο να σαρώνεται ένα αρχείο από το να ελέγχεται εάν τροποποιήθηκε από την τελευταία σάρωση.
- Η τεχνολογία υποστηρίζει έναν περιορισμένο αριθμό μορφών.

Τομέας εκκίνησης δίσκων

Ο τομέας εκκίνησης είναι μια ιδιαίτερη περιοχή του σκληρού δίσκου, της μονάδας δισκέτας ή μιας άλλης συσκευής αποθήκευσης δεδομένων του υπολογιστή. Περιέχει πληροφορίες για το σύστημα αρχείων του δίσκου και ένα πρόγραμμα φόρτωσης εκκίνησης το οποίο είναι υπεύθυνο για την εκκίνηση του λειτουργικού συστήματος.

Υπάρχει ένα πλήθος ιών που μολύνουν τους τομείς εκκίνησης, οι οποίοι ονομάζονται, κατά συνέπεια, ιοί εκκίνησης. Η εφαρμογή της Kaspersky επιτρέπει τη σάρωση των τομέων εκκίνησης για ιούς και την απολύμανσή τους σε περίπτωση εντοπισμού κάποιας μόλυνσης.

Τρωτό σημείο

Ένα ελάττωμα ενός λειτουργικού συστήματος ή μιας εφαρμογής, το οποίο μπορεί να γίνει αντικείμενο εκμετάλλευσης από δημιουργούς κακόβουλου λογισμικού με σκοπό να διεισδύσουν στο λειτουργικό σύστημα ή στην εφαρμογή και να επηρεάσουν την ακεραιότητά του/της. Η ύπαρξη μεγάλου αριθμού τρωτών σημείων σε ένα λειτουργικό σύστημα το καθιστά αναξιόπιστο, επειδή οι ιοί που έχουν διεισδύσει στο λειτουργικό σύστημα μπορεί να διαταράξουν τη λειτουργία του λειτουργικού συστήματος σύστημα και των εγκατεστημένων εφαρμογών.

Ψευδές θετικό

Κατάσταση όπου μια εφαρμογή της Kaspersky θεωρεί ένα μη μολυσμένο αντικείμενο ως μολυσμένο επειδή ο κώδικας του αντικειμένου μοιάζει με εκείνον ενός ιού.

Ψηφιακή υπογραφή

Ένα κρυπτογραφημένο μπλοκ δεδομένων που έχει ενσωματωθεί σε ένα έγγραφο ή σε μια εφαρμογή. Ο δημιουργός ενός εγγράφου ή εφαρμογής προσδιορίζεται με μια ψηφιακή υπογραφή. Για να δημιουργηθεί μια ψηφιακή υπογραφή, ο συντάκτης του εγγράφου ή της εφαρμογής πρέπει να διαθέτει ένα ψηφιακό πιστοποιητικό που αποδεικνύει την ταυτότητά του/της.

Μια ψηφιακή υπογραφή σάς επιτρέπει να επαληθεύσετε την προέλευση και την ακεραιότητα των δεδομένων και να προστατευτείτε από πλαστά δεδομένα.

Πληροφορίες σχετικά με κώδικα τρίτων

Οι πληροφορίες σχετικά με τον κώδικα τρίτων περιλαμβάνονται στο αρχείο legal_notices.txt που βρίσκεται στον φάκελο εγκατάστασης της εφαρμογής.

Επισημάνσεις για τα σήματα κατατεθέντα

Σήματα κατατεθέντα και σήματα υπηρεσιών αποτελούν ιδιοκτησία των αντίστοιχων κατόχων τους.

Οι ονομασίες Adobe και Reader είναι εμπορικά σήματα ή σήματα κατατεθέντα της Adobe Systems Incorporated στις Ηνωμένες Πολιτείες ή/και αλλού.

Οι ονομασίες Apple, macOS και Safari είναι εμπορικά σήματα της Apple Inc., κατοχυρωμένα στις Ηνωμένες Πολιτείες και αλλού.

Η ονομασία Dropbox είναι εμπορικό σήμα της Dropbox, Inc.

Οι ονομασίες Google, Google Chrome, Chromium, YouTube, SPDY, Android είναι εμπορικά σήματα της Google, Inc.

Οι ονομασίες Intel, Celeron και Atom είναι εμπορικά σήματα της Intel Corporation στις ΗΠΑ ή/και άλλες χώρες.

Οι ονομασίες Java και JavaScript είναι σήματα κατατεθέντα της Oracle ή/και των συνδεόμενων εταιρειών της.

Οι ονομασίες LogMeIn Pro και Remotely Anywhere είναι εμπορικά σήματα της LogMeIn, Inc.

Η ονομασία Mail.ru είναι εμπορικό σήμα της Mail.ru LLC.

Οι ονομασίες Microsoft, Bing, Windows, Internet Explorer, Outlook, PowerShell και Skype είναι εμπορικά σήματα της Microsoft Corporation στις Ηνωμένες Πολιτείες και άλλες χώρες.

Οι ονομασίες Mozilla, Thunderbird και Firefox είναι εμπορικά σήματα της Mozilla Foundation.

Η ονομασία VMware είναι σήμα κατατεθέν της VMware, Inc. στις Ηνωμένες Πολιτείες ή/και σε άλλες δικαιοδοσίες.

Η ονομασία IOS είναι σήμα κατατεθέν την Cisco Systems, Inc. ή/και των συνδεόμενων εταιρειών της στις Ηνωμένες Πολιτείες και σε ορισμένες άλλες χώρες.

Παράθυρο Αναβάθμιση

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Δοκιμαστική έκδοση ?</u>

Για να μεταβείτε από το Kaspersky Total Security στη δοκιμαστική έκδοση του Kaspersky Internet Security, κάντε κλικ σε αυτό το κουμπί.

<u>Αγορά κωδικού ενεργοποίησης</u> ?

Κάντε κλικ σε αυτήν τη σύνδεση για να ανοίξετε το eStore σε ένα παράθυρο του προγράμματος περιήγησης, όπου μπορείτε να αγοράσετε μια άδεια χρήσης για το Kaspersky Internet Security.

<u>Εισαγωγή κωδικού</u> 🕐

Κάντε κλικ σε αυτή τη σύνδεση για να εκτελέσετε τον οδηγό ενεργοποίησης του Kaspersky Internet Security.

Παράθυρο Αναβάθμιση

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Αγορά κωδικού ενεργοποίησης</u> 🖓

Κάντε κλικ σε αυτήν τη σύνδεση για να ανοίξετε το eStore σε ένα παράθυρο του προγράμματος περιήγησης, όπου μπορείτε να αγοράσετε έναν κωδικό ενεργοποίησης του Kaspersky Total Security.

<u>Εισαγωγή κωδικού</u> 🕐

Κάντε κλικ σε αυτή τη σύνδεση για να εκτελέσετε τον οδηγό ενεργοποίησης του Kaspersky Total Security.

<u>Δοκιμαστική έκδοση </u>?

Για να μεταβείτε από το Kaspersky Total Security στη δοκιμαστική έκδοση του Kaspersky Total Security, κάντε κλικ σε αυτό το κουμπί.

Ενεργοποίηση της εφαρμογής με νέο κωδικό ενεργοποίησης

Ανάπτυξη όλων | Σύμπτυξη όλων

Για να εφαρμόσετε νέο κωδικό ενεργοποίησης, κάντε κλικ στο κουμπί **Επόμενο**.

Εάν η άδεια χρήσης δεν έχει ακόμη λήξει, μπορείτε να εφαρμόσετε έναν κωδικό ενεργοποίησης που έχει χρησιμοποιηθεί προηγουμένως για την ενεργοποίηση της εφαρμογής σε άλλον υπολογιστή.

Για να ακυρώσετε την ενεργοποίηση της εφαρμογής, κάντε κλικ στη σύνδεση **Άκυρο**.

<u>Άκυρο</u> ?

Για να ακυρώσετε τη χρήση του νέου κωδικού ενεργοποίησης και να επιστρέψετε το παράθυρο **Εκχώρηση άδειας χρήσης**, κάντε κλικ σε αυτή τη σύνδεση.

Παράθυρο Εισαγωγή κωδικού

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κωδικός ενεργοποίησης</u> ?

Τέσσερα πεδία για την εισαγωγή του κωδικού ενεργοποίησης βρίσκονται κάτω από αυτήν τη γραμμή. Ο κωδικός ενεργοποίησης είναι η γραμμή που χωρίζεται με παύλες σε τέσσερις ομάδες χαρακτήρων και αριθμών (για παράδειγμα, **ABA9C-CDEFG-ABCBC-ABC2D**). Πληκτρολογήστε την πρώτη ομάδα των χαρακτήρων στο πρώτο πεδίο εισαγωγής, τη δεύτερη ομάδα στο δεύτερο πεδίο και ούτω καθεξής.

Κάνοντας κλικ στη σύνδεση **Πού μπορώ να βρω έναν κωδικό ενεργοποίησης;**, ανοίγει ο δικτυακός τόπος της Υπηρεσίας τεχνικής υποστήριξης σε ένα παράθυρο του προγράμματος περιήγησης, όπου παρέχονται λεπτομερείς πληροφορίες σχετικά με τον κωδικό ενεργοποίησης. Αυτή η επιλογή ενεργοποιεί τη δοκιμαστική έκδοση της εφαρμογής. Θα έχετε τη δυνατότητα να χρησιμοποιήσετε τη δοκιμαστική έκδοση της εφαρμογής με όλες τις λειτουργίες της για μια σύντομη περίοδο αξιολόγησης. Όταν λήξει η άδεια χρήσης, η δοκιμαστική έκδοση της εφαρμογής δεν θα μπορεί να επανενεργοποιηθεί.

Αυτή η επιλογή είναι διαθέσιμη αν δεν έχει χρησιμοποιηθεί ακόμη η δοκιμαστική έκδοση της εφαρμογής.

<u>Αγορά άδειας χρήσης </u>?

Κάντε κλικ σε αυτήν τη σύνδεση για να ανοίξετε το eStore σε ένα παράθυρο του προγράμματος περιήγησης, όπου μπορείτε να αγοράσετε μια άδεια χρήσης.

Ο κωδικός ενεργοποίησης αντιστοιχεί σε μια άλλη εφαρμογή

Ανάπτυξη όλων | Σύμπτυξη όλων

Αυτό το παράθυρο ανοίγει εάν ο κωδικός ενεργοποίησης που πληκτρολογήθηκε αντιστοιχεί σε άλλη εφαρμογή. Το όνομα της εφαρμογής εμφανίζεται στη γραμμή **Αντίστοιχη εφαρμογή**. Μπορείτε να αρχίσετε να χρησιμοποιείτε αυτήν την εφαρμογή τώρα ή μετά από τη λήξη της άδειάς χρήσης σας για το Kaspersky Total Security.

<u>Άκυρο</u> ?

Για να ακυρώσετε την ενεργοποίηση της εφαρμογής, κάντε κλικ σε αυτή τη σύνδεση.

<u>Συνέχεια</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ξεκινά η εγκατάσταση και ενεργοποίηση της εφαρμογής στην οποία αντιστοιχεί ο κωδικός ενεργοποίησης που πληκτρολογήθηκε.

Πώς να ρυθμίσετε το DNS μέσω προστασίας HTTPS

Ανάπτυξη όλων | Σύμπτυξη όλων

Όταν πληκτρολογείτε ένα όνομα μιας τοποθεσίας web στη γραμμή διευθύνσεων, το πρόγραμμα περιήγησης στέλνει το αίτημά σας σε έναν διακομιστή DNS. Ο διακομιστής DNS καθορίζει τη διεύθυνση IP της ζητούμενης τοποθεσίας web. Τα δεδομένα μεταφέρονται από τον υπολογιστή σας στον διακομιστή DNS χρησιμοποιώντας ένα συνηθισμένο μη κρυπτογραφημένο πρωτόκολλο κειμένου. Οι εισβολείς μπορούν να υποκλέψουν πληροφορίες σχετικά με τις τοποθεσίες web που επισκέπτεστε και να κάνουν κατάχρησή τους. Για να αποφευχθεί αυτό, αυτές οι πληροφορίες θα πρέπει να μεταφερθούν μέσω του ασφαλούς πρωτοκόλλου HTTPS. Ο διακομιστής που λαμβάνει και αναλύει αιτήματα αυτού του είδους ονομάζεται διακομιστής DNS μέσω HTTPS (ή DoH).

Το Kaspersky Total Security λαμβάνει αυτόματα δεδομένα σχετικά με τον διακομιστή DoH που χρησιμοποιείται στο πρόγραμμα περιήγησης Mozilla Firefox. Αν έχετε προσθέσει έναν διακομιστή DoH χειροκίνητα στην εφαρμογή Kaspersky Total Security και θέλετε να μεταφερθούν δεδομένα DNS μέσω του συγκεκριμένου διακομιστή DoH, θα πρέπει να προσθέσετε αυτόν τον διακομιστή στις ρυθμίσεις του προγράμματος περιήγησης Mozilla Firefox. Για πληροφορίες σχετικά με τη διαμόρφωση του διακομιστή DoH, ανατρέξτε στη Βοήθεια του Mozilla Firefox.

<u>Προσθήκη διακομιστή DoH</u> ?

Για να προσθέσετε έναν διακομιστή DoH:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- Κάντε κλικ στο κουμπί 🤨 που βρίσκεται στο κάτω μέρος του παραθύρου.
 Ανοίγει το παράθυρο Ρυθμίσεις.
- Στην ενότητα Πρόσθετα, επιλέξτε την υποενότητα Δίκτυο.
 Ανοίγει το παράθυρο Ρυθμίσεις δικτύου.
- 4. Στην ενότητα **Επεξεργασία κυκλοφορίας**, κάντε κλικ στη σύνδεση **Διαχείριση διακομιστών DoH** για να ανοίξετε το παράθυρο **Διακομιστές DoH**.
- 5. Κάντε κλικ στο κουμπί **Προσθήκη**.
- 6. Στο παράθυρο που ανοίγει, εισαγάγετε το όνομα ή τη διεύθυνση IP του διακομιστή DoH και κάντε κλικ στην επιλογή **Προσθήκη**.
- Ο διακομιστής DoH προστίθεται στη λίστα.

Παράθυρο πληροφοριών σχετικά με την τρέχουσα άδεια χρήσης

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Ναι, να χρησιμοποιηθεί το <εφαρμογή> ?</u>

Όταν ενεργοποιείται αυτή η επιλογή, ο Οδηγός ενεργοποίησης κλείνει. Η εφαρμογή θα εκτελεστεί στο πλαίσιο της τρέχουσας άδειας χρήσης που εντοπίστηκε. Εάν βρεθεί άδεια χρήσης για το Kaspersky Internet Security ή Kaspersky Anti-Virus, ανοίγει ο Οδηγός μετεγκατάστασης.

<u>Όχι, συνέχιση του Οδηγού και εισαγωγή νέου κωδικού ενεργοποίησης 🖻</u>

Εάν κάνετε αυτήν την επιλογή, ο Οδηγός ενεργοποίησης συνεχίζει να λειτουργεί και ενεργοποιεί το Kaspersky Total Security. Θα χρειαστεί να καταχωρήσετε έναν νέο κωδικό ενεργοποίησης που να είναι έγκυρος για το Kaspersky Total Security.

Παράθυρο Δήλωση εγγραφής

Καθορίστε σε αυτό το παράθυρο τα δεδομένα εγγραφής που απαιτούνται για την επικοινωνία με την Τεχνική υποστήριξη.

Η σύνδεση στο διαδίκτυο δεν είναι διαθέσιμη

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

Αυτό το παράθυρο εμφανίζεται εάν αποτύχει η ενεργοποίηση της εφαρμογής λόγω προβλημάτων με τη σύνδεσή σας στο Διαδίκτυο.

<u>Επανάληψη</u> 🕐

Αν κάνετε κλικ σε αυτή τη σύνδεση, ο Οδηγός ενεργοποίησης θα επιχειρήσει ξανά να ενεργοποιήσει την εφαρμογή. Εάν τα προβλήματα με τη σύνδεση στο Διαδίκτυο είναι προσωρινά, η νέα προσπάθεια μπορεί να είναι επιτυχημένη.

Παράθυρο Επιλέξτε πού θέλετε να τοποθετηθούν τα αρχεία μετά την επαναφορά τους

<u>Αρχικός φάκελος </u>

Όταν επιλέγεται αυτή η δυνατότητα, το Kaspersky Total Security επαναφέρει τα αρχεία στον φάκελο στον οποίο βρίσκονταν τα αρχεία προέλευσης τη στιγμή της δημιουργίας του αντιγράφου ασφαλείας.

Καθορισμένος φάκελος ?

Όταν επιλέγεται αυτή η δυνατότητα, το Kaspersky Total Security επαναφέρει τα αρχεία στον φάκελο ου καθορίζεται στο πεδίο **Επιλογή φακέλου**.

<u>Επιλογή φακέλου</u> 🕐

Το πεδίο περιέχει τη διαδρομή προς τον φάκελο στον οποίο πρέπει να εκτελεστεί η επαναφορά των αρχείων.

Το πεδίο αυτό είναι διαθέσιμο εάν έχει επιλεγεί το στοιχείο **Καθορισμένος φάκελος**.

<u>Αναζήτηση</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο **Επιλέξτε πού θέλετε να τοποθετηθούν τα αρχεία μετά την επαναφορά**. Σε αυτό το παράθυρο, μπορείτε να επιλέξετε έναν φάκελο στον οποίο πρέπει να εκτελεστεί η επαναφορά των αρχείων.

Το κουμπί αυτό είναι διαθέσιμο εάν έχει επιλεγεί το στοιχείο **Καθορισμένος φάκελος**.

<u>Σε περίπτωση διένεξης ονομάτων</u> ?

Αυτή η αναπτυσσόμενη λίστα σας δίνει τη δυνατότητα να επιλέξετε την ενέργεια που θα πραγματοποιείται από την εφαρμογή όταν στον φάκελο προορισμού για την επαναφορά του αρχείου, υπάρχει ήδη αρχείο με το ίδιο όνομα:

- Προτροπή χρήστη όταν υπάρχει διένεξη ονομάτων αρχείων, η εφαρμογή σας ειδοποιεί να επιλέξετε μία από τις εξής εναλλακτικές: αντικατάσταση του αρχείου με το αντίγραφο ασφαλείας, αποθήκευση και των δύο αρχείων ή να μην εκτελεστεί επαναφορά αυτού του αρχείου.
- αντικατάσταση αρχείου με αντίγραφο ασφαλείας Το Kaspersky Total Security διαγράφει το υπάρχον αρχείο και το αντικαθιστά με το αρχείο που επανέρχεται από

το αντίγραφο ασφαλείας.

- αποθήκευση και των δύο αρχείων Το Kaspersky Total Security αφήνει το υπάρχον αρχείο αμετάβλητο και αποθηκεύει το αρχείο που επανέρχεται από το αντίγραφο ασφαλείας με νέο όνομα στον ίδιο φάκελο.
- να μην γίνει επαναφορά αυτού του αρχείου Το Kaspersky Total Security αφήνει το υπάρχον αρχείο αμετάβλητο και δεν εκτελεί επαναφορά του αρχείου με το ίδιο όνομα από το αντίγραφο ασφαλείας.

<u>Επαναφορά</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ξεκινά η διαδικασία επαναφοράς αρχείων από τα αντίγραφα ασφαλείας.

Σφάλμα ενεργοποίησης

Ανάπτυξη όλων | Σύμπτυξη όλων

Αποτυχία ενεργοποίησης εφαρμογής. Για να δείτε πληροφορίες για το ζήτημα στη Γνωσιακή βάση, κάντε κλικ στη σύνδεση **Αιτίες και πιθανές λύσεις**.

<u>Αιτίες και πιθανές λύσεις </u>?

Ο σύνδεσμος παρέχει πρόσβασης σε ένα άρθρο της Γνωσιακής βάσης με πληροφορίες σχετικά με τις αιτίες του σφάλματος και τις πιθανές λύσεις.

Για ορισμένα σφάλματα μπορεί να μην διατίθενται σύνδεσμοι σε άρθρα της Γνωσιακής βάσης.

<u>Άκυρο</u> ?

Για να ακυρώσετε την ενεργοποίηση της εφαρμογής, κάντε κλικ σε αυτή τη σύνδεση.

Εναλλαγή σε άλλη εφαρμογή

Ανάπτυξη όλων | Σύμπτυξη όλων

Για να εκτελέσετε τον Οδηγό μετεγκατάστασης, κάντε κλικ στο κουμπί **Επόμενο**. Ο Οδηγός μετεγκατάστασης εγκαθιστά την εφαρμογή που αντιστοιχεί στον κωδικό ενεργοποίησης που πληκτρολογήθηκε (Kaspersky Internet Security ή Kaspersky Anti-Virus).

Εάν η άδεια χρήσης σας για το Kaspersky Total Security δεν έχει ακόμη λήξει, μπορείτε να εφαρμόσετε τον κωδικό ενεργοποίησης για το Kaspersky Total Security σε έναν άλλο υπολογιστή.

Για να ακυρώσετε τη μετεγκατάσταση στο Kaspersky Internet Security ή Kaspersky Anti-Virus, κάντε κλικ στη σύνδεση **Άκυρο**.

<u>Άκυρο</u> ?

Κάντε κλικ σε αυτή τη σύνδεση για να κλείσετε τον Οδηγό μετεγκατάστασης και να επιστρέψετε στο προηγούμενο βήμα.

Βεβαιωθείτε ότι ο κωδικός ενεργοποίησης που πληκτρολογείτε δεν είναι κωδικός ενεργοποίησης για συνδρομή

Ανάπτυξη όλων | Σύμπτυξη όλων

Βεβαιωθείτε ότι ο κωδικός ενεργοποίησης που ορίζετε ως νέο κωδικό, δεν προορίζεται για χρήση της εφαρμογής βάσει συνδρομής. Η πληρωμή για τη χρήση της εφαρμογής βάσει συνδρομής πραγματοποιείται κατά την αγορά της συνδρομής. Εάν έχετε αγοράσει συνδρομή για το Kaspersky Total Security, μην χρησιμοποιήσετε την εφαρμογή με την τρέχουσα άδεια χρήσης. Αντ' αυτού, ενεργοποιήστε την εφαρμογή με έναν κωδικό ενεργοποίησης συνδρομής.

Μέχρι να λήξει η άδεια χρήσης, μπορείτε να χρησιμοποιήσετε έναν ήδη χρησιμοποιημένο κωδικό ενεργοποίησης για να ενεργοποιήσετε την εφαρμογή σε άλλον υπολογιστή.

Παράθυρο Ακολουθία εκτέλεσης

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Σειρά εκτέλεσης εφαρμογών</u> ?

Η λίστα περιέχει πληροφορίες σχετικά με τις εφαρμογές που έχουν εκκινηθεί από την επιλεγμένη εφαρμογή (θυγατρικές εφαρμογές). Από προεπιλογή, οι θυγατρικές εφαρμογές ταξινομούνται σύμφωνα με το χρόνο εκκίνησής τους, ξεκινώντας με τις πιο πρόσφατες.

<u>Έναρξη</u> ?

Η στήλη αυτή εμφανίζει την ώρα κατά την οποία εκκινήθηκε μια θυγατρική εφαρμογή.

<u>ΙD διεργασίας</u> ?

Αυτή η στήλη εμφανίζει τον αριθμό της διεργασίας της εφαρμογής για παιδιά.

<u>Εφαρμογή</u> 🕐

Αυτή η στήλη εμφανίζει το όνομα της διεργασίας της εφαρμογής για παιδιά.

<u>Ομάδα αξιοπιστίας ?</u>

Αυτή η στήλη δείχνει την ομάδα αξιοπιστίας στην οποία ανήκει η εφαρμογή:

- Αξιόπιστες. Η εφαρμογή εκτελείται χωρίς οποιονδήποτε περιορισμό, αλλά παρακολουθείται από την Προστασία αρχείων από ιούς.
- Χαμηλού περιορισμού. Απαγορεύεται η πρόσβαση της εφαρμογής στα προσωπικά δεδομένα και τις ρυθμίσεις του χρήστη, καθώς και η επεξεργασία οποιωνδήποτε δημόσιων δεδομένων. Οποιαδήποτε απόπειρα αλλαγής δεδομένων συστήματος ή εκτέλεσης προνομιούχων λειτουργιών απαιτεί την άδεια του χρήστη. Η δραστηριότητα δικτύου της εφαρμογής αυτού του είδους είναι περιορισμένη.
- Υψηλού περιορισμού. Απαγορεύεται η πρόσβαση της εφαρμογής στα προσωπικά δεδομένα και τις ρυθμίσεις του χρήστη, καθώς και η πρόσβαση σε δημόσια δεδομένα ή δεδομένα συστήματος. Τυχόν προνομιούχες λειτουργίες απαιτούν την άδεια του χρήστη. Η δραστηριότητα δικτύου εφαρμογών τέτοιου είδους είναι αποκλεισμένη.
- Μη αξιόπιστες. Όλες οι δραστηριότητες των εφαρμογών αυτού του είδους αποκλείονται εντελώς.

Καρτέλα Σε εκτέλεση

Η λίστα περιέχει εφαρμογές και διεργασίες που εκτελούνται στον υπολογιστή σας τη δεδομένη στιγμή.

Κάντε δεξί κλικ για να ανοίξετε το μενού περιβάλλοντος της κεφαλίδας μιας στήλης. Το μενού περιβάλλοντος σας δίνει τη δυνατότητα να διαμορφώσετε τον τρόπο εμφάνισης των στηλών με τις πρόσθετες πληροφορίες σχετικά με τις εφαρμογές και τις διεργασίες:

- Όνομα του εκτελέσιμου αρχείου της εφαρμογής ή διεργασίας
- Λεπτομέρειες για τον προμηθευτή της εφαρμογής
- ID διεργασίας
- Διαδρομή προς το εκτελέσιμο αρχείο της εφαρμογής
- Το όνομα του χρήστη που ξεκίνησε την εφαρμογή ή τη διεργασία
- Το χρόνο δημιουργίας και εκκίνησης της εφαρμογής ή διεργασίας
- Ρυθμίσεις αυτόματης εκτέλεσης εφαρμογών

Το στοιχείο **Επαναφορά προεπιλεγμένου συνόλου στηλών** σας επιτρέπει να επαναφέρετε την προεπιλεγμένη εμφάνιση του πίνακα.

Κάνοντας δεξί κλικ στη σειρά μιας εφαρμογής ή διεργασίας, ανοίγει ένα μενού περιβάλλοντος. Από το μενού περιβάλλοντος, μπορείτε να εκτελέσετε τις παρακάτω ενέργειες:

- Να ανοίξετε το παράθυρο Κανόνες εφαρμογής, στο οποίο μπορείτε να διαμορφώσετε κανόνες για τον περιορισμό της δραστηριότητας της εφαρμογής.
- Να εμφανίσετε τη σειρά εκκίνησης των διεργασιών στο παράθυρο Αλληλουχία εκτέλεσης.
- Να μετακινήσετε την εφαρμογή σε άλλη ομάδα αξιοπιστίας.
- Να εφαρμόσετε τις προεπιλεγμένες ρυθμίσεις Ελέγχου προνομίων εφαρμογών σε μια εφαρμογή.
- Να τερματίσετε τη διεργασία.
- Να ανοίξετε το φάκελο που περιέχει το εκτελέσιμο αρχείο της εφαρμογής.

Στην αναπτυσσόμενη λίστα, μπορείτε να ενεργοποιήσετε την εμφάνιση των διεργασιών του συστήματος και των διεργασιών που εκκινήθηκαν από το Kaspersky Total Security:

- Εμφάνιση διεργασιών συστήματος. Εάν επιλέξετε αυτό το στοιχείο, η συνολική λίστα εφαρμογών και διεργασιών εμφανίζει τις διεργασίες που απαιτούνται για τη σωστή λειτουργία του λειτουργικού συστήματος.
- Εμφάνιση διεργασιών του Kaspersky Total Security. Εάν επιλέξετε αυτό το στοιχείο, η συνολική λίστα εφαρμογών και διεργασιών εμφανίζει τις διεργασίες που εκκινήθηκαν από το Kaspersky Total Security.

Στην αναπτυσσόμενη λίστα, μπορείτε να επιλέξετε έναν τρόπο προβολής για τις εφαρμογές και διεργασίες:

- Προβολή ως λίστα. Εάν επιλέξετε αυτό το στοιχείο επιλογής, οι εφαρμογές και οι διεργασίες θα εμφανίζονται ως λίστα.
- Προβολή ως δομή. Εάν επιλέξετε αυτό το στοιχείο επιλογής, οι εφαρμογές και οι διεργασίες θα εμφανίζονται σε ιεραρχική δομή με βάση τη σειρά κλήσης των διεργασιών.

<u>Εφαρμογή</u> 🕐

Αυτή η στήλη εμφανίζει το όνομα μιας εφαρμογής ή διεργασίας.

<u>Ψηφιακή υπογραφή </u>

Αυτή η στήλη εμφανίζει πληροφορίες σχετικά με το αν η εφαρμογή έχει ψηφιακά υπογεγραμμένη και πληροφορίες για τον ιδιοκτήτη της ψηφιακής υπογραφής.

<u>Ομάδα αξιοπιστίας </u>

Αυτή η στήλη δείχνει την ομάδα αξιοπιστίας στην οποία ανήκει η εφαρμογή. Ανάλογα με την ομάδα αξιοπιστίας στην οποία ανήκει η εφαρμογή, η στήλη περιέχει τα παρακάτω εικονίδια:

 Το κόκκινο εικονίδιο σημαίνει ότι η εφαρμογή βρίσκεται στη ομάδα Μη αξιόπιστες.

- Το ροζ εικονίδιο σημαίνει ότι η εφαρμογή βρίσκεται στην ομάδα Υψηλού Περιορισμού.
- Το κίτρινο εικονίδιο σημαίνει ότι η εφαρμογή βρίσκεται στην ομάδα Χαμηλού Περιορισμού.
- Το πράσινο εικονίδιο σημαίνει ότι η εφαρμογή βρίσκεται στην ομάδα αξιοπιστίας.

<u>Δημοτικότητα </u>?

Αυτή η στήλη εμφανίζει τη δημοτικότητα της εφαρμογής μεταξύ συμμετεχόντων του Kaspersky Security Network (KSN). Το επίπεδο δημοτικότητας αντικατοπτρίζει τον αριθμό των συμμετεχόντων του KSN που χρησιμοποιούν την εφαρμογή.

<u>CPU</u> ?

Αυτή η στήλη εμφανίζει το τρέχον ποσοστό κατανάλωσης πόρων CPU που αντιστοιχεί στην εφαρμογή ή τη διεργασία.

<u>Μνήμη</u> 🕐

Αυτή η στήλη εμφανίζει το τρέχον ποσοστό κατανάλωσης μνήμης RAM από την εφαρμογή ή τη διεργασία.

<u>Δίσκος</u> 🖓

Αυτή η στήλη εμφανίζει τη συνολική ταχύτητα ανάγνωσης / εγγραφής δεδομένων στο δίσκο για την εφαρμογή ή τη διεργασία.

<u>Δίκτυο</u> ?

Αυτή η στήλη εμφανίζεται τη συνολική ταχύτητα μεταφοράς δεδομένων από την εφαρμογή μέσω της διασύνδεσης δικτύου.

<u>Τερματισμός διεργασίας</u> ?

Καρτέλα που εκτελείται κατά την εκκίνηση

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

Λίστα εφαρμογών που εκτελούνται κατά την εκκίνηση 🕑

Αυτή η λίστα περιέχει τις εφαρμογές που ξεκινούν κατά την εκκίνηση του λειτουργικού συστήματος.

Κάντε δεξί κλικ για να ανοίξετε το μενού περιβάλλοντος της κεφαλίδας μιας στήλης. Το μενού περιβάλλοντος σας δίνει τη δυνατότητα να διαμορφώσετε τον τρόπο με τον οποίο εμφανίζονται οι στήλες στον πίνακα. Το στοιχείο **Επαναφορά προεπιλεγμένου συνόλου στηλών** σας επιτρέπει να επαναφέρετε την προεπιλεγμένη εμφάνιση του πίνακα.

Κάνοντας δεξί κλικ στη σειρά μιας εφαρμογής ή διεργασίας, ανοίγει ένα μενού περιβάλλοντος. Από το μενού περιβάλλοντος, μπορείτε να εκτελέσετε τις παρακάτω ενέργειες:

- Να ανοίξετε το παράθυρο Κανόνες εφαρμογής, στο οποίο μπορείτε να διαμορφώσετε κανόνες για τον περιορισμό της δραστηριότητας της εφαρμογής.
- Να μετακινήσετε την εφαρμογή σε άλλη ομάδα αξιοπιστίας.
- Να εφαρμόσετε τις προεπιλεγμένες ρυθμίσεις Ελέγχου προνομίων εφαρμογών σε μια εφαρμογή.
- Να ανοίξετε το φάκελο που περιέχει το εκτελέσιμο αρχείο της εφαρμογής.

<u>Εφαρμογή</u> 🕐

Αυτή η στήλη εμφανίζει το όνομα μιας εφαρμογής που εκτελείται κατά την εκκίνηση του λειτουργικού συστήματος.

<u>Κατάσταση</u> 🕐

Αυτή η στήλη εμφανίζει την κατάσταση της εφαρμογής: Σε εκτέλεση ή Διακόπηκε.

Αυτή η στήλη εμφανίζει πληροφορίες σχετικά με το αν η εφαρμογή έχει ψηφιακά υπογεγραμμένη και πληροφορίες για τον ιδιοκτήτη της ψηφιακής υπογραφής.

<u>Ομάδα αξιοπιστίας </u>

Αυτή η στήλη δείχνει την ομάδα αξιοπιστίας στην οποία ανήκει η εφαρμογή. Ανάλογα με την ομάδα αξιοπιστίας στην οποία ανήκει η εφαρμογή, η στήλη περιέχει τα παρακάτω εικονίδια:

- Το κόκκινο εικονίδιο σημαίνει ότι η εφαρμογή βρίσκεται στη ομάδα Μη αξιόπιστες.
- Το ροζ εικονίδιο σημαίνει ότι η εφαρμογή βρίσκεται στην ομάδα Υψηλού Περιορισμού.
- Το κίτρινο εικονίδιο σημαίνει ότι η εφαρμογή βρίσκεται στην ομάδα Χαμηλού Περιορισμού.
- Το πράσινο εικονίδιο σημαίνει ότι η εφαρμογή βρίσκεται στην ομάδα αξιοπιστίας.

<u>Δημοτικότητα</u> 🕐

Αυτή η στήλη εμφανίζει τη δημοτικότητα της εφαρμογής μεταξύ συμμετεχόντων του Kaspersky Security Network (KSN). Το επίπεδο δημοτικότητας αντικατοπτρίζει τον αριθμό των συμμετεχόντων του KSN που χρησιμοποιούν την εφαρμογή.

Τελευταία εκτέλεση ?

Αυτή η στήλη εμφανίζει την πιο πρόσφατη ώρα εκκίνησης της εφαρμογής.

Καρτέλα Όλες οι εφαρμογές

Ανάπτυξη όλων | Σύμπτυξη όλων

Αυτή η λίστα περιέχει εφαρμογές που είναι εγκατεστημένες στον υπολογιστή σας. Για κάθε εφαρμογή στη λίστα, μπορείτε να προβάλλετε πληροφορίες σχετικά με την κατάσταση, την ψηφιακή υπογραφή, την ομάδα αξιοπιστίας, τη δημοτικότητα μεταξύ των χρηστών του KSN και τον χρόνο της πιο πρόσφατης εκκίνησής της.

Κάνοντας διπλό κλικ στη σειρά μιας εφαρμογής ή διεργασίας, ανοίγει το παράθυρο **Κανόνες εφαρμογής**. Σε αυτό το παράθυρο, μπορείτε να διαμορφώσετε κανόνες για τον έλεγχο των ενεργειών της εφαρμογής.

Κάνοντας δεξί κλικ στη γραμμή της εφαρμογής ανοίγει ένα μενού περιβάλλοντος. Από το μενού περιβάλλοντος, μπορείτε να εκτελέσετε τις παρακάτω ενέργειες:

- Να ανοίξετε το παράθυρο Κανόνες εφαρμογής, στο οποίο μπορείτε να διαμορφώσετε τα δικαιώματα για τη δραστηριότητα της εφαρμογής.
- Να επιτρέψετε ή να αποκλείσετε την εκκίνηση εφαρμογών.
- Να μετακινήσετε την εφαρμογή σε άλλη ομάδα αξιοπιστίας.
- Να εφαρμόσετε τις προεπιλεγμένες ρυθμίσεις Ελέγχου προνομίων εφαρμογών σε μια εφαρμογή (επαναφορά ρυθμίσεων εφαρμογής).
- Να αφαιρέσετε την εφαρμογή από τη λίστα.
- Να ανοίξετε το φάκελο που περιέχει το εκτελέσιμο αρχείο της εφαρμογής.

Οι εφαρμογές της λίστας περιλαμβάνονται σε ομάδες και υποομάδες. Κάνοντας δεξί κλικ στη γραμμή της ομάδας, ανοίγει ένα μενού περιβάλλοντος. Από το μενού περιβάλλοντος, μπορείτε να εκτελέσετε τις παρακάτω ενέργειες:

- Να ανοίξετε το παράθυρο Κανόνες ομάδας, όπου μπορείτε να ορίσετε προεπιλεγμένα δικαιώματα για ενέργειες των εφαρμογών της συγκεκριμένης ομάδας.
- Να δημιουργήσετε μια υποομάδα στην ομάδα. Από προεπιλογή, οι κανόνες που καθορίζονται για την ομάδα στην οποία ανήκει η υποομάδα εφαρμόζονται και στην υποομάδα.
- Να προσθέσετε μια εφαρμογή στην ομάδα. Από προεπιλογή, οι κανόνες που καθορίζονται για την ομάδα στην οποία ανήκει η εφαρμογή εφαρμόζονται και στην εφαρμογή.
- Να εφαρμόσετε τις προεπιλεγμένες ρυθμίσεις Ελέγχου προνομίων εφαρμογών στην ομάδα και σε όλες τις υποομάδες και τις εφαρμογές της ομάδας (επαναφορά

ρυθμίσεων ομάδας).

- Να εφαρμόσετε τις προεπιλεγμένες ρυθμίσεις Ελέγχου προνομίων εφαρμογών σε όλες τις υποομάδες και τις εφαρμογές της ομάδας, διατηρώντας παράλληλα ανέπαφες τις ρυθμίσεις της ομάδας (επαναφορά ρυθμίσεων υποομάδας και εφαρμογής).
- Να διαγράψετε υποομάδες και εφαρμογές από την ομάδα.

<u>Εφαρμογή</u> 🕐

Αυτή η στήλη εμφανίζει το όνομα της εφαρμογής.

<u>Κατάσταση</u> 🕐

Αυτή η στήλη εμφανίζει την κατάσταση της εφαρμογής: Σε εκτέλεση ή Διακόπηκε.

<u>Ψηφιακή υπογραφή</u> 🕐

Αυτή η στήλη εμφανίζει πληροφορίες σχετικά με το αν η εφαρμογή έχει ψηφιακά υπογεγραμμένη και πληροφορίες για τον ιδιοκτήτη της ψηφιακής υπογραφής.

<u>Ομάδα αξιοπιστίας </u>

Αυτή η στήλη δείχνει την ομάδα αξιοπιστίας στην οποία ανήκει η εφαρμογή. Η ομάδα αξιοπιστίας ορίζει τους κανόνες χρήσης της εφαρμογής στον υπολογιστή: απαγόρευση ή παραχώρηση άδειας εκκίνησης, πρόσβαση της εφαρμογής σε αρχεία και στο μητρώο συστήματος και περιορισμοί στη δραστηριότητα δικτύου της εφαρμογής.

<u>Δημοτικότητα </u>

Αυτή η στήλη εμφανίζει τη δημοτικότητα της εφαρμογής μεταξύ συμμετεχόντων του Kaspersky Security Network (KSN). Το επίπεδο δημοτικότητας αντικατοπτρίζει τον αριθμό των συμμετεχόντων του KSN που χρησιμοποιούν την εφαρμογή.

Τελευταία εκτέλεση ?

Αυτή η στήλη εμφανίζει την πιο πρόσφατη ώρα εκκίνησης της εφαρμογής.

Παράθυρο Άσεμνη γλώσσα

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Συμφωνία</u> ?

Περιέχει τις προϋποθέσεις που πρέπει να πληρείτε για να πραγματοποιήσετε αλλαγές στη λίστα άσεμνων φράσεων.

<u>Είμαι ενήλικας και αποδέχομαι τους όρους 🖓</u>

Η επιλογή του πλαισίου ελέγχου υποδηλώνει αποδοχή των όρων. Εάν επιλέξετε αυτό το πλαίσιο ελέγχου, η λίστα άσεμνων φράσεων θα είναι διαθέσιμη για επεξεργασία.

Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, η λίστα άσεμνων φράσεων δεν είναι διαθέσιμη για επεξεργασία.

Παράθυρο Αποστολή σχολίων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Πρόβλημα</u> ?

Μια αναπτυσσόμενη λίστα στην οποία μπορείτε να επιλέξετε μια κατηγορία για τα σχόλιά σας. Η κατηγορία σχολίων μπορεί να ενεργοποιηθεί για πρόβλημα με δικτυακό τόπο που ανοίχτηκε στο Προστατευμένο πρόγραμμα περιήγησης:

- Δεν το χρησιμοποιώ. Επιλέξτε αυτό το στοιχείο εάν δεν χρησιμοποιείτε
 Ασφαλείς τραπεζικές συναλλαγές ή εάν αποφασίσατε να αρνηθείτε τη χρήση
 Ασφαλών τραπεζικών συναλλαγών.
- Η τοποθεσία web ανοίγει αργά. Επιλέξτε αυτό το στοιχείο εάν ο δικτυακός τόπος χρειάζεται περισσότερο χρόνο για να ανοίξει από ό,τι σε ένα κανονικό πρόγραμμα περιήγησης.
- Το Προστατευμένο πρόγραμμα περιήγησης εκκινείται όταν δεν χρειάζεται. Επιλέξτε αυτό το στοιχείο εάν ανοίγουν δικτυακοί τόποι που δεν απαιτούν τη

χρήση των Ασφαλών τραπεζικών συναλλαγών στο Προστατευμένο πρόγραμμα περιήγησης.

- **Ο έλεγχος ταυτότητας της τοποθεσίας web αποτυχαίνει**. Επιλέξτε αυτό το στοιχείο εάν προκύπτουν σφάλματα κατά την προσπάθεια εξουσιοδότησης σε δικτυακό τόπο που ανοίχτηκε στο Προστατευμένο πρόγραμμα περιήγησης.
- Η τοποθεσία web δεν εμφανίζεται σωστά ή δεν ανοίγει. Επιλέξτε αυτό το στοιχείο εάν οι δικτυακοί τόποι δεν ανοίγουν στο Προστατευμένο πρόγραμμα περιήγησης ή εάν εμφανίζονται με σφάλματα ή στρεβλώσεις.
- Σφάλματα επαλήθευσης του πιστοποιητικού τοποθεσίας web. Επιλέξτε αυτό το στοιχείο εάν εμφανίζονται μηνύματα σφάλματος κατά την επικύρωση των πιστοποιητικών δικτυακών τόπων.
- Δεν είναι δυνατή η λήψη στιγμιότυπου οθόνης όταν εκτελείται το
 Προστατευμένο πρόγραμμα περιήγησης. Επιλέξτε αυτό το στοιχείο εάν δεν δημιουργούνται στιγμιότυπα στο Προστατευμένο πρόγραμμα περιήγησης.
- Σφάλματα κατά την εισαγωγή δεδομένων μέσω πληκτρολογίου ή από το Πρόχειρο. Επιλέξτε αυτό το στοιχείο εάν προκύπτουν σφάλματα κατά την καταχώρηση δεδομένων στο Προστατευμένο πρόγραμμα περιήγησης.
- Δεν γίνεται εκτύπωση ιστοσελίδας που είναι ανοιχτή στο Προστατευμένο πρόγραμμα περιήγησης. Επιλέξτε αυτό το στοιχείο εάν δεν μπορείτε να εκτυπώσετε μια ανοικτή σελίδα ενός δικτυακού τόπου.
- Εμφανίζεται ένα μήνυμα που προειδοποιεί ότι δεν είναι εγκατεστημένες σημαντικές ενημερώσεις του λειτουργικού συστήματος. Επιλέξτε αυτό το στοιχείο εάν εμφανίζεται το μήνυμα "Δεν έχουν εγκατασταθεί κρίσιμες ενημερώσεις συστήματος" όταν εκτελείται το Προστατευμένο πρόγραμμα περιήγησης.
- Άλλο ένα πρόγραμμα περιήγησης εκτελείται ως Προστατευμένο πρόγραμμα περιήγησης. Επιλέξτε αυτό το στοιχείο εάν έχει ανοιχθεί πρόγραμμα περιήγησης σε προστατευμένη λειτουργία διαφορετικό από αυτό στο οποίο ξεκινήσατε.
- Σφάλματα λειτουργίας. Επιλέξτε αυτό το στοιχείο αν το Προστατευμένο πρόγραμμα περιήγησης επιστρέφει σφάλματα που δεν προσδιορίζονται στη λίστα.
- Άλλο. Επιλέξτε αυτό το στοιχείο εάν αντιμετωπίζετε προβλήματα που δεν καλύπτονται από τα άλλα στοιχεία.

Δεν απαιτείται να καθορίσετε την κατηγορία σχολίων.

<u>Λεπτομέρειες ?</u>

Μπορείτε να χρησιμοποιήσετε αυτό το πεδίο για να παρέχετε πληροφορίες που μπορούν να βοηθήσουν την Kaspersky στην επίλυση του προβλήματός σας. Αυτό το πεδίο είναι προαιρετικό.

<u>Αποστολή</u> ?

Αποστολή σχολίων στην Kaspersky

Μπορείτε να στέλνετε σχόλια σχετικά με τη λειτουργία του στοιχείου Ασφαλείς τραπεζικές συναλλαγές έως και 10 φορές την ημέρα. Εάν η εφαρμογή αποτύχει να στείλει τα σχόλιά σας (για παράδειγμα, δεν είναι διαθέσιμη η σύνδεση στο Διαδίκτυο), αυτά τα σχόλια θα αποθηκευτούν στον υπολογιστή σας. Τα σχόλια αποθηκεύονται φανερά για 30 ημέρες.

Δικαιώματα

Ο κωδικός πρόσβασης προστατεύει τις παρακάτω ρυθμίσεις της εφαρμογής από τυχόν αλλαγή από κάποιον χρήση ή ομάδα. Αν επιλεγεί ένα πλαίσιο ελέγχου δίπλα σε μια ενέργεια, ο χρήστης ή η ομάδα χρηστών επιτρέπεται να πραγματοποιήσει την επιλεγμένη ενέργεια.

Διαμόρφωση ρυθμίσεων εφαρμογής	Αλλάξτε τις ρυθμίσεις της εφαρμογής στο κύριο παράθυρο, το παράθυρο Ρυθμίσεις , το Κέντρο ειδοποιήσεων και τις ειδοποιήσεις. Ενεργοποιήστε και απενεργοποιήστε τα ίχνη της εφαρμογής.
Διαχείριση δημιουργίας αντιγράφων ασφαλείας	Δημιουργήστε, τροποποιήστε και καταργήστε εργασίες δημιουργίας αντιγράφων ασφαλείας και επαναφοράς.
Διαχείριση προστασίας για παιδιά	Αποκλείστε την εκκίνηση του Kaspersky Safe Kids χρησιμοποιώντας το στοιχείο Έλεγχος εφαρμογών, πραγματοποιήστε έξοδο από το Kaspersky Total Security ή ρυθμίστε τις παραμέτρους του Kaspersky Total Security, έτσι ώστε να απενεργοποιήσετε την προστασία.

	Όταν επιχειρείτε να πραγματοποιήσετε λήψη, εγκατάσταση ή εκκίνηση του Kaspersky Safe Kids, δεν σας ζητείται ο κωδικός πρόσβασης.
Έξοδος από την εφαρμογή	Πραγματοποιήστε έξοδο από την εφαρμογή.
Κατάργηση / τροποποίηση / επαναφορά της εφαρμογής	Καταργήστε, τροποποιήστε και επαναφέρετε την εφαρμογή.
Κατάργηση κλειδιού	Καταργήστε ή τροποποιήστε έναν κωδικό ενεργοποίησης. και δημιουργήστε αντίγραφο ασφαλείας κωδικού ενεργοποίησης.
Προβολή αναφορών	Μεταβείτε στο παράθυρο Αναφορές .
Απενεργοποίηση στοιχείων προστασίας	Απενεργοποιήστε και ενεργοποιήστε τα στοιχεία προστασίας που είναι διαθέσιμα στο παράθυρο Ρυθμίσεις , στην ενότητα Προστασία .

Αντιμετώπιση προβλημάτων / Επαναφορά αλλαγών

Αυτό το παράθυρο εμφανίζει την πρόοδο διόρθωσης της αλλοίωσης του λειτουργικού συστήματος που εντοπίζεται κατά την ανάλυση. Ενδέχεται να χρειαστεί αρκετή ώρα για τη διόρθωση της βλάβης.

Εάν επιλέξατε **Επαναφορά αλλαγών** στο πρώτο βήμα, ο Οδηγός αντιμετώπισης προβλημάτων των Microsoft Windows επαναφέρει τις ενέργειες που επιλέχθηκαν στο προηγούμενο βήμα.

Παράθυρο Στοιχεία άδειας χρήσης

Αυτό το παράθυρο εμφανίζει τις ακόλουθες πληροφορίες άδειας χρήσης εφαρμογής:

- Κλειδί άδειας χρήσης
- Κατάσταση άδειας χρήσης
- Αριθμός υπολογιστών που καλύπτονται από την άδεια χρήσης
- Ημερομηνία ενεργοποίησης

- Ημερομηνία λήξης άδειας
- Αριθμός ημερών πριν από τη λήξη της άδειας χρήσης
- Αναγνωριστικό ενεργοποίησης

<u>Προβολή του κωδικού ενεργοποίησης στο My Kaspersky</u> 🔋

Όταν κάνετε κλικ στη σύνδεση, η τοποθεσία web My Kaspersky ανοίγει σε μια σελίδα με πληροφορίες σχετικά με τον κωδικό ενεργοποίησης που χρησιμοποιήθηκε για την ενεργοποίηση της εφαρμογής. Μπορεί να ζητήσει να εισαγάγετε το όνομα χρήστη και τον κωδικό πρόσβασης για τον λογαριασμό σας στο My Kaspersky.

Πώς να ρυθμίσετε τις παραμέτρους το VPN για μια επιλεγμένη τοποθεσία web

Για να ρυθμίσετε τις παραμέτρους ενός VPN για μια επιλεγμένη τοποθεσία web:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Στο κύριο παράθυρο της εφαρμογής, κάντε κλικ στο κουμπί 📃.
- 3. Επιλέξτε **Ρυθμίσεις** -> **Τοποθεσίες web**.
- 4. Κάντε κλικ στο κουμπί Ρυθμίσεις.

Ανοίγει το παράθυρο **Κανόνες για τη σύνδεση σε τοποθεσίες web**.

- 5. Στην ενότητα **Εξαιρέσεις για τοποθεσίες web**, κάντε κλικ στο κουμπί **Ρυθμίσεις**. Ανοίγει το παράθυρο **Εξαιρέσεις για τοποθεσίες web**.
- Κάντε κλικ στο κουμπί Προσθήκη για να προσθέσετε έναν δικτυακό τόπο στη λίστα εξαιρέσεων από τις ρυθμίσεις που έχουν διαμορφωθεί για κατηγορίες δικτυακών τόπων.
 Ανοίγει το παράθυρο Προσθήκη τοποθεσίας web.
- 7. Εισαγάγετε τη διεύθυνση του δικτυακού τόπου στο πεδίο Διεύθυνση web (URL).
- 8. Στην ενότητα Ενέργεια όταν γίνεται πρόσβαση στην τοποθεσία web, καθορίστε την ενέργεια που θα πρέπει να εκτελεί η εφαρμογή όταν επισκέπτεστε τον συγκεκριμένο δικτυακό τόπο:

- Ενεργοποίηση VPN. Το Kaspersky Total Security θα ενεργοποιήσει μια ασφαλή σύνδεση όταν επισκεφθείτε τον καθορισμένο δικτυακό τόπο. Για παράδειγμα, μπορείτε να διαμορφώσετε την εφαρμογή έτσι, ώστε να ενεργοποιεί την ασφαλή σύνδεση όταν επισκέπτεστε τον δικτυακό τόπο της τράπεζάς σας. Αυτή η ρύθμιση εφαρμόζεται ακόμα και όταν έχει επιλεγεί η δυνατότητα Παράβλεψη στην ενότητα Κατά την περιήγηση σε μη ασφαλείς τοποθεσίες web τραπεζικών συναλλαγών στο παράθυρο Κανόνες για τη σύνδεση σε τοποθεσίες web.
 - a. Στην αναπτυσσόμενη λίστα Επιλογή διακομιστή VPN, επιλέξτε τη περιοχή από την οποία θέλετε να δημιουργείται μια ασφαλής σύνδεση όταν επισκέπτεστε τη συγκεκριμένη τοποθεσία web. Εάν η περιοχή που επιλέξατε για τη ασφαλή σύνδεση στην τοποθεσία web διαφέρει από την περιοχή που επιλέξατε για την κατηγορία τοποθεσιών web στην οποία ανήκει η τοποθεσία web, η σύνδεση στην τοποθεσία web θα δημιουργηθεί μέσω της περιοχής που έχει καθοριστεί για τη συγκεκριμένη τοποθεσία web και όχι για την κατηγορία τοποθεσιών web.
 - b. Επιλέξτε το πλαίσιο ελέγχου **Ειδοποίηση κατά την ενεργοποίηση** εάν θέλετε να λαμβάνετε ειδοποιήσεις σχετικά με το αν γίνεται ενεργοποίηση ασφαλούς σύνδεσης όταν επισκέπτεστε τον συγκεκριμένο δικτυακό τόπο.
- Παράβλεψη. Το Kaspersky Total Security δεν ενεργοποιεί την ασφαλή σύνδεση όταν επισκέπτεστε τον καθορισμένο δικτυακό τόπο.
- 9. Κάντε κλικ στο κουμπί **Προσθήκη**.

Το Kaspersky VPN Secure Connection δεν ενεργοποιεί την ασφαλή σύνδεση εάν χρησιμοποιείται πρωτόκολλο HTTPS για τη σύνδεση σε δικτυακό τόπο.

Επιστροφή στη Βοήθεια για το Kaspersky VPN Secure Connection 🗷 .

Ρύθμιση παραμέτρων VPN για κατηγορίες τοποθεσιών web

Από προεπιλογή, το Kaspersky VPN Secure Connection δεν δημιουργεί ασφαλή σύνδεση όταν ανοίγετε δικτυακούς τόπους σε κάποιο πρόγραμμα περιήγησης. Εάν το Kaspersky Internet Security, το Kaspersky Total Security ή το Kaspersky Security Cloud είναι εγκατεστημένο και ενεργοποιημένο στον υπολογιστή σας, μπορείτε να ρυθμίσετε τις παραμέτρους ενεργοποίησης VPN για διαφορετικές κατηγορίες τοποθεσιών web. Για παράδειγμα, μπορείτε να καθορίσετε ότι το VPN πρέπει να ενεργοποιείται όταν επισκέπτεστε τοποθεσίες web συστημάτων πληρωμής ή κοινωνικών δικτύων.

Για να ρυθμίσετε τις παραμέτρους VPN για κατηγορίες τοποθεσιών web:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Στο κύριο παράθυρο της εφαρμογής, κάντε κλικ στο κουμπί 🗮.
- 3. Επιλέξτε **Ρυθμίσεις** → **Τοποθεσίες web**.
- 4. Κάντε κλικ στο κουμπί **Ρυθμίσεις**.

Ανοίγει το παράθυρο **Κανόνες για τη σύνδεση σε τοποθεσίες web**.

- 5. Επιλέξτε κατηγορία δικτυακών τόπων:
 - Δικτυακοί τόποι τραπεζικών συναλλαγών. Αυτή η κατηγορία περιλαμβάνει δικτυακούς τόπους τραπεζών.
 - Συστήματα πληρωμής. Αυτή η κατηγορία περιλαμβάνει δικτυακούς τόπους συστημάτων πληρωμών.
 - Διαδικτυακά καταστήματα με ηλεκτρονικές πληρωμές. Αυτή η κατηγορία περιλαμβάνει δικτυακούς τόπους από ηλεκτρονικά καταστήματα λιανικών πωλήσεων με ενσωματωμένα συστήματα πληρωμών.
 - Μέσα κοινωνικής δικτύωσης. Αυτή η κατηγορία περιλαμβάνει δικτυακούς τόπους από κοινωνικά δίκτυα.
- Επιλέξτε μια ενέργεια που ενεργοποιείται από την επίσκεψη σε αυτή την κατηγορία δικτυακών τόπων:
 - Ενεργοποίηση VPN. Η εφαρμογή θα ενεργοποιήσει το VPN όταν επισκέπτεστε τοποθεσίες web αυτής της κατηγορίας.
 - Ερώτηση. Όταν επισκέπτεστε δικτυακό τόπο αυτής της κατηγορίας, η εφαρμογή θα σας ρωτά εάν πρέπει να δημιουργήσει ασφαλή σύνδεση για αυτό τον δικτυακό τόπο. Στο παράθυρο του προγράμματος περιήγησης, επιλέξτε την κατάλληλη ενέργεια και μετά το πλαίσιο ελέγχου Απομνημόνευση της επιλογής μου για αυτήν την τοποθεσία web. Η εφαρμογή θα εκτελεί την επιλεγμένη ενέργεια κάθε φορά που επισκέπτεστε αυτό τον δικτυακό τόπο. Εάν δεν επιλεγεί το πλαίσιο ελέγχου, η εφαρμογή απομνημονεύει την επιλογή σας για μία ώρα.
 - Παράβλεψη. Η εφαρμογή δεν θα δημιουργήσει ασφαλή σύνδεση όταν επισκέπτεστε δικτυακούς τόπους αυτής της κατηγορίας.
- 7. Εάν έχει ενεργοποιηθεί η επιλογή Ενεργοποίηση VPN, στην αναπτυσσόμενη λίστα Επιλογή διακομιστή VPN, καθορίστε την περιοχή μέσω της οποίας επιθυμείτε να

δημιουργήσετε ασφαλή σύνδεση για αυτή την κατηγορία τοποθεσιών web.

8. Επιλέξτε το πλαίσιο ελέγχου Ειδοποίηση κατά την ενεργοποίηση εάν θέλετε να λαμβάνετε ειδοποιήσεις σχετικά με το αν γίνεται ενεργοποίηση ασφαλούς σύνδεσης όταν επισκέπτεστε τη συγκεκριμένη κατηγορία δικτυακών τόπων.

Από προεπιλογή, το Kaspersky VPN Secure Connection δεν σας προτρέπει να ενεργοποιήσετε το VPN, εάν χρησιμοποιείται πρωτόκολλο HTTPS για τη σύνδεση σε δικτυακό τόπο.

Επιστροφή στη Βοήθεια για το Kaspersky VPN Secure Connection 🖬 .

Έλεγχος εφαρμογών

Ανάπτυξη όλων | Σύμπτυξη όλων

Η ενότητα **Εφαρμογές** εμφανίζει πληροφορίες για τον αριθμό των εφαρμογών που ελέγχονται από το Kaspersky Total Security.

<u>Διαχείριση εφαρμογών </u>?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Διαχείριση εφαρμογών**. Σε αυτό το παράθυρο, μπορείτε να καθορίσετε τις ομάδες αξιοπιστίας των εφαρμογών, να επιτρέψετε ή να αποκλείσετε την έναρξη των εφαρμογών, και να προβείτε στη διαμόρφωση των δικαιωμάτων για μια επιλεγμένη εφαρμογή.

Η ενότητα **Τρέχουσα δραστηριότητα** εμφανίζει πληροφορίες για τον αριθμό των εφαρμογών και διεργασιών που εκτελούνται επί του παρόντος. Πληροφορίες σχετικά με το φορτίο της CPU, τον όγκο της RAM, τον ελεύθερο χώρο στο δίσκο, και τη δραστηριότητα του δικτύου παρέχονται σε μορφή γραφικών.

<u>Εμφάνιση όλης της δραστηριότητας 🖓</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Δραστηριότητα εφαρμογών** στην καρτέλα **Σε εκτέλεση**. Σε αυτό το παράθυρο, μπορείτε να δείτε πληροφορίες σχετικά με την κατανάλωση των πόρων από κάθε μία από τις εφαρμογές που εκτελούνται τη δεδομένη στιγμή ή να προχωρήσετε στη διαμόρφωση των δικαιωμάτων για μια επιλεγμένη εφαρμογή.

Έλεγχος εφαρμογών. Εξαιρέσεις

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Εξαιρέσεις</u> 🕐

Περιλαμβάνει πόρους με προσωπικά δεδομένα που εξαιρούνται από την ισχύ προστασίας του Ελέγχου εφαρμογών. Ο πόρος μπορεί να είναι ένα αρχείο, ένας φάκελος ή ένα κλειδί μητρώου.

<u>Πόρος</u> ?

Αυτή η στήλη εμφανίζει το όνομα του πόρου.

<u>Διαδρομή</u> 🕐

Αυτή η στήλη εμφανίζει την τοποθεσία του πόρου. Η διαδρομή μπορεί να περιλαμβάνει μια μάσκα.

<u>Κατάσταση </u>

Η στήλη αυτή περιέχει μια αναπτυσσόμενη λίστα με τις επιλογές κατάστασης πόρων:

- Ενεργοποίηση ελέγχου. Εάν επιλέξετε αυτή την εναλλακτική, η εφαρμογή ελέγχει τη δραστηριότητα που σχετίζεται ειδικά με αυτόν τον πόρο.
- Απενεργοποίηση ελέγχου. Εάν επιλέξετε αυτή την εναλλακτική, η εφαρμογή δεν ελέγχει τη δραστηριότητα που σχετίζεται ειδικά με αυτόν τον πόρο.

Μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε τον έλεγχο πόρων στην αναπτυσσόμενη λίστα κάνοντας αριστερό κλικ στο εικονίδιο κατάστασης.

<u>Προσθήκη</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο στο οποίο μπορείτε να ορίσετε τον πόρο με τα προσωπικά δεδομένα που προσθέτετε στη λίστα.

<u>Επεξεργασία</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί ανοίγει το παράθυρο **Επεξεργασία αρχείου ή φακέλου/Επεξεργασία κλειδιού μητρώου**. Σε αυτό το παράθυρο, μπορείτε να επεξεργαστείτε τις ρυθμίσεις του πόρου.

Δεν μπορείτε να επεξεργαστείτε πόρους που έχουν προστεθεί στη λίστα από προεπιλογή.

<u>Διαγραφή</u> 🕐

Εάν κάνετε κλικ σε αυτό το κουμπί, ο επιλεγμένος πόρος καταργείται από τη λίστα. Δεν μπορείτε να διαγράψετε πόρους που έχουν προστεθεί στη λίστα από προεπιλογή.

Καρτέλα Γενικά

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Καρτέλα Γενικά</u> ?

Περιγραφή της επιλεγμένης ομάδας εφαρμογών.

Καρτέλα Πόροι

Ανάπτυξη όλων | Σύμπτυξη όλων

Η καρτέλα αυτή σας δίνει τη δυνατότητα να επιλέξετε πόρους συστήματος ή χρήστη και να τροποποιήσετε τα δικαιώματα πρόσβασης των εφαρμογών σε αυτούς τους πόρους.



Το κουμπί αυτό μπορεί να χρησιμοποιηθεί για την εμφάνιση ή απόκρυψη του πίνακα ρυθμίσεων κανόνων.

<u>Εμφάνιση</u> 🕐

Σε αυτή την αναπτυσσόμενη λίστα μπορείτε να επιλέξετε ανάμεσα σε δύο επιλογές φιλτραρίσματος πόρων:

 Απόκρυψη εφαρμογών συστήματος. Εάν επιλέξετε αυτή την εναλλακτική, οι πόροι των εφαρμογών συστήματος αποκρύπτονται από τη λίστα πόρων. • **Απόκρυψη Kaspersky Total Security**. Εάν επιλέξετε αυτή την εναλλακτική, οι πόροι του Kaspersky Total Security αποκρύπτονται από τη λίστα πόρων.

<u>Λειτουργικό σύστημα </u>?

Αυτή η λίστα περιέχει τις ρυθμίσεις και τους πόρους του λειτουργικού συστήματος εντός της επιλεγμένης κατηγορίας. Ο πόρος μπορεί να είναι αρχείο, φάκελος, κλειδί μητρώου, υπηρεσία δικτύου ή διεύθυνση IP. Ο Έλεγχος εφαρμογών παρακολουθεί την πρόσβαση που έχουν άλλες εφαρμογές στους πόρους αυτής της λίστας.

Από προεπιλογή, η λίστα **Λειτουργικό σύστημα** περιλαμβάνει τα ακόλουθα αντικείμενα:

- Κλειδιά μητρώου που περιέχουν ρυθμίσεις εκκίνησης
- Κλειδιά μητρώου που περιέχουν ρυθμίσεις για τη χρήση του Διαδικτύου
- Κλειδιά μητρώου που επηρεάζουν την ασφάλεια του λειτουργικού συστήματος
- Κλειδιά μητρώου που περιέχουν ρυθμίσεις για τις υπηρεσίες συστήματος
- Αρχεία και φακέλους του συστήματος
- Φακέλους εκκίνησης

<u>Προσωπικά δεδομένα</u> ?

Περιέχει τα προσωπικά δεδομένα του χρήστη, ταξινομημένα κατά πόρους και κατηγορίες. Ο πόρος μπορεί να είναι αρχείο ή φάκελος. Ο Έλεγχος εφαρμογών αναλύει τις ενέργειες που εκτελούν άλλες εφαρμογές στους πόρους της λίστας.

Από προεπιλογή, η λίστα προσωπικών δεδομένων περιλαμβάνει τα ακόλουθα αντικείμενα:

- Αρχεία χρήστη (τον φάκελο Τα έγγραφά μου (My Documents), αρχεία cookie, πληροφορίες σχετικά με τις δραστηριότητες του χρήστη)
- Αρχεία, φακέλους και κλειδιά μητρώου που περιέχουν τις ρυθμίσεις και σημαντικά δεδομένα των εφαρμογών που χρησιμοποιούνται πιο συχνά: προγράμματα περιήγησης, προγράμματα διαχείρισης αρχείων, προγράμματαπελάτες email, προγράμματα-πελάτες IM και ηλεκτρονικά πορτοφόλια

<u>Πόρος</u> ?

Αυτή η στήλη εμφανίζει το όνομα του πόρου του λειτουργικού συστήματος που προστατεύεται από τον Έλεγχο εφαρμογών.

<u>Διαδρομή</u> 🕐

Αυτή η στήλη εμφανίζει την τοποθεσία του πόρου. Η διαδρομή μπορεί να περιλαμβάνει μια μάσκα.

<u>Κατάσταση</u> 🕐

Η στήλη αυτή περιέχει μια αναπτυσσόμενη λίστα με τις επιλογές κατάστασης πόρων:

- Ενεργοποίηση ελέγχου. Εάν επιλέξετε αυτή την εναλλακτική, η εφαρμογή ελέγχει τη δραστηριότητα που σχετίζεται ειδικά με αυτόν τον πόρο.
- Απενεργοποίηση ελέγχου. Εάν επιλέξετε αυτή την εναλλακτική, η εφαρμογή δεν ελέγχει τη δραστηριότητα που σχετίζεται ειδικά με αυτόν τον πόρο.

Μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε τον έλεγχο πόρων στην αναπτυσσόμενη λίστα κάνοντας αριστερό κλικ στο εικονίδιο κατάστασης.

<u>Προσθήκη</u> ?

Σε αυτή την αναπτυσσόμενη λίστα μπορείτε να προσθέσετε μια κατηγορία πόρων, ένα αρχείο ή φάκελο με πόρους, ή ένα κλειδί μητρώου συστήματος.

<u>Επεξεργασία</u> 🕐

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο στο οποίο μπορείτε να επεξεργαστείτε το όνομα του επιλεγμένου πόρου καθώς και τη διαδρομή προς αυτόν.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτή τη σύνδεση, καταργείται η επιλεγμένη κατηγορία πόρων, το αρχείο ή ο φάκελος με τους πόρους, ή ένα κλειδί μητρώου συστήματος από τη λίστα. Ο Έλεγχος εφαρμογών σταματά να ελέγχει την πρόσβαση άλλων εφαρμογών σε αυτόν τον πόρο. Από αυτήν την αναπτυσσόμενη λίστα μπορείτε να επιλέξετε μία από τις εξής επιλογές:

- **ρυθμίσεις της κατηγορίας**. Εάν αυτή η επιλογή είναι ενεργοποιημένη,
 εκχωρούνται προεπιλεγμένες τιμές στις ρυθμίσεις της επιλεγμένης κατηγορίας.
- ρυθμίσεις υποομάδων και πόρων. Εάν αυτή η επιλογή είναι ενεργοποιημένη, εκχωρούνται προεπιλεγμένες τιμές στις ρυθμίσεις των υποομάδων και των πόρων που ανήκουν στην κατηγορία.

<u>Λίστα εφαρμογών </u>

Η λίστα αυτή παραθέτει τις ομάδες αξιοπιστίας και τις εφαρμογές που ανήκουν σε αυτές. Οι στήλες **Ανάγνωση, Εγγραφή**, **Δημιουργία** και **Διαγραφή** καθορίζουν τα δικαιώματα πρόσβασης που έχει μια εφαρμογή ή ομάδα εφαρμογών για τον επιλεγμένο πόρο.

Ο παρακάτω πίνακας περιέχει τις λειτουργίες που εκτελούνται από το Kaspersky Total Security όταν μια εφαρμογή ή ομάδα εφαρμογών επιχειρεί να αποκτήσει πρόσβαση στον πόρο.

Περιγραφή των ενεργειών του Kaspersky Total Security

Ενέργεια	Περιγραφή
Μεταβίβαση	Η απόκριση από τη γονική ομάδα μεταβιβάζεται στην εφαρμογή ή την ομάδα εφαρμογών.
Να επιτρέπεται	Το Kaspersky Total Security επιτρέπει την πρόσβαση στο δίκτυο στις εφαρμογές που περιλαμβάνονται στον επιλεγμένο πόρο.
Αποκλεισμός	Το Kaspersky Total Security δεν επιτρέπει την πρόσβαση στο δίκτυο στις εφαρμογές που περιλαμβάνονται στον επιλεγμένο πόρο.
Προτροπή χρήστη	Εάν το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών είναι επιλεγμένο στις Ρυθμίσεις → Γενικά , το Kaspersky Total Security επιλέγει αυτόματα την ενέργεια που θα εκτελέσει σε αυτόν τον πόρο βάσει των κανόνων που έχουν δημιουργήσει οι ειδικοί της Kaspersky. Μπορείτε να ακολουθήσετε την υποσημείωση για να διαβάσετε ακριβώς ποια ενέργεια θα επιλεγεί.

	Εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου, η εφαρμογή ρωτά τον χρήστη εάν θα επιτρέψει ή όχι σε αυτήν την εφαρμογή να έχει πρόσβαση στον πόρο.
Καταγραφή συμβάντων	Εκτός από την καθορισμένη απόκριση, το Kaspersky Total Security καταγράφει πληροφορίες σχετικά με τις προσπάθειες της εφαρμογής για πρόσβαση στον πόρο και προσθέτει τις πληροφορίες σε μια αναφορά.

Παράθυρο Άδειας Χρήσης Τελικού Χρήστη

Ανάπτυξη όλων | Σύμπτυξη όλων

Το παράθυρο αυτό περιέχει το κείμενο της Άδειας Χρήσης Τελικού Χρήστη. Χρησιμοποιήστε τη ράβδο κύλισης για να δείτε την Άδεια Χρήσης Τελικού Χρήστη.

Πώς να κάνετε επαναφορά σε προηγούμενη έκδοση της εφαρμογής

Για επαναφορά στην έκδοση premium της εφαρμογής:

- 1. Πατήστε Win + Ε στο πληκτρολόγιο.
- 2. Μεταβείτε στον φάκελο:
 - C:\Program Files\Kaspersky Lab\Kaspersky Total Security <application version> – Για χρήστες λειτουργικών συστημάτων 32 bit.
 - C:\Program Files (x86)\Kaspersky Lab\Kaspersky Total Security
 <application version> Για χρήστες λειτουργικών συστημάτων 64 bit.
- 3. Αντιγράψτε το αρχείο install.cfg.imported στην επιφάνεια εργασίας.
- 4. Μετονομάστε το αντιγραμμένο αρχείο σε settings.cfg.
- 5. Διαγραφή του Kaspersky Total Security.
- 6. Όταν διαγράφετε την εφαρμογή, βεβαιωθείτε ότι στο παράθυρο **Αποθήκευση** αντικειμένων είναι επιλεγμένο το πλαίσιο ελέγχου **Στοιχεία άδειας χρήσης**.
- Επανεκκινήστε τον υπολογιστή σας και πραγματοποιήστε <u>λήψη του αρχείου</u> εγκατάστασης ^I για την προηγούμενη έκδοση της εφαρμογής από τον διακομιστή Kaspersky.
- 8. Εκκινήστε το αρχείο εγκατάστασης.
- 9. Απορρίψτε την προσφορά για έλεγχο και λήψη της τελευταίας έκδοσης κάνοντας κλικ στο κουμπί **Παράλειψη**. Συνεχίστε την εγκατάσταση.
- 10. Μετά την ολοκλήρωση της εγκατάστασης, στο κύριο παράθυρο του Kaspersky Total Security κάντε κλικ στο κουμπί 💿.
- 11. Επιλέξτε **Διαχείριση ρυθμίσεων** → **Εισαγωγή**.
- 12. Επιλέξτε το αρχείο settings.cfg και κάντε κλικ στο κουμπί Άνοιγμα.
- 13. Εάν η εφαρμογή σας ζητήσει επιβεβαίωση, κάντε κλικ στο κουμπί **Συνέχεια**.

Περιμένετε να ολοκληρωθεί η εισαγωγή των ρυθμίσεων.

- 14. Μεταβείτε στην ενότητα **Πρόσθετα** και επιλέξτε **Αναβάθμιση**.
- 15. Επιλέξτε Να μην γίνεται αυτόματη λήψη των νέων εκδόσεων και να μην λαμβάνω ειδοποίηση όταν υπάρχουν διαθέσιμες νέες εκδόσεις.

Θα εγκατασταθεί η προηγούμενη έκδοση της εφαρμογής με διατήρηση των ρυθμίσεων και δεν θα αναβαθμιστεί πλέον.

Παράθυρο Εκχώρηση άδειας χρήσης

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

Στοιχεία για την άδεια χρήσης εμφανίζονται στην ενότητα που βρίσκεται στο επάνω μέρος του παραθύρου:

• Κλειδί άδειας χρήσης

Μπορείτε να σταματήσετε τη χρήση της εφαρμογής με την τρέχουσα άδεια χρήσης, κάνοντας κλικ στο κουμπί 🗙.

- Κατάσταση κλειδιού
- Αριθμός υπολογιστών που καλύπτονται από την άδεια χρήσης
- Ημερομηνία ενεργοποίησης

- Ημερομηνία λήξης άδειας
- Αριθμός ημερών πριν από τη λήξη της άδειας χρήσης

Για τις συνδρομές, είναι επίσης δυνατή η εμφάνιση πρόσθετων πληροφοριών σχετικά με την κατάσταση της συνδρομής.

<u>Σχετικά με την άδειά σας/Σχετικά με τη συνδρομή σας 🖻</u>

Κάνοντας κλικ σε αυτήν τη σύνδεση ανοίγει ένα παράθυρο που παρέχει πληροφορίες σχετικά με την τρέχουσα άδεια χρήσης ή τη συνδρομή.

Άδεια Χρήσης Τελικού Χρήστη 🖓

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο στο οποίο εμφανίζεται το κείμενο της Άδειας Χρήσης.

Ανάλογα με την παρουσία άδειας χρήσης, τη συνδρομή και τις ιδιότητες της δικής σας έκδοσης της εφαρμογής, το παράθυρο ενδέχεται να εμφανίζει διαφορετικά κουμπιά για την εκκίνηση ενεργειών που σχετίζονται με την άδεια χρήσης ή τη συνδρομή σας. Τα προεπιλεγμένα κουμπιά περιγράφονται παρακάτω.

<u>Ενεργοποίηση της εφαρμογής / Εισαγωγή κωδικού 🖓</u>

Εάν κάνετε κλικ σε αυτό το κουμπί, εκκινεί ο Οδηγός Ενεργοποίησης.

Αυτό το κουμπί εμφανίζεται σε περίπτωση που η εφαρμογή δεν είναι ενεργοποιημένη, εάν μπορεί να εισαχθεί νέος κωδικός ενεργοποίησης ή εάν η συνδρομή υπό την οποία χρησιμοποιείτε την εφαρμογή έχει λήξει ή λήγει σύντομα.

<u>Αγορά άδειας χρήσης </u>

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει στο πρόγραμμα περιήγησης ένα ηλεκτρονικό κατάστημα, όπου μπορείτε να αγοράσετε μια άδεια χρήσης.

Το κουμπί δεν εμφανίζεται αν έχει οριστεί κάποιος νέος κωδικός ενεργοποίησης, επιπλέον της τρέχουσας άδειας χρήσης.

Ανάκτηση των δικών μου κωδικών ενεργοποίησης ව

Κάνοντας κλικ σε αυτή τη σύνδεση, μπορείτε να μεταβείτε στην τοποθεσία web My Kaspersky και να δείτε πληροφορίες σχετικά με τους δικούς σας κωδικούς ενεργοποίησης.

Επιστροφή στο Kaspersky Anti-Virus 🖓

Κάνοντας κλικ σε αυτό το κουμπί, γίνεται μετάβαση από το Kaspersky Total Security στο Kaspersky Anti-Virus.

Το κουμπί είναι διαθέσιμο εάν έχετε πραγματοποιήσει μετάβαση από την εμπορική ή δοκιμαστική έκδοση του Kaspersky Anti-Virus στη δοκιμαστική έκδοση του Kaspersky Total Security και η άδεια χρήσης σας για το Kaspersky Anti-Virus δεν έχει λήξει.

<u>Ενεργοποίηση τώρα</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, η εφαρμογή ενεργοποιείται με ένα νέο κωδικό ενεργοποίησης.

Αυτό το κουμπί είναι διαθέσιμο εάν, πριν τη λήξη της άδειας χρήσης, η εφαρμογή δεν έχει ενεργοποιηθεί αυτόματα με νέο κωδικό ενεργοποίησης.

<u>Διαγραφή κωδικού ενεργοποίησης </u>

Κάνοντας κλικ σε αυτό το κουμπί, διαγράφεται ο νέος κωδικός ενεργοποίησης. Αυτό δεν επηρεάζει την τρέχουσα άδεια χρήσης.

Το κουμπί εμφανίζεται αν έχει καθοριστεί κάποιος νέος κωδικός ενεργοποίησης.

<u>Ενημέρωση βάσεων δεδομένων</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ξεκινάει η ενημέρωση των βάσεων δεδομένων των εφαρμογών.

Αυτό το κουμπί είναι διαθέσιμο σε περίπτωση που κάποια προβλήματα με την τρέχουσα άδεια χρήσης μπορούν να λυθούν με την ενημέρωση των βάσεων δεδομένων (για παράδειγμα, η ημερομηνία έκδοσης των βάσεων δεδομένων δεν αντιστοιχεί στην ημερομηνία λήξης της άδειας χρήσης). Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο ενός προγράμματος περιήγησης, στο οποίο εμφανίζεται μια ιστοσελίδα στο δικτυακό τόπο της Τεχνικής υποστήριξης που παρέχει πληροφορίες σχετικά με κάποιο πρόβλημα που προέκυψε.

Αυτό το κουμπί είναι διαθέσιμο σε περίπτωση που προκύψουν προβλήματα με την τρέχουσα άδεια χρήσης ή το νέο κωδικό ενεργοποίησης.

Επαλήθευση κωδικού ενεργοποίησης ?

Κάνοντας κλικ σε αυτό το κουμπί, εκκινείται ο Οδηγός ενεργοποίησης προκειμένου να επαληθευτεί ο νέος κωδικός ενεργοποίησης.

Αυτό το κουμπί είναι διαθέσιμο, εάν απέτυχε μια προσπάθεια αυτόματης επαλήθευσης του νέου κωδικού ενεργοποίησης.

<u>Ενημέρωση κατάστασης</u> ව

Κάνοντας κλικ σε αυτό το κουμπί, πραγματοποιείται λήψη ενημερωμένων πληροφοριών σχετικά με την κατάσταση της συνδρομής από τον διακομιστή του παρόχου.

Αυτό το κουμπί εμφανίζεται εάν η εφαρμογή χρησιμοποιείται στα πλαίσια συνδρομής.

Επισκεφθείτε την τοποθεσία web του παρόχου της υπηρεσίας 💿

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο του προγράμματος περιήγησης, στο οποίο εμφανίζεται ο δικτυακός τόπος του φορέα παροχής υπηρεσιών.

Αυτό το κουμπί εμφανίζεται εάν η εφαρμογή χρησιμοποιείται στα πλαίσια συνδρομής.

Άλλες μη συμβατές εφαρμογές που εντοπίστηκαν

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

<u>Λίστα μη συμβατών εφαρμογών 🖓</u>

Η λίστα περιέχει τις εφαρμογές που δεν είναι συμβατές με την εφαρμογή που εγκαθίσταται. Καταργήστε τις μη συμβατές εφαρμογές για να λειτουργήσει σωστά η εφαρμογή που εγκαθίσταται.

Κατάργηση χειροκίνητα 🖓

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο που περιέχει μια λίστα εφαρμογών που είναι εγκατεστημένες στον υπολογιστή. Σε αυτό το παράθυρο μπορείτε να επιλέξετε εφαρμογές που δεν είναι συμβατές με την εφαρμογή που εγκαθίσταται τη συγκεκριμένη χρονική στιγμή προκειμένου να τις αφαιρέσετε από τον υπολογιστή σας.

<u>Συνέχεια</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, οι μη συμβατές εφαρμογές που περιλαμβάνονται στη λίστα παραμένουν στον υπολογιστή σας και ο Οδηγός συνεχίζει να εκτελείται.

Η ταυτόχρονη χρήση μη συμβατών εφαρμογών με την εφαρμογή που εγκαθίσταται μπορεί να οδηγήσει στη λανθασμένη λειτουργία της εφαρμογής που εγκαθίσταται και να διαταράξει σε σημαντικό βαθμό την προστασία του υπολογιστή σας.

Εντοπίστηκε μη συμβατό λογισμικό

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Λίστα μη συμβατών εφαρμογών 🖻</u>

Η λίστα περιέχει τις εφαρμογές που δεν είναι συμβατές με την εφαρμογή που εγκαθίσταται. Καταργήστε τις μη συμβατές εφαρμογές για να λειτουργήσει σωστά η εφαρμογή που εγκαθίσταται.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, οι μη συμβατές εφαρμογές που περιλαμβάνονται στη λίστα καταργούνται από τον υπολογιστή σας και ο Οδηγός συνεχίζει να εκτελείται.

<u>Διατήρηση</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, οι μη συμβατές εφαρμογές που περιλαμβάνονται στη λίστα παραμένουν στον υπολογιστή σας και ο Οδηγός συνεχίζει να εκτελείται.

Η ταυτόχρονη χρήση μη συμβατών εφαρμογών με την εφαρμογή που εγκαθίσταται μπορεί να οδηγήσει στη λανθασμένη λειτουργία της εφαρμογής που εγκαθίσταται και να διαταράξει σε σημαντικό βαθμό την προστασία του υπολογιστή σας.

Απαιτείται επανεκκίνηση του υπολογιστή

Ανάπτυξη όλων | Σύμπτυξη όλων

Επανεκκίνηση του υπολογιστή 🖓

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την επανεκκίνηση του υπολογιστή. Ο υπολογιστής πρέπει να επανεκκινηθεί για να συνεχιστεί ο Οδηγός μετεγκατάστασης.

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, τότε κάνοντας κλικ στο κουμπί **Ολοκληρώθηκε** γίνεται επανεκκίνηση του υπολογιστή, μετά από την οποία συνεχίζεται ο Οδηγός μετεγκατάστασης.

Εάν αυτό το πλαίσιο ελέγχου δεν είναι επιλεγμένο, δεν γίνεται επανεκκίνηση του υπολογιστή. Ο Οδηγός μετεγκατάστασης συνεχίζεται αυτόματα αφού κάνετε επανεκκίνηση του υπολογιστή ή την επόμενη φορά που θα τον ανοίξετε.

Πρώτα βήματα

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Εμφάνιση πληροφοριών πιστοποιητικού 🖓</u>

Ο σύνδεσμος αυτός ανοίγει ένα παράθυρο όπου εμφανίζονται πληροφορίες σχετικά με το πιστοποιητικό της Kaspersky.

<u>Επόμενο</u> ?

Εάν κάνετε κλικ σε αυτό το κουμπί, ανοίγει ο Οδηγός εγκατάστασης πιστοποιητικού.

Εγκατάσταση πιστοποιητικού

Αυτό το παράθυρο εμφανίζει την πρόοδο της αυτόματης εγκατάστασης του πιστοποιητικού. Η ολοκλήρωση της εργασίας ενδέχεται να διαρκέσει αρκετή ώρα.

Το Kaspersky Total Security αναζητά στον υπολογιστή του χρήστη εγκατεστημένα προγράμματα περιήγησης στον ιστό και, στη συνέχεια, εγκαθιστά πιστοποιητικά αυτόματα στο χώρο αποθήκευσης πιστοποιητικών των Microsoft Windows.

Κατά την εγκατάσταση του πιστοποιητικού, ενδεχομένως να εμφανιστεί στην οθόνη μια ειδοποίηση από το σύστημα ασφάλειας των Microsoft Windows, η οποία σας ζητά να επιβεβαιώσετε την εγκατάσταση του πιστοποιητικού.

Ολοκλήρωση Οδηγού

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Ολοκληρώθηκε</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security κλείνει τον Οδηγό εγκατάστασης πιστοποιητικού.

Ενότητα Υπολογιστές που έχουν αποκλειστεί

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

Υπολογιστές που έχουν αποκλειστεί 🖓

Περιλαμβάνει πληροφορίες σχετικά με τους υπολογιστές για τους οποίους ο Αποκλεισμός επιθέσεων δικτύου έχει απαγορεύσει κάθε δραστηριότητα δικτύου με προορισμό τον υπολογιστή σας.

<u>Διεύθυνση υπολογιστή</u> 🕑

Αυτή η στήλη εμφανίζει τη διεύθυνση ΙΡ ενός υπολογιστή που έχει αποκλειστεί.

<u> Άρα έναρξης αποκλεισμού</u> ?

Αυτή η στήλη εμφανίζει την ώρα που έχει περάσει από τον αποκλεισμό του υπολογιστή.

Από προεπιλογή, ο Αποκλεισμός επιθέσεων δικτύου αποκλείει για μία ώρα την εισερχόμενη κυκλοφορία από έναν υπολογιστή που επιτίθεται.

Για να καταργήσετε τον αποκλεισμό ενός υπολογιστή που έχει επιλεγεί στη λίστα, ανοίξτε το μενού περιβάλλοντός του.

<u>Κατάργηση αποκλεισμού</u> 🖓

Κάνοντας κλικ σε αυτή τη σύνδεση, το Πρόγραμμα αποκλεισμού επιθέσεων δικτύου καταργεί τον αποκλεισμό του επιλεγμένου υπολογιστή.

<u>Κατάργηση αποκλεισμού όλων των υπολογιστών 🖻</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, το Πρόγραμμα αποκλεισμού επιθέσεων δικτύου καταργεί τον αποκλεισμό όλων των αποκλεισμένων υπολογιστών.

Ενότητα Ανοικτές θύρες

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

<u>Εμφάνιση</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα μενού που περιλαμβάνει τα ακόλουθα στοιχεία:

- Εμφάνιση όλων των θυρών στη λίστα εμφανίζονται όλες οι ανοικτές θύρες που υπάρχουν στον υπολογιστή σας.
- Απόκρυψη θυρών βρόχου επιστροφής (loopback) στη λίστα εμφανίζονται όλες οι θύρες εκτός από αυτές που χρησιμοποιούνται από το λογισμικό δικτύου του λειτουργικού σας συστήματος.

<u>Ανοικτές θύρες </u>

Περιλαμβάνει πληροφορίες σχετικά με όλες τις ανοικτές θύρες για κάθε διεργασία. Για κάθε θύρα εμφανίζονται οι ακόλουθες πληροφορίες:

- Αριθμός θύρας
- Όνομα διεργασίας (εφαρμογή, υπηρεσία, διακομιστής) που χρησιμοποιεί τη θύρα
- ID διεργασίας
- Τοπική διεύθυνση ΙΡ της διεργασίας
- Πρωτόκολλο για τη σύνδεση μέσω της θύρας

Κάνοντας διπλό κλικ σε μια γραμμή στη λίστα, ανοίγει το παράθυρο **Κανόνες** εφαρμογής στην καρτέλα **Κανόνες δικτύου**. Σε αυτό το παράθυρο, μπορείτε να ρυθμίσετε τους κανόνες του δικτύου για την εφαρμογή που χρησιμοποιεί την επιλεγμένη θύρα.

Κάνοντας δεξί κλικ σε ένα στοιχείο της λίστας, ανοίγει ένα μενού περιβάλλοντος, από το οποίο μπορείτε να ρυθμίσετε τους κανόνες του δικτύου.

Το μενού περιλαμβάνει τα ακόλουθα στοιχεία:

- Κανόνες δικτύου εφαρμογής. Επιλέγοντας αυτό το στοιχείο μενού, ανοίγει το παράθυρο Κανόνες εφαρμογής στην καρτέλα Κανόνες δικτύου. Σε αυτό το παράθυρο, μπορείτε να διαμορφώσετε έναν κανόνα δικτύου για την εφαρμογή που χρησιμοποιεί τη θύρα που επιλέχθηκε από τη λίστα.
- Όλοι οι κανόνες δικτύου. Η επιλογή αυτού του στοιχείου μενού ανοίγει το παράθυρο Κανόνες πακέτου. Σε αυτό το παράθυρο, μπορείτε να διαμορφώσετε κανόνες πακέτων για την εφαρμογή που χρησιμοποιεί τη θύρα που επιλέχθηκε από τη λίστα.

Ενότητα Δραστηριότητα δικτύου

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

<u>Εμφάνιση</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα μενού. Το μενού περιλαμβάνει τα ακόλουθα στοιχεία:

Εμφάνιση τοπικών συνδέσεων – η λίστα εμφανίζει πληροφορίες σχετικά με τις συνδέσεις του υπολογιστή σας προς άλλους υπολογιστές στο ίδιο τοπικό δίκτυο.

 Εμφάνιση συνδέσεων του Kaspersky Total Security – η λίστα εμφανίζει πληροφορίες σχετικά με τις συνδέσεις που έχει πραγματοποιήσει το Kaspersky Total Security.

<u>Δραστηριότητα δικτύου</u> 🖓

Αυτή η λίστα περιέχει όλες τις ενεργές συνδέσεις δικτύου που έχουν δημιουργηθεί εκείνη τη στιγμή στον υπολογιστή σας.

Για κάθε σύνδεση εμφανίζονται οι ακόλουθες πληροφορίες:

- Όνομα διεργασίας (εφαρμογή, υπηρεσία, διακομιστής) που ξεκίνησε τη σύνδεση
- Κατεύθυνση σύνδεσης (εισερχόμενη / εξερχόμενη)
- Πρωτόκολλο σύνδεσης
- Ρυθμίσεις σύνδεσης (απομακρυσμένη θύρα και διεύθυνση IP)
- Όγκος δεδομένων μεταφοράς / λήψης (σε kilobyte)

Κάνοντας δεξί κλικ σε ένα στοιχείο της λίστας, ανοίγει ένα μενού περιβάλλοντος, από το οποίο μπορείτε να ρυθμίσετε τους κανόνες του δικτύου.

Το μενού περιλαμβάνει τα ακόλουθα στοιχεία:

- Κανόνες δικτύου εφαρμογής. Επιλέγοντας αυτό το στοιχείο μενού, ανοίγει το παράθυρο Κανόνες εφαρμογής στην καρτέλα Κανόνες δικτύου. Σε αυτό το παράθυρο, μπορείτε να διαμορφώσετε ένα κανόνα δικτύου για μια εφαρμογή που επιλέχθηκε από τη λίστα.
- Όλοι οι κανόνες δικτύου. Η επιλογή αυτού του στοιχείου μενού ανοίγει το παράθυρο Κανόνες πακέτου. Σε αυτό το παράθυρο, μπορείτε να διαμορφώσετε κανόνες πακέτων για την εφαρμογή επιλεγμένη από τη λίστα.

<u>Αποκλεισμός όλης της δραστηριότητας δικτύου 🖓</u>

Κάνοντας κλικ στη σύνδεση οδηγεί το Τείχος προστασίας στο να αποκλείσει τη δραστηριότητα δικτύου όλων των διεργασιών.

Στο κάτω μέρος του παραθύρου εμφανίζεται ένα διάγραμμα της κυκλοφορίας δικτύου που παρουσιάζει όγκους εισερχόμενης και εξερχόμενης κυκλοφορίας για μια διεργασία που επιλέγετε από τη λίστα. Το διάγραμμα αντικατοπτρίζει τον όγκο της κυκλοφορίας σε πραγματικό χρόνο. Ο όγκος της κυκλοφορίας εμφανίζεται σε kilobyte.

Ειδικές συνθήκες κατά την προσθήκη ενός κανόνα για έναν προσαρμογέα δικτύου

Όταν δημιουργείτε έναν κανόνα αποδοχής για έναν προσαρμογέα δικτύου ή/και έναν κανόνα με καθορισμένο TTL, αυτός ο κανόνας ενδέχεται να έρχεται σε διένεξη με έναν κανόνα απόρριψης για εφαρμογές. Για παράδειγμα, εάν μια εφαρμογή ανήκει στην ομάδα Υψηλού Περιορισμού, δεν θα έχει πρόσβαση στο δίκτυο ακόμα και αν δημιουργήσατε έναν κανόνα πακέτου αποδοχής για τον προσαρμογέα δικτύου (και για TTL).

Για να διαμορφώσετε έναν κανόνα αποδοχής για όλες τις εφαρμογές που προσπαθούν να συνδεθούν στο δίκτυο μέσω αυτού του προσαρμογέα δικτύου, πρέπει να δημιουργήσετε τους ακόλουθους κανόνες με σειρά προτεραιότητας από την υψηλότερη προτεραιότητα έως τη χαμηλότερη προτεραιότητα (στη γενική λίστα κανόνων πακέτων, η προτεραιότητα καθορίζεται από επάνω προς τα κάτω, από την υψηλότερη προτεραιότητα έως τη χαμηλότερη προτεραιότητα).

- 1. Κανόνας αποδοχής για τον επιλεγμένο προσαρμογέα δικτύου.
- 2. Κανόνες απόρριψης για όλους τους άλλους προσαρμογείς δικτύου.
- 3. Κανόνας αποδοχής χωρίς να καθορίζεται προσαρμογέας δικτύου.

Για να ρυθμίσετε τις παραμέτρους ενός κανόνα αποδοχής για να λειτουργεί για έναν προσαρμογέα δικτύου που χρησιμοποιεί TTL, πρέπει να δημιουργήσετε τους ακόλουθους κανόνες με σειρά προτεραιότητας από την υψηλότερη έως τη χαμηλότερη προτεραιότητα:

- 1. Κανόνας αποδοχής για συγκεκριμένη τιμή ΤΤL.
- 2. Κανόνας απόρριψης για τιμή ΤΤL ίση με 255.
- 3. Κανόνας αποδοχής χωρίς να καθορίζεται τιμή TTL.

Ενότητα Κυκλοφορία δικτύου

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Περίοδος</u> ?

Η λίστα περιέχει χρονικά διαστήματα για την προβολή της κατανομής της κυκλοφορίας δικτύου.

Διαθέσιμες τιμές:

- Για σήμερα. Αυτή η λίστα εμφανίζει δεδομένα για την κατανομή της κυκλοφορίας δικτύου για την τρέχουσα ημέρα.
- Για χθες. Αυτή η λίστα εμφανίζει δεδομένα για την κατανομή της κυκλοφορίας δικτύου για την προηγούμενη ημέρα.
- Για τον μήνα. Αυτή η λίστα εμφανίζει δεδομένα σχετικά με την κατανομή της κυκλοφορίας δικτύου για τον τρέχοντα μήνα.
- Για το έτος. Αυτή η λίστα εμφανίζει δεδομένα σχετικά με την κατανομή της κυκλοφορίας δικτύου για το τρέχον έτος.

<u>Κυκλοφορία δικτύου</u> ?

Περιέχει πληροφορίες για όλες τις εισερχόμενες και εξερχόμενες συνδέσεις που έχουν πραγματοποιηθεί μεταξύ του υπολογιστή σας και άλλων υπολογιστών.

Ο όγκος της εισερχόμενης και εξερχόμενης κυκλοφορίας εμφανίζεται για κάθε εφαρμογή (υπολογιστής, υπηρεσία, διακομιστής, διεργασία).

Κάνοντας διπλό κλικ σε μια εφαρμογή στη λίστα, ανοίγει το παράθυρο **Κανόνες** εφαρμογής στην καρτέλα **Κανόνες δικτύου**. Σε αυτό το παράθυρο, μπορείτε να διαμορφώσετε τους κανόνες δικτύου της επιλεγμένης εφαρμογής.

Κάνοντας δεξί κλικ σε ένα στοιχείο της λίστας, ανοίγει ένα μενού περιβάλλοντος, από το οποίο μπορείτε να ρυθμίσετε τους κανόνες του δικτύου.

Το μενού περιλαμβάνει τα ακόλουθα στοιχεία:

- Κανόνες δικτύου εφαρμογής. Αν επιλέξετε αυτό το στοιχείο, ανοίγει το παράθυρο Κανόνες εφαρμογής στην καρτέλα Κανόνες δικτύου, όπου μπορείτε να διαμορφώσετε έναν κανόνα δικτύου για την επιλεγμένη εφαρμογή.
- Όλοι οι κανόνες δικτύου. Αν επιλέξετε αυτό το στοιχείο ανοίγει το παράθυρο Κανόνες πακέτου, στο οποίο μπορείτε να διαμορφώσετε κανόνες πακέτων για την επιλεγμένη εφαρμογή.

Στο κάτω μέρος του παραθύρου εμφανίζεται ένα διάγραμμα που δείχνει την κατανομή της κυκλοφορίας για την επιλεγμένη εφαρμογή συν τω χρόνω κατά το καθορισμένο χρονικό διάστημα.

Τερματισμός συνδέσεων δικτύου

Εάν ο υπολογιστής τερματιστεί ή η προστασία διακοπεί όταν η εφαρμογή παρακολουθεί ενεργές συνδέσεις δικτύου, θα εμφανιστεί μια ειδοποίηση τερματισμού αυτών των συνδέσεων. Αυτό είναι απαραίτητο για τη σωστή έξοδο από την εφαρμογή. Ο τερματισμός πραγματοποιείται αυτόματα αφού περάσουν 10 δευτερόλεπτα ή μόλις κάνετε κλικ στο κουμπί **Ναι**. Οι περισσότερες από τις συνδέσεις που τερματίζονται, ανακτώνται μετά από λίγο.

Εάν η σύνδεση τερματιστεί όταν πραγματοποιείτε λήψη ενός αρχείου χωρίς το πρόγραμμα διαχείρισης λήψεων, η μετάδοση δεδομένων θα διακοπεί. Για να πραγματοποιήσετε λήψη του αρχείου, πρέπει να ξεκινήσετε εκ νέου τη διαδικασία λήψης.

Μπορείτε να ακυρώσετε τον τερματισμό των συνδέσεων. Για να το κάνετε αυτό, κάντε κλικ στο κουμπί **Όχι** στο πλαίσιο διαλόγου της ειδοποίησης. Η εφαρμογή συνεχίζει να εκτελείται.

Αναζήτηση για προβλήματα / Αναζήτηση για αλλαγές

Αυτό το παράθυρο εμφανίζει την πρόοδο της ανάλυσης των ρυθμίσεων του Microsoft Internet Explorer ή της αναζήτησης των προηγούμενων αλλαγών που είχαν γίνει από τον Οδηγό ρύθμισης παραμέτρων του προγράμματος περιήγησης.

Η διαδικασία αυτή μπορεί να διαρκέσει αρκετή ώρα. Μπορείτε να διακόψετε τη διαδικασία κάνοντας κλικ στο **Άκυρο**.

Η αναζήτηση για προβλήματα ολοκληρώθηκε / Η αναζήτηση για αλλαγές ολοκληρώθηκε

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Λίστα προβλημάτων</u> 😨

Παραθέτει τα προβλήματα που εντοπίστηκαν από το Kaspersky Total Security κατά το προηγούμενο βήμα. Το Kaspersky Total Security ομαδοποιεί τα εντοπισμένα προβλήματα ανάλογα με τον κίνδυνο που ενέχουν:

- Προβλήματα που συνιστάται ιδιαίτερα να επιδιορθωθούν. Τρωτά σημεία του προγράμματος περιήγησης που αποτελούν σοβαρή απειλή για την ασφάλεια του συστήματος.
- Προβλήματα που συνιστάται να επιδιορθωθούν. Τρωτά σημεία του προγράμματος περιήγησης που ενδεχομένως να είναι επικίνδυνα για τον

υπολογιστή.

 Προβλήματα που μπορούν να επιδιορθωθούν. Τρωτά σημεία τα οποία δεν αποτελούν άμεση απειλή αυτήν τη στιγμή, αλλά ενδέχεται να απειλήσουν την ασφάλεια του υπολογιστή στο μέλλον.

Εάν το πλαίσιο ελέγχου στη γραμμή ενός προβλήματος είναι επιλεγμένο, το Kaspersky Total Security επιχειρεί να εξαλείψει το πρόβλημα.

Εάν αυτό το πλαίσιο ελέγχου στη γραμμή ενός προβλήματος δεν είναι επιλεγμένο, το Kaspersky Total Security δεν θα εξαλείψει το πρόβλημα.

Εάν επιλέξατε **Επαναφορά αλλαγών** στο πρώτο βήμα του Οδηγού ρύθμισης παραμέτρων του προγράμματος περιήγησης, η λίστα περιέχει προβλήματα που διορθώθηκαν σε προγενέστερο χρόνο. Μπορείτε να επαναφέρετε τις αλλαγές που διενεργήθηκαν για την εξάλειψη αυτών των προβλημάτων.

Ρυθμίσεις παραμέτρων προγράμματος περιήγησης

Ανάπτυξη όλων | Σύμπτυξη όλων

Εκτέλεση διαγνωστικού ελέγχου για τον Microsoft Internet Explorer ව

Το Kaspersky Total Security ξεκινά την ανάλυση των ρυθμίσεων του Microsoft Internet Explorer.

<u>Επαναφορά αλλαγών ?</u>

Το Kaspersky Total Security επαναφέρει τις αλλαγές που πραγματοποιήθηκαν σε προγενέστερο χρόνο από τον Οδηγό ρύθμισης παραμέτρων του προγράμματος περιήγησης.

Αυτή η επιλογή είναι διαθέσιμη αν ο Οδηγός ρύθμισης παραμέτρων του προγράμματος περιήγησης έχει κάνει τυχόν αλλαγές στις ρυθμίσεις του προγράμματος περιήγησης σε προγενέστερο χρόνο.

Επιδιόρθωση προβλημάτων / Επαναφορά αλλαγών

Αυτό το παράθυρο εμφανίζει την πρόοδο της εξάλειψης των προβλημάτων που προκύπτουν κατά την ανάλυση των ρυθμίσεων του προγράμματος περιήγησης. Ενδέχεται να χρειαστεί αρκετή ώρα για τη διόρθωση των προβλημάτων.

Εάν επιλέξατε **Επαναφορά αλλαγών** στο πρώτο βήμα, ο Οδηγός ρύθμισης παραμέτρων του προγράμματος περιήγησης επαναφέρει τις ενέργειες που επιλέχθηκαν στο προηγούμενο βήμα.

Ολοκλήρωση του Οδηγού

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Ολοκληρώθηκε</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, εκτελείται έξοδος από τον Οδηγό ρύθμισης παραμέτρων του προγράμματος περιήγησης.

<u>Επανεκκίνηση του υπολογιστή ?</u>

Αν το πλαίσιο ελέγχου είναι επιλεγμένο, ο υπολογιστής πραγματοποιεί επανεκκίνηση αφού ολοκληρώσετε τον Οδηγό.

Σχετικά με τις προηγμένες επιλογές για VPN

Οι πρόσθετες δυνατότητες ασφαλούς σύνδεσης είναι διαθέσιμες όταν το Kaspersky Internet Security, το Kaspersky Total Security ή το Kaspersky Security Cloud είναι εγκατεστημένο και εκτελείται στον υπολογιστή σας.

Οι πρόσθετες δυνατότητες του VPN περιλαμβάνουν:

- Ρυθμίσεις για την ενεργοποίηση του VPN κατά την επίσκεψη των ακόλουθων κατηγοριών τοποθεσιών web:
 - Δικτυακοί τόποι τραπεζικών συναλλαγών
 - Συστήματα πληρωμής
 - Ηλεκτρονικά καταστήματα και ηλεκτρονικού εμπορίου
 - Μέσα κοινωνικής δικτύωσης
- Ρυθμίσεις για την αυτόματη αλλαγή της περιοχής. Εάν έχετε καθορίσει διαφορετικές περιοχές για τοποθεσίες web διαφορετικών κατηγοριών στις ρυθμίσεις VPN, μπορείτε να καθορίσετε εάν θέλετε να αλλάζει ή να μην αλλάζει η περιοχή κατά την μετακίνησή σας μεταξύ τοποθεσιών web διαφορετικών κατηγοριών.

 Ρυθμίσεις VPN για μεμονωμένες τοποθεσίες web, για παράδειγμα, για τοποθεσίες web που επισκέπτεστε συχνά.

Επιστροφή στη Βοήθεια για το Kaspersky VPN Secure Connection 🖬 .

Αντικείμενα που εντοπίστηκαν

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

<u>Επίλυση</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security ξεκινά την επεξεργασία του αντικειμένου που εντοπίστηκε.

Το κουμπί αυτό είναι διαθέσιμο εάν έχει εντοπιστεί κάποιο αντικείμενο.

Κάνοντας κλικ στο κουμπί , ανοίγει ένα μενού από το οποίο μπορείτε να επιλέξετε μια πρόσθετη ενέργεια:

- Η επιλογή Προσθήκη στις εξαιρέσεις δημιουργεί μια εξαίρεση που προβλέπει ότι το αντικείμενο δεν πρέπει να αναγνωρίζεται ως κακόβουλο.
- Η επιλογή Παράβλεψη μετακινεί την ειδοποίηση στην ενότητα Ειδοποιήσεις που έχουν παραβλεφθεί.
- Η επιλογή Άνοιγμα φακέλου στον οποίο περιέχεται ανοίγει το φάκελο που περιείχε αρχικά το αρχείο.
- Η επιλογή Μάθετε περισσότερα ανοίγει μια ιστοσελίδα με την περιγραφή του αντικειμένου που έχει εντοπιστεί.

Παράθυρο Ειδοποιήσεις του Kaspersky Total Security

Οι ειδοποιήσεις που εμφανίζονται στην περιοχή ειδοποιήσεων της γραμμής εργασιών σάς ενημερώνουν για συμβάντα που παρουσιάζονται κατά τη λειτουργία της εφαρμογής και απαιτούν την προσοχή σας.

Εάν μια ειδοποίηση εμφανιστεί στην οθόνη, θα πρέπει να κάνετε μία από τις επιλογές που προτείνονται στην ειδοποίηση. Η βέλτιστη επιλογή είναι εκείνη που συνιστάται ως προεπιλογή από τους ειδικούς της Kaspersky.

Παράθυρο Γονικός έλεγχος

Περιέχει λογαριασμούς χρηστών.

Η λίστα εμφανίζει τις ακόλουθες πληροφορίες για τον χρήστη:

- Εικόνα του χρήστη που έχει επιλεγεί στις ρυθμίσεις του Γονικού ελέγχου
- Ψευδώνυμο χρήστη
- Κατάσταση ελέγχου χρήστη όπως έχει οριστεί για τον Γονικό έλεγχο (Ενεργοποιημένο ή Απενεργοποιημένο)

<u>Εικόνα χρήστη</u> 🕐

Κάνοντας κλικ σε μια εικόνα χρήστη, ανοίγει ένα παράθυρο με στατιστικά στοιχεία αναφορικά με τη χρήση του Διαδικτύου και των εφαρμογών από τον συγκεκριμένο χρήστη. Από αυτό το παράθυρο, μπορείτε να δείτε την αναφορά Γονικού ελέγχου και να διαμορφώσετε τις ρυθμίσεις Γονικού ελέγχου.

<u>Ρύθμιση παραμέτρων περιορισμών</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο στο οποίο μπορείτε να διαμορφώσετε τον έλεγχο των ενεργειών του χρήστη χρησιμοποιώντας το Γονικό έλεγχο.

<u>Προβολή αναφοράς</u> 🕐

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο που εμφανίζει στατιστικά στοιχεία χρήσης του Διαδικτύου και της εφαρμογής από τον επιλεγμένο χρήστη. Από αυτό το παράθυρο, μπορείτε να δείτε την αναφορά Γονικού ελέγχου και να διαμορφώσετε τις ρυθμίσεις Γονικού ελέγχου.

<u>Κουμπί</u> 🛛 🌔 / 🔵

Αυτό το κουμπί ενεργοποιεί / απενεργοποιεί τον έλεγχο των ενεργειών του χρήστη:

💽 – όταν είναι ενεργοποιημένος ο έλεγχος των ενεργειών του χρήστη

– όταν είναι απενεργοποιημένος ο έλεγχος των ενεργειών του χρήστη

Παράθυρο Δημιουργία κωδικού

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Προστασία με χρήση κωδικού πρόσβασης </u>

Εμφανίζεται κατά την πρόσβαση στις ρυθμίσεις του Γονικού ελέγχου, αν δεν έχει οριστεί κωδικός πρόσβασης για τον περιορισμό της πρόσβασης στις επιλογές διαχείρισης του Kaspersky Total Security. Περιλαμβάνει τα ακόλουθα στοιχεία περιβάλλοντος διασύνδεσης:

- Κωδικός πρόσβασης. Σε αυτό το πεδίο, πληκτρολογήστε έναν κωδικό πρόσβασης.
- Επιβεβαίωση. Σε αυτό το πεδίο, πληκτρολογήστε ξανά τον κωδικό πρόσβασης.
- Συνέχεια. Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο Γονικός έλεγχος, από το οποίο μπορείτε να δείτε τα προφίλ χρηστών και να διαμορφώσετε τις ρυθμίσεις του Γονικού ελέγχου.
- Παράλειψη. Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο Γονικός έλεγχος. Η πρόσβαση στη διαχείριση του Γονικού ελέγχου δεν είναι περιορισμένη.

<u>Εισαγωγή κωδικού πρόσβασης</u> 🖓

Εμφανίζεται όταν επιχειρείτε να αποκτήσετε πρόσβαση στις ρυθμίσεις Γονικού ελέγχου, εάν η πρόσβαση προστατεύεται με κωδικό πρόσβασης. Περιλαμβάνει τα ακόλουθα στοιχεία περιβάλλοντος διασύνδεσης:

- Πεδίο εισαγωγής κωδικού πρόσβασης.
- Σύνδεση. Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο Γονικός έλεγχος.
- Αποθήκευση κωδικού για την περίοδο λειτουργίας. Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security διατηρεί στη μνήμη τον κωδικό πρόσβασης και δεν εμφανίζει πλέον σχετική ερώτηση κατά τη διάρκεια της τρέχουσας περιόδου λειτουργίας.

Πληροφορίες για την Προστασία Cloud

Μπορείτε να ενημερωθείτε για το Kaspersky Security Network σε αυτό το παράθυρο.

Παράθυρο Ενεργοποίηση

Ανάπτυξη όλων | Σύμπτυξη όλων

Το παράθυρο αυτό εμφανίζει την πρόοδο της ενεργοποίησης της εφαρμογής.

<u>Άκυρο</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, μπορείτε να ακυρώσετε την ενεργοποίηση της εφαρμογής.

Εγγραφή

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Διεύθυνση email 🕐</u>

Ένα πεδίο για την εισαγωγή της διεύθυνσης email για τη σύνδεση στην τοποθεσία web My Kaspersky.

<u>Κωδικός πρόσβασης </u>

Ένα πεδίο για την εισαγωγή του κωδικού πρόσβασης για τη σύνδεση στην τοποθεσία web My Kaspersky.

<u>Σύνδεση</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, συνδέεστε στην τοποθεσία web My Kaspersky.

Ξεχάσατε τον κωδικό πρόσβασής σας; ?

Μεταβείτε στο παράθυρο επαναφοράς ξεχασμένου κωδικού πρόσβασης για λογαριασμό My Kaspersky.

<u>Δημιουργία λογαριασμού</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, μεταβαίνετε στη φόρμα εγγραφής της τοποθεσίας web My Kaspersky.

<u>Επιβεβαίωση σύνδεσης</u> ?

Εάν ρυθμίσατε τις παραμέτρους για επαλήθευση δύο βημάτων στην τοποθεσία web My Kaspersky, θα σταλεί γραπτό μήνυμα με τον κωδικό επαλήθευσης στο τηλέφωνό σας. Εισαγάγετε τον κωδικό επαλήθευσης στο αντίστοιχο πεδίο και κάντε κλικ στο κουμπί **Επιβεβαίωση σύνδεσης**.

Η επαλήθευση δύο βημάτων δεν είναι διαθέσιμη σε κάθε περιοχή. Για περισσότερες πληροφορίες, ανατρέξτε στη <u>Βοήθεια για το My Kaspersky</u>.

Όταν συνεχίζετε με την εγγραφή στην τοποθεσία web My Kaspersky, το παράθυρο εμφανίζει τα ακόλουθα πεδία:

<u>Διεύθυνση email ?</u>

Ένα πεδίο για την εισαγωγή της διεύθυνσης email για εγγραφή στην τοποθεσία web My Kaspersky.

<u>Κωδικός πρόσβασης</u> 🕐

Ένα πεδίο για την εισαγωγή του κωδικού πρόσβασης για εγγραφή στην τοποθεσία web My Kaspersky.

<u>Περιοχή</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο επιλογής περιοχής. Οι εφαρμογές που μπορείτε να εγκαταστήσετε και οι διαθέσιμες μέθοδοι πληρωμών που μπορείτε να χρησιμοποιήσετε εξαρτώνται από την περιοχή που έχετε επιλέξει.

<u>Το όνομά σας</u> 🕐

Πεδίο εισαγωγής του ονόματός σας. Το πεδίο αυτό μπορεί να μην εμφανίζεται σε όλες τις περιοχές. Πεδίο εισαγωγής του επιθέτου σας. Το πεδίο αυτό μπορεί να μην εμφανίζεται σε όλες τις περιοχές.

<u>Πού αγοράσατε την εφαρμογή;</u> 🖓

Σε αυτό το πεδίο, μπορείτε να επιλέξετε το κατάστημα από όπου αγοράσατε το Kaspersky Total Security.

<u>Συμφωνώ να παρέχω στην Kaspersky τη διεύθυνση email μου για τη λήψη εξατομικευμένων</u> <u>προσφορών μάρκετινγκ</u> ?

Εάν επιλέξετε αυτό το πλαίσιο ελέγχου, θα λαμβάνετε τα νέα της Kaspersky στην καθορισμένη διεύθυνση ηλεκτρονικού ταχυδρομείου.

Επιβεβαιώνω ότι επιτρέπω στην AO Kaspersky Lab να χρησιμοποιεί το προσωπικό μου email και το ονοματεπώνυμό μου για να επικοινωνεί μαζί μου μέσω email για εξατομικευμένες ειδικές προσφορές, κριτικές, έρευνες, υπενθυμίσεις ολοκλήρωσης παραγγελιών, σχετικά νέα και εκδηλώσεις.

Εάν επιλέξετε αυτό το πλαίσιο ελέγχου, θα λαμβάνετε τα νέα της Kaspersky και ειδικές προσφορές στην καθορισμένη διεύθυνση ηλεκτρονικού ταχυδρομείου. Αυτό το πλαίσιο ελέγχου είναι διαθέσιμο σε <u>συγκεκριμένες περιοχές</u>.

Σε ορισμένες περιοχές αυτό το πλαίσιο ελέγχου ονομάζεται Επιβεβαιώνω ότι επιτρέπω στην AO Kaspersky Lab να χρησιμοποιεί την προσωπική μου διεύθυνση email για να επικοινωνεί μαζί μου μέσω email για εξατομικευμένες ειδικές προσφορές, κριτικές, έρευνες, υπενθυμίσεις ολοκλήρωσης παραγγελιών, σχετικά νέα και εκδηλώσεις.

<u>Δημιουργία</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, καταχωρείται ο λογαριασμός My Kaspersky. Αποστέλλεται ένα μήνυμα email με τη σύνδεση ενεργοποίησης του λογαριασμού My Kaspersky, στη διεύθυνση email που καθορίσατε. Η διάταξη του πεδίου κατά τη δημιουργία ενός λογαριασμού σχεδιάζεται από ειδικούς της Kaspersky και ενδέχεται να αλλάξει.

Παράθυρο Επιλογή κλειδιού από μητρώο

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

<u>Επιλογή</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, τα πεδία στο παράθυρο **Προσθήκη κλειδιού** μητρώου συμπληρώνονται με τις τιμές του επιλεγμένου κλειδιού.

Παράθυρο Επιλογή θέσης θαλάμου δεδομένων

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

Σε αυτό το παράθυρο μπορείτε να επιλέξετε τον φάκελο όπου θα αποθηκευτεί ο θάλαμος δεδομένων.

<u>Επιλογή</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, μπορείτε να επιβεβαιώσετε ότι η συγκεκριμένη διαδρομή είναι σωστή.

Παράθυρο Επιλογή αρχείου ή φακέλου

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

<u>Επιλογή</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, εμφανίζεται η διαδρομή προς ένα αρχείο ή φάκελο στο πεδίο **Διαδρομή** του παραθύρου **Προσθήκη αρχείου ή φακέλου**.

Παράθυρο Ομάδα αξιοπιστίας για τις άγνωστες εφαρμογές

Ανάπτυξη όλων | Σύμπτυξη όλων

Αυτό το παράθυρο εμφανίζει εφαρμογές που δεν ήταν δυνατόν να προστεθούν στις υπάρχουσες ομάδες. Μπορείτε να επιλέξετε μια ομάδα αξιοπιστίας και να κάνετε κλικ στο κουμπί **Αποθήκευση**. Οι εφαρμογές που δεν μπορούσαν να προστεθούν σε άλλες ομάδες θα προστεθούν στην ομάδα που καθορίσατε.

Από προεπιλογή, αυτές οι εφαρμογές προστίθενται στην ομάδα Χαμηλού περιορισμού.

Παράθυρο Ομάδα αξιοπιστίας για εφαρμογές που εκκινούνται πριν από την εκκίνηση του Kaspersky Total Security

Ανάπτυξη όλων | Σύμπτυξη όλων

Σε αυτό το παράθυρο μπορείτε να επιλέξετε μια ομάδα αξιοπιστίας για τις άγνωστες εφαρμογές που εκκινούνται πριν από την εκκίνηση του Kaspersky Total Security.

Λίστα ομάδων αξιοπιστίας ?

Χρησιμοποιήστε αυτήν τη λίστα για να καθορίσετε μια ομάδα αξιοπιστίας στην οποία θα εκχωρούνται οι εφαρμογές που εκκινούνται πριν από την εκκίνηση του Kaspersky Total Security. Η δραστηριότητα δικτύου αυτών των εφαρμογών περιορίζεται σύμφωνα με τους κανόνες της επιλεγμένης ομάδας αξιοπιστίας. Από προεπιλογή, η δραστηριότητα δικτύου των εφαρμογών που εκκινούνται πριν από την εκκίνηση του Kaspersky Total Security περιορίζεται σύμφωνα με τους κανόνες που έχουν διαμορφωθεί από την Kaspersky.

Αυτόματη επιλογή ομάδας αξιοπιστίας 🖓

Εάν επιλέξετε αυτή την εναλλακτική, το στοιχείο Ελέγχου εφαρμογών προσθέτει εφαρμογές που ξεκίνησαν πριν από την εκκίνηση του Kaspersky Total Security σε μια ομάδα αξιοπιστίας βάσει των κανόνων που έχουν δημιουργηθεί από τους ειδικούς της Kaspersky.

<u>Χειροκίνητη επιλογή ομάδας αξιοπιστίας </u>?

Εάν επιλέξετε αυτή την εναλλακτική, μπορείτε να επιλέξετε χειροκίνητα την ομάδα αξιοπιστίας στην οποία θα πρέπει να προστίθενται οι εφαρμογές που ξεκινούν πριν από την εκκίνηση του Kaspersky Total Security.

Παράθυρο Προσθήκη / επεξεργασία εξαίρεσης από την Ιδιωτική περιήγηση

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Μάσκα διεύθυνσης web</u> ?

Χρησιμοποιήστε αυτό το πεδίο για να καθορίσετε τη διεύθυνση IP ή τη διεύθυνση web (URL) του δικτυακού τόπου στον οποίο θέλετε να επιτρέπεται η παρακολούθηση της online δραστηριότητάς σας.

Παράθυρο Προσθήκη / Επεξεργασία κατηγορίας

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

<u>Όνομα κατηγορίας </u>

Σε αυτό το πεδίο μπορείτε να καθορίσετε το όνομα μιας κατηγορίας πόρων. Η πρόσβαση σε αυτήν την κατηγορία πόρων θα αναλύεται και θα ελέγχεται από τον Έλεγχο εφαρμογών.

Παράθυρο Προσθήκη / Επεξεργασία κλειδιού μητρώου

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Επιλογή</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο **Επιλογή κλειδιού από μητρώο** στο οποίο μπορείτε να επιλέξετε ένα κλειδί μητρώου, το οποίο πρέπει να διαχειρίζεται ο Έλεγχος εφαρμογών όσον αφορά την πρόσβαση.

<u>Όνομα</u> ?

Σε αυτό το πεδίο μπορεί να εισαχθεί το όνομα ενός πόρου με το κλειδί μητρώου.

Διαδρομή προς το κλειδί 🖓

Σε αυτό το πεδίο μπορεί να εισαχθεί η διαδρομή προς ένα κλειδί μητρώου.

<u>Προστασία τιμής κλειδιού</u> ?

Εάν επιλεγεί αυτό το πλαίσιο ελέγχου, μόνο η τιμή του κλειδιού που ορίζεται στο πεδίο **Τιμή κλειδιού** θα προστατεύεται από τροποποίηση.

Εάν το πλαίσιο ελέγχου δεν είναι επιλεγμένο, προστατεύονται όλες οι τιμές αυτού του κλειδιού μητρώου.

Εάν δεν οριστεί κάποια τιμή στο πεδίο **Τιμή κλειδιού**, η προεπιλεγμένη τιμή του κλειδιού μητρώου προστατεύεται από προεπιλογή.

Αυτό το πλαίσιο ελέγχου επιλέγεται αυτόματα όταν επιλέγεται ένα κλειδί μητρώου.

<u>Τιμή κλειδιού</u> ?

Σε αυτό το πεδίο μπορείτε να καθορίσετε την τιμή ενός κλειδιού μητρώου, το οποίο πρέπει να προστατεύεται από τον Έλεγχο εφαρμογών όσον αφορά την τροποποίηση.

Το πεδίο αυτό είναι επεξεργάσιμο εάν είναι επιλεγμένο το πλαίσιο ελέγχου **Προστασία τιμής κλειδιού**.

<u>Προσθήκη</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, προστίθεται ένα κλειδί μητρώου στη λίστα πόρων.

Παράθυρο Προσθήκη / Επεξεργασία πρόστυχης λέξης

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Μάσκα πρόστυχης λέξης</u> ?

Λέξη ή μάσκα λέξης, η οποία θεωρείται ως ένδειξη spam όταν εντοπίζεται σε ένα μήνυμα.

Μια αριθμητική τιμή που υποδεικνύει την πιθανότητα ένα μήνυμα που περιέχει μια άσεμνη λέξη να είναι spam. Όσο μεγαλύτερος είναι ο συντελεστής στάθμισης, τόσο υψηλότερη η πιθανότητα να είναι spam το μήνυμα που περιέχει μια άσεμνη λέξη.

Το Πρόγραμμα Anti-Spam κατατάσσει ένα μήνυμα ως ανεπιθύμητη αλληλογραφία αν το άθροισμα των συντελεστών αξιολόγησης των άσεμνων λέξεων και αποκλεισμένων φράσεων που περιέχει υπερβαίνει την καθορισμένη τιμή.

<u>Κατάσταση</u> ?

Στην ενότητα **Κατάσταση**, μπορείτε να καθορίσετε εάν το Πρόγραμμα Anti-Spam θα σαρώνει τα μηνύματα για μια άσεμνη λέξη:

- Ενεργό. Το Πρόγραμμα Anti-Spam σαρώνει τα μηνύματα για να ελέγξει αν περιλαμβάνουν μια άσεμνη λέξη.
- Ανενεργό. Το Πρόγραμμα Anti-Spam δεν σαρώνει τα μηνύματα για να ελέγξει αν περιλαμβάνουν μια άσεμνη λέξη.

Παράθυρο Προσθήκη / Επεξεργασία αρχείου ή φακέλου

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Όνομα</u> ?

Σε αυτό το πεδίο μπορείτε να καθορίσετε το όνομα ενός πόρου με το αρχείο ή τον φάκελο, τα οποία πρέπει να διαχειρίζεται ο Έλεγχος εφαρμογών όσον αφορά την πρόσβαση.

<u>Διαδρομή</u> 🕐

Σε αυτό το πεδίο μπορεί να καθορίσετε χειροκίνητα τη διαδρομή προς ένα αρχείο ή φάκελο.

Όταν εισάγετε τη διαδρομή χειροκίνητα, μπορείτε να χρησιμοποιείτε μια μάσκα.

Η μάσκα * σας επιτρέπει να καθορίσετε ότι επιθυμείτε να ελέγχετε την πρόσβαση σε όλα τα αρχεία ή τους υποφακέλους στον επιλεγμένο φάκελο.

Η μάσκα *<extension> σας επιτρέπει να καθορίσετε ότι επιθυμείτε να ελέγχετε την πρόσβαση σε όλα τα αρχεία με την καθορισμένη επέκταση στον επιλεγμένο φάκελο.

Μπορείτε επίσης να ελέγξετε την πρόσβαση των εφαρμογών σε πόρους αρχείων που βρίσκονται σε έναν απομακρυσμένο υπολογιστή. Για να το κάνετε αυτό, καθορίστε τη διαδρομή προς τον πόρο δικτύου σε μορφή UNC σύμφωνα με τον κανόνα \\Server\Share\Relative path, όπου:

- Server είναι το όνομα τομέα του υπολογιστή ή της διεύθυνσης IP σε μορφή IPv4 ή IPv6 (απαιτείται).
- Share είναι το όνομα δικτύου του κοινόχρηστου φακέλου (απαιτείται).
- Relative path είναι η διαδρομή προς τον φάκελο ή το αρχείο από τον κοινόχρηστο φάκελο (προαιρετικό).

Παραδείγματα διαδρομών:

- \\Server1\ShareFolder1\test\example.exe
- \\Server1\ShareFolder1\test*.docx
- \\Server1\ShareFolder1*

Η εφαρμογή δεν ελέγχει την πρόσβαση στον πόρο του αρχείου εάν η διαδρομή που ορίζεται στον κανόνα διαφέρει από τη ζητούμενη διαδρομή.

<u>Επιλογή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο στο οποίο μπορείτε να επιλέξετε ένα αρχείο ή έναν φάκελο.

<u>Προσθήκη</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, προστίθεται ένα αρχείο ή ένας φάκελος στη λίστα πόρων.

Παράθυρο "Η ενεργοποίηση ολοκληρώθηκε"

Ανάπτυξη όλων | Σύμπτυξη όλων

Αυτό το παράθυρο ανοίγει εάν η εφαρμογή ενεργοποιήθηκε με επιτυχία.

<u>Ολοκληρώθηκε</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ολοκληρώνεται η διαδικασία ενεργοποίησης της εφαρμογής και ανοίγει το παράθυρο εκχώρησης άδειας χρήσης.

Παράθυρο Εφαρμογές που αποκλείονται και επιτρέπονται

Ανάπτυξη όλων | Σύμπτυξη όλων

Το παράθυρο αυτό εμφανίζει μια λίστα εφαρμογών που επιτρέπεται ή δεν επιτρέπεται να αλλάξουν τις ρυθμίσεις του λειτουργικού συστήματος. Μια κενή λίστα σημαίνει ότι δεν έχετε επιτρέψει ή αποκλείσει ακόμη καμία εφαρμογή από το να τροποποιεί τις ρυθμίσεις του λειτουργικού συστήματος.

<u>Λίστα εφαρμογών </u>

Η λίστα εφαρμογών περιέχει τα παρακάτω δεδομένα:

- **Εφαρμογή**. Αυτή η στήλη εμφανίζει το όνομα της εφαρμογής.
- Όνομα αρχείου. Αυτή η στήλη εμφανίζει το όνομα του εκτελέσιμου αρχείου μιας εφαρμογής.
- Διαδρομή. Αυτή η στήλη εμφανίζει τη διαδρομή προς το εκτελέσιμο αρχείο μιας εφαρμογής στη μονάδα σκληρού δίσκου του υπολογιστή σας.
- Πωλητής. Αυτή η στήλη εμφανίζει την ψηφιακή υπογραφή του εκδότη της εφαρμογής.
- Αλλαγές. Αυτή η στήλη εμφανίζει αν μια εφαρμογή έχει αποκλειστεί από το να ή επιτρέπεται να τροποποιεί ρυθμίσεις του λειτουργικού συστήματος, ρυθμίσεις του προγράμματος περιήγησης και ρυθμίσεις δικτύου.

Παράθυρο Ιδιωτική προστασία

Σε αυτό το παράθυρο, μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε τα ακόλουθα στοιχεία:

<u>Προστασία της Webcam</u>

<u>Ιδιωτική περιήγηση</u>

Ενημέρωση λογισμικού. Εξαιρέσεις

<u>Εξαιρέσεις</u> ?

Οι ενημερώσεις των εγκατεστημένων που εφαρμογών που παραλείφθηκαν τοποθετούνται στη λίστα **Εξαιρέσεις**. Μπορείτε να παραλείψετε μεμονωμένες ενημερώσεις, καθώς και ενημερώσεις μιας συγκεκριμένης εφαρμογής οι οποίες είναι εγκατεστημένες στον υπολογιστή σας.

Η λίστα Εξαιρέσεις αποτελείται από τις ακόλουθες στήλες:

- **Εφαρμογή** αυτή η στήλη εμφανίζει το όνομα της εφαρμογής.
- Παράλειψη αυτή η στήλη ενδέχεται να περιλαμβάνει τις ακόλουθες τιμές:
 - Έκδοση ενημέρωσης εμφανίζεται εάν παραλείψατε την μεμονωμένη ενημέρωση μιας εγκατεστημένης εφαρμογής.
 - Όλες οι ενημερώσεις εμφανίζεται εάν αποφασίσατε να μην ενημερώσετε την εφαρμογή.

<u>Κατάργηση από τη λίστα</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, οι επιλεγμένες εφαρμογές καταργούνται από τη λίστα εξαιρέσεων. Αυτό το κουμπί είναι διαθέσιμο εάν η εφαρμογή επιλεγεί στη λίστα.

Το Kaspersky Total Security θα σας ειδοποιήσει για τη διαθεσιμότητα των ενημερώσεων για εφαρμογές που έχουν καταργηθεί από τη λίστα.

Παράθυρο εξαιρέσεων ιδιωτικής περιήγησης

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Λίστα εξαιρέσεων </u>?

Η λίστα αυτή περιλαμβάνει τις διευθύνσεις των δικτυακών τόπων στους οποίους επιτρέπεται η παρακολούθηση της online δραστηριότητάς σας. Σε αυτούς τους δικτυακούς τόπους, το στοιχείο Ιδιωτική περιήγηση εντοπίζει τις προσπάθειες συλλογής δεδομένων, αλλά δεν τις εμποδίζει ακόμη και αν το στοιχείο έχει ρυθμιστεί έτσι ώστε να αποκλείει τη συλλογή δεδομένων από αυτές τις κατηγορίες υπηρεσιών παρακολούθησης.

Μπορείτε να προσθέσετε μια διεύθυνση web ή μάσκα διεύθυνσης στη λίστα.

<u>Επεξεργασία </u>

Αυτό ανοίγει ένα παράθυρο, στο οποίο μπορείτε να αλλάξετε την επιλεγμένη διεύθυνση web / μάσκα διεύθυνσης web.

<u>Διαγραφή</u> 🕐

Καταργεί από τη λίστα την επιλεγμένη διεύθυνση web/μάσκα διεύθυνσης.

<u>Προσθήκη</u> 🕐

Αυτό ανοίγει ένα παράθυρο, στο οποίο μπορείτε να προσθέσετε μια διεύθυνση web / μάσκα διεύθυνσης web.

Παράθυρο χρήσης εφαρμογών

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Εφαρμογή</u> 🕐

Η στήλη εμφανίζει εφαρμογές και ομάδες εφαρμογών τη χρήση των οποίων μπορείτε να περιορίσετε.

<u>Χρήση</u> ?

Η στήλη αυτή εμφανίζει εάν ο χρήστης επιτρέπεται ή όχι να χρησιμοποιεί μια εφαρμογή ή ομάδα εφαρμογών:

- Επιτράπηκε(-αν) ο χρήστης μπορεί να χρησιμοποιήσει αυτήν την εφαρμογή ή ομάδα εφαρμογών.
- Αποκλείστηκε(-αν) ο χρήστης δεν επιτρέπεται να χρησιμοποιήσει αυτήν την εφαρμογή ή ομάδα εφαρμογών.
- Περιορισμένη ο χρήστης μπορεί να χρησιμοποιήσει αυτήν την εφαρμογή ή ομάδα εφαρμογών για μια περιορισμένη χρονική περίοδο.

Μπορείτε να επιτρέψετε, αποκλείσετε ή να περιορίσετε τη χρήση μιας εφαρμογής ή ομάδας εφαρμογών για τον επιλεγμένο χρήστη επιλέγοντας το απαιτούμενο στοιχείο από την αναπτυσσόμενη λίστα.

<u>Διαδρομή</u> 🕐

Αυτή η στήλη εμφανίζει την διαδρομή προς το εκτελέσιμο αρχείο της εφαρμογής.

<u>Κανόνες</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο από το οποίο μπορείτε να περιορίσετε το χρόνο χρήσης της επιλεγμένης εφαρμογής.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, διαγράφεται η επιλεγμένη εφαρμογή από τη λίστα. Μετά από διαγραφή της εφαρμογής από τη λίστα, το Kaspersky Total Security σταματά να παρακολουθεί τη χρήση της εφαρμογής και ο χρήστης μπορεί να χρησιμοποιεί τη συγκεκριμένη εφαρμογή χωρίς περιορισμούς.

<u>Προσθήκη εφαρμογής</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα πλαίσιο διαλόγου στο οποίο μπορείτε να επιλέξετε το εκτελέσιμο αρχείο μιας εφαρμογής που επιθυμείτε να προσθέσετε στη λίστα. Ο Γονικός έλεγχος προσθέτει την εφαρμογή στην αντίστοιχη κατηγορία της λίστας.

Παράθυρο Καραντίνα

Ανάπτυξη όλων | Σύμπτυξη όλων

Αντικείμενα στη λίστα Καραντίνας 🖓

Περιέχει μια λίστα αρχείων που έχουν μετακινηθεί στην Καραντίνα. Η Καραντίνα έχει σχεδιαστεί για την αποθήκευση αντιγράφων ασφαλείας των αρχείων που έχουν διαγραφεί ή τροποποιηθεί κατά τη διεργασία απολύμανσης.

<u>Αρχείο ?</u>

Αυτή η στήλη εμφανίζει το όνομα ενός αρχείου σε καραντίνα.

Κάνοντας δεξί κλικ, ανοίγει ένα μενού περιβάλλοντος από το οποίο μπορείτε να εκτελέσετε τις ενέργειες που είναι διαθέσιμες για τα αρχεία σε καραντίνα: επαναφορά, κατάργηση ή άνοιγμα στον αρχικό φάκελο.

<u>Διαδρομή</u> 🕐

Αυτή η στήλη εμφανίζει τη διαδρομή προς ένα αρχείο.

<u>Εντοπίστηκε</u> ?

Αυτή η στήλη εμφανίζει τον τύπο ενός αντικειμένου που εντοπίστηκε, για παράδειγμα *Επίθεση δικτύου*.

<u>Ημερομηνία και ώρα</u> 🕐

Αυτή η στήλη εμφανίζει την ημερομηνία και ώρα μετακίνησης του αρχείου στην Καραντίνα.

<u>Επαναφορά</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security επαναφέρει το αρχείο που επιλέγεται από τη λίστα, στον φάκελο στον οποίο ήταν αποθηκευμένο πριν μετακινηθεί στην Καραντίνα.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security διαγράφει το αρχείο που έχει επιλεγεί στη λίστα.

<u>Κατάργηση όλων </u>

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security διαγράφει όλα τα αντίγραφα ασφαλείας των αρχείων που έχουν μεταφερθεί στην Καραντίνα.

To Kaspersky Total Security δεν απολυμαίνει τις εφαρμογές του Windows Store. Αν τα αποτελέσματα του ελέγχου υποδείξουν ότι μια από αυτές τις εφαρμογές είναι επικίνδυνη, θα διαγραφεί από τον υπολογιστή σας. Όταν γίνεται διαγραφή μιας εφαρμογής του Windows Store, το Kaspersky Total Security δεν δημιουργεί αντίγραφο ασφαλείας της. Για να επαναφέρετε αντικείμενα αυτού του τύπου, θα πρέπει να χρησιμοποιήσετε τα εργαλεία ανάκτησης που περιλαμβάνει το λειτουργικό σας σύστημα (για λεπτομέρειες, δείτε την τεκμηρίωση που συνοδεύει το λειτουργικό σύστημα που έχει εγκατασταθεί στον υπολογιστή σας) ή να κάνετε ενημέρωση εφαρμογών μέσω του Windows Store.

Παράθυρο Άσεμνη γλώσσα

Ανάπτυξη όλων | Σύμπτυξη όλων

Αυτό το παράθυρο εμφανίζει μια λίστα άσεμνων λέξεων. Εάν οποιαδήποτε από αυτές τις λέξεις υπάρχει σε κάποιο μήνυμα, το Kaspersky Total Security επισημαίνει το μήνυμα ως spam.

Κουμπί 🛛 🗗

Κάνοντας κλικ στο κουμπί, ανοίγει ένα μενού όπου μπορείτε να επιλέξετε μία από τις παρακάτω ενέργειες:

- Εισαγωγή και προσθήκη στα υπάρχοντα. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εισαγωγής μιας λίστας άσεμνων φράσεων από ένα αρχείο CSV. Οι τρέχουσες φράσεις δεν διαγράφονται.
- Εισαγωγή και αντικατάσταση υπαρχόντων. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εισαγωγής μιας λίστας άσεμνων φράσεων από ένα αρχείο CSV. Οι τρέχουσες φράσεις διαγράφονται.
- Εξαγωγή. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εξαγωγής μιας λίστας άσεμνων φράσεων σε ένα αρχείο CSV.

<u>Άσεμνη γλώσσα</u> ?

Αυτή η στήλη δείχνει τη λέξη ή φράση. Η παρουσία αυτής της λέξης ή φράσης μπορεί να σημαίνει ότι το μήνυμα είναι spam. Αυτή η στήλη εμφανίζει τον συντελεστή αξιολόγησης που εκχωρείται σε μία άσεμνη λέξη. Αν ένα μήνυμα περιέχει αρκετές άσεμνες λέξεις με τον συνολικό συντελεστή αξιολόγησης να υπερβαίνει το 100, το μήνυμα σημαίνεται ως spam.

<u>Κατάσταση</u> 🕐

Η στήλη αυτή υποδεικνύει εάν το Πρόγραμμα Anti-Spam χρησιμοποιεί τη συγκεκριμένη λέξη κατά τη σάρωση μηνυμάτων για άσεμνη γλώσσα.

- **Ενεργό**. Η εφαρμογή ελέγχει τα μηνύματα για αυτήν τη λέξη.
- **Ανενεργό**. Η εφαρμογή δεν ελέγχει τα μηνύματα για αυτήν τη λέξη.

<u>Επεξεργασία </u>

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο στο οποίο μπορείτε να αλλάξετε την άσεμνη λέξη ή μάσκα λέξης που είναι επιλεγμένη στη λίστα.

<u>Διαγραφή</u> ?

Κάνοντας κλικ σε αυτό το κουμπί μπορείτε να διαγράψετε την άσεμνη λέξη.

<u>Προσθήκη</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο, στο οποίο μπορείτε να προσθέσετε μια άσεμνη λέξη ή μάσκα λέξης στη λίστα.

Παράθυρο Νέα

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Λίστα νέων</u> 🕐

Τα νέα εμφανίζονται με τη μορφή λίστας στο παράθυρο. Για κάθε στοιχείο νέων, υποδεικνύεται ο τίτλος του, η ανακοίνωση και η ώρα δημοσίευσης.

Αν κάνετε κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο με το κείμενο των νέων.

Παράθυρο Νέα

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Σύνδεσμοι προς το Twitter και άλλα κοινωνικά δίκτυα 😨</u>

Κάνοντας κλικ στους συνδέσμους, ανοίγουν οι σελίδες σας στο Twitter ή άλλα κοινωνικά δίκτυα για την ανάρτηση νέων. Μπορείτε να επεξεργαστείτε το κείμενο που θα αναρτηθεί.

Εάν δεν έχετε συνδεθεί, εμφανίζεται η σελίδα σύνδεσης του αντίστοιχου δικτυακού τόπου του κοινωνικού δικτύου.

Οι σύνδεσμοι προς τα κοινωνικά δίκτυα εμφανίζονται εάν σας επιτρέπεται να επισκεφθείτε αυτούς τους δικτυακούς τόπους.

<u>Κουμπιά</u> ? < >

Κουμπιά που μπορείτε να χρησιμοποιείτε για εναλλαγή μεταξύ στοιχείων νέων.

Παράθυρο Ρυθμίσεις της Διαχείρισης εφαρμογών

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

<u>Ενεργοποίηση / απενεργοποίηση της Διαχείρισης εφαρμογών 💿</u>

Ενεργοποίηση της Διαχείριση εφαρμογών. Εάν ο διακόπτης εναλλαγής είναι ρυθμισμένος στη θέση ενεργοποίησης, το Kaspersky Total Security ελέγχει την εγκατάσταση και την κατάργηση των πρόσθετων εφαρμογών, καθώς και την εμφάνιση των βημάτων εγκατάστασης που περιέχουν διαφημίσεις.

<u>Κατά την εγκατάσταση εφαρμογών, αυτόματη εκκαθάριση πλαισίων ελέγχου για την</u> εγκατάσταση πρόσθετου λογισμικού. Προειδοποίηση για τυχόν προσπάθειες εγκατάστασης πρόσθετων προγραμμάτων 💿

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, κατά την εγκατάσταση των εφαρμογών στον υπολογιστή σας το Kaspersky Total Security αποκλείει την εγκατάσταση πρόσθετων προγραμμάτων.

Εάν το πλαίσιο ελέγχου αποεπιλέχθηκε αφότου ξεκινήσατε με την εγκατάσταση μιας συγκεκριμένης εφαρμογής, ο βοηθός εγκατάστασης συνεχίζει να εκτελείται για τη διάρκεια της τρέχουσας εγκατάστασης. Τα πλαίσια ελέγχου απέναντι από εφαρμογές που προσφέρουν πρόσθετη εγκατάσταση αποεπιλέγονται και οι πρόσθετες εφαρμογές δεν εγκαθίστανται. Αυτή η λειτουργία θα απενεργοποιηθεί κατά την επόμενη εγκατάσταση. Οι πρόσθετες εφαρμογές θα εγκατασταθούν μαζί με την κύρια εφαρμογή.

Η λειτουργία Βοηθός εγκατάστασης είναι περιορισμένη στα Microsoft Windows XP (x64). Η λειτουργία Βοηθός εγκατάστασης ενδεχομένως να μην είναι διαθέσιμη για ορισμένα προγράμματα εγκατάστασης.

<u>Να μην εμφανίζονται βήματα εγκατάστασης που ενδεχομένως να περιέχουν διαφημίσεις και</u> προσφορές για την εγκατάσταση πρόσθετων προγραμμάτων 🛙

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, κατά την εγκατάσταση των εφαρμογών στον υπολογιστή σας το Kaspersky Total Security αποκλείει την εμφάνιση διαφημίσεων ή προσφορών για την εγκατάσταση πρόσθετων προγραμμάτων.

Ανάλυση εγκατεστημένων εφαρμογών και επεκτάσεων του προγράμματος περιήγησης 💽

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security θα αναλύσει τακτικά τις επεκτάσεις σε εγκατεστημένες εφαρμογές και προγράμματα περιήγησης για να βρει αιτίες για την κατάργησή τους.

Επιλογή κατηγοριών για αντικείμενα 🖓

Κάνοντας κλικ, ανοίγει ένα παράθυρο όπου μπορείτε να επιλέξετε τις κατηγορίες επεκτάσεων σε εγκατεστημένες εφαρμογές και προγράμματα περιήγησης που το Kaspersky Total Security θα αναλύσει για να βρει πιθανές αιτίες για την κατάργησή τους.

<u>Ρύθμιση παραμέτρων χρονοδιαγράμματος </u>?

Κάνοντας κλικ στη σύνδεση, ανοίγει ένα παράθυρο όπου μπορείτε να καθορίσετε ποιες ημέρες και ποια ώρα το Kaspersky Total Security θα εκτελεί ανάλυση των επεκτάσεων σε εγκατεστημένες εφαρμογές και προγράμματα περιήγησης.

<u>Εξαιρέσεις</u> ?
Κάνοντας κλικ σε αυτήν τη σύνδεση, ανοίγει το παράθυρο **Εξαιρέσεις**. Το παράθυρο δείχνει τις εφαρμογές που έχετε προσθέσει στη λίστα εξαιρέσεων κάνοντας κλικ στο κουμπί **Παράβλεψη** στη λίστα των εφαρμογών που εντοπίστηκαν από το στοιχείο Εκκαθάριση λογισμικού υπολογιστή.

Παράθυρο Ρυθμίσεις της Ενημέρωσης λογισμικού

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Ενεργοποίηση αναζήτησης για ενημερώσεις της εφαρμογής 🕑</u>

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security πραγματοποιεί αναζήτηση για ενημερώσεις εγκατεστημένων εφαρμογών και σας προτρέπει να τις καταφορτώσετε και να τις εγκαταστήσετε.

<u>Ρύθμιση λειτουργίας αναζήτησης για ενημερώσεις </u>?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο στο οποίο μπορείτε να ορίσετε τη λειτουργία για αυτόματη αναζήτηση ενημερώσεων για τις εφαρμογές που είναι εγκατεστημένες στον υπολογιστή σας.

<u>Αυτόματη λήψη και εγκατάσταση των ενημερώσεων εάν δεν χρειάζεται να αποδεχτείτε τις</u> <u>νέες άδειες χρήσης</u>

Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security πραγματοποιεί αυτόματα αναζήτηση για ενημερώσεις εγκατεστημένων εφαρμογών και εγκαθιστά τις διαθέσιμες ενημερώσεις εφόσον δεν απαιτείται η συγκατάθεσή σας για νέες άδειες χρήσης τελικού χρήστη.

<u>Αναζήτηση για ενημερώσεις της εφαρμογής 🖻</u>

Σε αυτήν τη ρύθμιση πρέπει να επιλέξετε ποιες ενημερώσεις εφαρμογών να καταφορτώσει και να εγκαταστήσει το Kaspersky Total Security:

 Σημαντικές ενημερώσεις που βελτιώνουν την ασφάλεια του υπολογιστή – το Kaspersky Total Security εγκαθιστά μόνο τις σημαντικές ενημερώσεις που διορθώνουν τα τρωτά σημεία λογισμικού του υπολογιστή και που βελτιώνουν την ασφάλεια του υπολογιστή σας. Όλες οι ενημερώσεις για γνωστές εφαρμογές – το Kaspersky Total Security εγκαθιστά όλες τις ενημερώσεις εφαρμογών.

<u>Εξαιρέσεις</u> ?

Κάνοντας κλικ στη σύνδεση ανοίγει το παράθυρο **Εξαιρέσεις** με τη λίστα εξαιρέσεων. Οι ενημερώσεις των εγκατεστημένων που εφαρμογών που παραλείφθηκαν τοποθετούνται στη λίστα εξαιρέσεων. Μπορείτε να παραλείψετε μεμονωμένες ενημερώσεις, καθώς και ενημερώσεις μιας συγκεκριμένης εφαρμογής οι οποίες είναι εγκατεστημένες στον υπολογιστή σας.

Ενημέρωση λειτουργίας αναζήτησης/Χρονοδιαγράμματος

Ο πίνακας περιγράφει τις ρυθμίσεις που ελέγχουν το χρονοδιάγραμμα για τα στοιχεία Ενημέρωση λογισμικού και Διαχείριση εφαρμογών.

Ρυθμίσεις	Περιγραφή
Ενημέρωση λειτουργίας αναζήτησης (Ενημέρωση λογισμικού)	Αυτόματα . Το Kaspersky Total Security εκτελεί την εργασία μία φορά κάθε 24 ώρες σύμφωνα με τις εσωτερικές ρυθμίσεις.
	Κάθε λεπτό/Κάθε ώρα/Κάθε ημέρα/Εβδομαδιαία / Κάθε μήνα/Σε καθορισμένη ώρα. Το Kaspersky Total Security εκτελεί
Εκτέλεση ανάλυσης	το οποίο μπορεί να καθοριστεί έως το ακριβές λεπτό. Όταν έχει
(Διαχείριση εφαρμογών)	ενεργοποιηθεί μία από αυτές τις επιλογές, είναι διαθέσιμο το πλαίσιο ελέγχου Αναβολή εκτέλεσης μετά την εκκίνηση της εφαρμογής για Ν λεπτά .
	Μετά την εκκίνηση της εφαρμογής . Μετά την εκκίνηση του Kaspersky Total Security, εκτελεί την εργασία μετά από αναμονή για τον αριθμό των λεπτών που υποδεικνύονται στο πεδίο Έναρξη σε Ν λεπτά .
	Έπειτα από κάθε ενημέρωση . Το Kaspersky Total Security εκτελεί την εργασία μετά τη λήψη και την εγκατάσταση ενός νέου πακέτου ενημέρωσης.
Αναζήτηση για ενημερώσεις την επόμενη ημέρα εάν ο υπολογιστής	Σε περίπτωση που μια προγραμματισμένη αναζήτηση για ενημερώσεις της εφαρμογής ή ανάλυση αντικειμένου παραλείφθηκε επειδή ο υπολογιστής ήταν απενεργοποιημένος,

είναι το Kaspersky Total Security εκτελεί την εργασία μετά την ενεργοποίηση του υπολογιστή. απενεργοποιημένος (Ενημέρωση Αυτό το πλαίσιο ελέγχου εμφανίζεται εάν έχει επιλεγεί μία από λογισμικού) τις ακόλουθες λειτουργίες εκτέλεσης: Καθημερινά/ Εβδομαδιαία/Μηνιαία/Σε καθορισμένη ώρα. Εκτέλεση ανάλυσης αντικειμένων την επόμενη ημέρα εάν ο υπολογιστής είναι απενεργοποιημένος (Διαχείριση εφαρμογών) Αναζήτηση για Το Kaspersky Total Security εκτελεί την εργασία όταν ολοκληρώσετε τις εργασίες σας με τον υπολογιστή. Αυτό ενημερώσεις εφαρμογών μόνο σημαίνει ότι η εργασία δεν θα χρησιμοποιεί τους πόρους του όταν η προστασία συστήματος ενώ εργάζεστε. οθόνης είναι ενεργή ή όταν ο Αυτό το πλαίσιο ελέγχου εμφανίζεται εάν είναι επιλεγμένη η λειτουργία εκτέλεσης Έπειτα από κάθε ενημέρωση. υπολογιστής είναι κλειδωμένος (Ενημέρωση λογισμικού) Εκτέλεση ανάλυσης αντικειμένων μόνο όταν η προστασία οθόνης είναι ενεργή ή όταν ο υπολογιστής είναι κλειδωμένος (Διαχείριση εφαρμογών)

Ρυθμίσεις ενημέρωσης

Ρυθμίσεις

Χρονοδιάγραμμα ενημέρωσης βάσεων δεδομένων	Κάνοντας κλικ σε αυτήν τη σύνδεση ανοίγει το παράθυρο Χρονοδιάγραμμα ενημέρωσης βάσεων δεδομένων στο οποίο μπορείτε να επιλέξετε μία από τις λειτουργίες εκτέλεσης της ενημέρωσης βάσης δεδομένων:

Περιγραφή

	Αυτόματα . Λειτουργία εκτέλεσης της εργασίας ενημέρωσης, με βάση την οποία το Kaspersky Total Security σαρώνει το πακέτο ενημέρωσης στην πηγή ενημέρωσης με συγκεκριμένη συχνότητα. Η συχνότητα σάρωσης μπορεί να αυξηθεί κατά τη διάρκεια επιδημικών εκρήξεων ιών και να ελαττωθεί όταν δεν υπάρχουν νέοι ιοί. Μετά τον εντοπισμό ενός νέου πακέτου ενημέρωσης, το Kaspersky Total Security πραγματοποιεί λήψη του πακέτου και το εγκαθιστά τις ενημερώσεις στον υπολογιστή σας.
	Χειροκίνητα . Αυτή η λειτουργία εκτέλεσης εργασιών σάς επιτρέπει να εκτελείτε την εργασία ενημέρωσης χειροκίνητα.
	Κάθε λεπτό/Κάθε ώρα/Κάθε ημέρα/Εβδομαδιαία/Κάθε μήνα / Σε καθορισμένη ώρα/Μετά την εκκίνηση της εφαρμογής . Λειτουργία εκτέλεσης εργασίας ενημέρωσης κατά την οποία το Kaspersky Total Security εκτελεί την εργασία ενημέρωσης σύμφωνα με το χρονοδιάγραμμα που έχετε δημιουργήσει. Εάν επιλέξετε αυτήν τη λειτουργία εκτέλεσης εργασιών ενημέρωσης, μπορείτε επίσης να εκτελέσετε χειροκίνητα την εργασία ενημέρωσης του Kaspersky Total Security.
Επιλέξτε πηγές ενημερώσεων	Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο με τη λίστα των πηγών ενημέρωσης.
	<i>Μια πηγή ενημέρωσης</i> είναι ένας δημόσιος διακομιστής HTTP ή FTP ή ένας κοινόχρηστος φάκελος (τοπικός ή δίκτυο) από τον οποίο η εφαρμογή μπορεί να πραγματοποιήσει λήψη των βάσεων δεδομένων και των λειτουργικών μονάδων ενημέρωσης.
	Από προεπιλογή, η λίστα των πηγών ενημέρωσης περιέχει διακομιστές ενημέρωσης της Kaspersky. Μπορείτε να προσθέσετε άλλες πηγές ενημέρωσης στη λίστα.
	Εάν έχουν επιλεγεί πολλές πηγές ενημέρωσης από τη λίστα, το Kaspersky Total Security θα τους υποβάλει ερωτήματα διαδοχικά έως ότου φτάσει στην πρώτη διαθέσιμη πηγή ενημέρωσης από την οποία θα είναι σε θέση να πραγματοποιήσει λήψη του πακέτου ενημέρωσης.
Εκτέλεση ενημερώσεων της βάσης δεδομένων ως	Κάνοντας κλικ στη σύνδεση ανοίγει ένα παράθυρο στο οποίο μπορείτε να επιλέξετε να εκτελέσετε την ενημέρωση της βάσης δεδομένων με δικαιώματα ενός συγκεκριμένου χρήστη.

Από προεπιλογή, η εργασία ενημέρωσης του Kaspersky Total Security εκτελείται στο όνομα του χρήστη με τα δικαιώματα του οποίου είστε εγγεγραμμένοι στο λειτουργικό σύστημα. Ωστόσο, το Kaspersky Total Security μπορεί να ενημερωθεί από μια πηγή ενημέρωσης στην οποία ο χρήστης δεν έχει δικαιώματα πρόσβασης (για παράδειγμα, από έναν κοινόχρηστο φάκελο που περιέχει το πακέτο ενημέρωσης) ή για την οποία δεν έχει γίνει ρύθμιση παραμέτρων του ελέγχου ταυτότητας στον διακομιστή μεσολάβησης. Μπορείτε να καθορίσετε έναν χρήστη που διαθέτει τα απαιτούμενα δικαιώματα στις ρυθμίσεις του Kaspersky Total Security και να εκτελέσετε την εργασία ενημέρωσης του Kaspersky Total Security εκ μέρους του συγκεκριμένου χρήστη.

Παράθυρο Σάρωση για τρωτά σημεία

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Έναρξη σάρωσης</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, εκκινείται μια σάρωση για τρωτά σημεία.

<u>Διακοπή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, η σάρωση για τρωτά σημεία σταματά.

Το κουμπί είναι διαθέσιμο εάν εκτελείται σάρωση για τρωτά σημεία.

<u><N> τρωτές εφαρμογές ?</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Τρωτές εφαρμογές**, το οποίο περιέχει μια λίστα με τις τρωτές εφαρμογές που έχουν εντοπιστεί κατά τη διάρκεια της σάρωσης. Ο σύνδεσμος είναι διαθέσιμος εάν εκτελείται σάρωση για τρωτά σημεία.

Παράθυρο Παύση προστασίας

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Παύση για</u> ?

Τρόπος συνέχισης της λειτουργίας των στοιχείων προστασίας στον οποίο η προστασία ενεργοποιείται αυτόματα μετά από ένα χρονικό διάστημα που καθορίζετε εσείς.

Μπορείτε να καθορίσετε ένα χρονικό διάστημα στην αναπτυσσόμενη λίστα παρακάτω.

Παύση μέχρι επανεκκίνηση της εφαρμογής 💿

Τρόπος συνέχισης της λειτουργίας των στοιχείων προστασίας στον οποίο η προστασία ενεργοποιείται μετά από έξοδο και επανεκκίνηση της εφαρμογής ή του λειτουργικού συστήματος (εφόσον είναι ενεργοποιημένη η αυτόματη εκκίνηση της εφαρμογής).

<u>Παύση</u> ?

Τρόπος συνέχισης της λειτουργίας των στοιχείων προστασίας στον οποίο η προστασία ενεργοποιείται μόνο όταν αποφασίσετε να τη συνεχίσετε.

Παράθυρο Έλεγχος κωδικού πρόσβασης

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κωδικός πρόσβασης ?</u>

Κωδικός πρόσβασης που περιορίζει την πρόσβαση στις επιλογές διαχείρισης του Kaspersky Total Security.

Αποθήκευση κωδικού για την περίοδο λειτουργίας 🖓

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security διατηρεί στη μνήμη τον κωδικό πρόσβασης που εισάγεται και δεν εμφανίζει πλέον σχετική ερώτηση κατά τη διάρκεια της τρέχουσας περιόδου λειτουργίας.

Παράθυρο Εφαρμογές για τις οποίες η πρόσβαση στην Webcam είναι αποκλεισμένη

Ανάπτυξη όλων | Σύμπτυξη όλων

Αυτό το παράθυρο εμφανίζει τις εφαρμογές για τις οποίες έχετε αποκλείσει την Πρόσβαση στην Webcam.

<u>Να επιτραπεί η Πρόσβαση στην Webcam 😨</u>

Κάνοντας κλικ σε αυτό το κουμπί, επιτρέπετε στην εφαρμογή που είναι επιλεγμένη στη λίστα να έχει πρόσβαση στην Webcam.

Παράθυρο συνιστώμενης ρύθμισης

Ανάπτυξη όλων | Σύμπτυξη όλων

Ενεργοποίηση προστασίας από διαφημίσεις ώστε να γίνεται εγκατάσταση μόνο του επιθυμητού λογισμικού και να αποκλείονται οι πρόσθετες εγκαταστάσεις 🛙

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security αποκλείει την εμφάνιση διαφημίσεων κατά την εγκατάσταση οποιουδήποτε λογισμικού στον υπολογιστή. Αποκλείεται, επίσης, η εγκατάσταση του πρόσθετου λογισμικού που διαφημίζεται τη δεδομένη στιγμή.

<u>Ολοκληρώθηκε</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, μεταβαίνετε στο κύριο παράθυρο της εφαρμογής.

Παράθυρο Αναφορές

Μπορείτε να χρησιμοποιήσετε τις παρακάτω δυνατότητες για εύκολη διαχείριση αναφορών:

- Φιλτράρισμα ανά ημερομηνία.
- Φιλτράρισμα ανά τιμή σε οποιοδήποτε κελί.
- Αναζήτηση ανά κείμενο εγγραφής συμβάντος.
- Ταξινόμηση της λίστας ανά στήλη αναφοράς.
- Αλλαγή της σειράς και της διάταξης των στηλών που εμφανίζονται στην αναφορά.

Τα ακόλουθα επίπεδα σημασίας συμβάντος χρησιμοποιούνται στις αναφορές:

① Πληροφοριακά μηνύματα. Πληροφοριακά συμβάντα που δεν περιέχουν γενικά σημαντικές πληροφορίες.

Λ **Προειδοποιήσεις**. Συμβάντα που θα πρέπει να προσέξετε, καθώς περιέχουν πληροφορίες σχετικά με σημαντικές καταστάσεις που αντιμετωπίζει το Kaspersky Total Security κατά την εκτέλεση.

Γ Κρίσιμα συμβάντα. Συμβάντα κρίσιμης σημασίας που υποδεικνύουν ότι το Kaspersky Total Security αντιμετώπισε προβλήματα που επηρεάζουν την ικανότητά του να λειτουργεί ή τρωτά σημεία που επηρεάζουν το επίπεδο προστασίας του υπολογιστή του χρήστη.

Όταν κάνετε κλικ στο κουμπί **Αποθήκευση αναφοράς**, μπορείτε να αποθηκεύσετε την αναφορά ως αρχείο μορφής είτε ΤΧΤ είτε CSV.

Παράθυρο Ρυθμίσεις λογαριασμού χρήστη

Ανάπτυξη όλων | Σύμπτυξη όλων

Εκτέλεση ενημερώσεων της βάσης δεδομένων ως ව

Οι εργασίες ενημέρωσης για το Kaspersky Total Security εκτελούνται με τα δικαιώματα του λογαριασμού χρήστη που επιλέγετε. Η λειτουργία αυτή είναι διαθέσιμη για την εκτέλεση μιας εργασίας ενημέρωσης του Kaspersky Total Security χειροκίνητα αλλά και σύμφωνα με ένα χρονοδιάγραμμα.

Είναι διαθέσιμες οι παρακάτω επιλογές:

- Τρέχων χρήστης. Τα δικαιώματα του τρέχοντος λογαριασμού (ο λογαριασμός λειτουργικού συστήματος με τον οποίο έχετε συνδεθεί) θα εφαρμοστούν στις εργασίες ενημέρωσης.
- Άλλος χρήστης. Οι εργασίες ενημέρωσης θα εκτελούνται στον καθορισμένο λογαριασμό χρήστη. Εάν κάνετε αυτή την επιλογή, προσδιορίστε το όνομα του λογαριασμού και τον κωδικό πρόσβασης στα πεδία Λογαριασμός χρήστη και Κωδικός πρόσβασης αντίστοιχα.

Αποστολή αναφοράς

Ανάπτυξη όλων | Σύμπτυξη όλων

Αυτό το πλαίσιο ελέγχου επιτρέπει την προσθήκη πληροφοριών σχετικά με την κατάσταση του λειτουργικού συστήματος στην αναφορά που πρόκειται να αποσταλεί σε ένα διακομιστή Τεχνικής υποστήριξης.

Ληφθέντα δεδομένα για ανάλυση 💿

Επιλέγοντας αυτό το πλαίσιο ελέγχου, μπορείτε να προσθέσετε αρχεία ιχνών ? και αρχεία ένδειξης σφαλμάτων ? στην αναφορά που αποστέλλεται στο διακομιστή Τεχνικής υποστήριξης. Το ιστορικό εκτέλεσης των εντολών από την εφαρμογή και οι πληροφορίες για την κατάσταση της εφαρμογής αποθηκεύονται σε αυτά τα αρχεία.

Κάνοντας κλικ στη σύνδεση **<αριθμός αρχείων>**, **<όγκος δεδομένων>** δίπλα στο πλαίσιο ελέγχου, ανοίγει το παράθυρο **Ληφθέντα δεδομένα για ανάλυση**. Το παράθυρο εμφανίζει τη λίστα των αρχείων και τον συνολικό όγκο δεδομένων που πρόκειται να μεταφερθούν στο διακομιστή Τεχνικής υποστήριξης.

Αποθήκευση αναφοράς στον υπολογιστή σας 🖻

Κάνοντας κλικ στη σύνδεση, ανοίγει ένα πλαίσιο διαλόγου για την αποθήκευση του αρχείου.

<u>Εισαγωγή αριθμού αιτήματος 🖻</u>

Ο αριθμός που εκχωρείται στο αίτημά σας κατά την επικοινωνία με την Τεχνική υποστήριξη από την τοποθεσία web My Kaspersky.

<u>Αποστολή αναφοράς </u>

Κάνοντας κλικ σε αυτό το κουμπί, γίνεται αποστολή των επιλεγμένων αρχείων σε έναν διακομιστή FTP της Τεχνικής υποστήριξης.

Παράθυρο Ληφθέντα δεδομένα για ανάλυση

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

Μια λίστα με τα αρχεία που θα συμπεριλάβει το Kaspersky Total Security στην αναφορά που θα σταλεί στο διακομιστή της Τεχνικής υποστήριξης. Η λίστα περιλαμβάνει αρχεία ιχνών 🔋 και ένδειξης σφαλμάτων 🗿. Το ιστορικό εκτέλεσης των εντολών από την εφαρμογή και οι πληροφορίες για την κατάσταση της εφαρμογής αποθηκεύονται σε αυτά τα αρχεία.

Εάν το πλαίσιο ελέγχου στη γραμμή του αρχείου είναι επιλεγμένο, το αρχείο θα αποσταλεί στον διακομιστή της Τεχνικής υποστήριξης. Πριν από την αποστολή, τα αρχεία δεδομένων προετοιμάζονται και αρχειοθετούνται.

Εάν το πλαίσιο ελέγχου στη γραμμή του αρχείου δεν είναι επιλεγμένο, το αρχείο δεν θα αποσταλεί στον διακομιστή της Τεχνικής υποστήριξης.

<u>Αρχείο</u> ?

Αυτή η στήλη εμφανίζει το όνομα ενός αρχείου που είναι έτοιμο να σταλεί στο διακομιστή Τεχνικής υποστήριξης.

<u>Μέγεθος</u> ?

Ο όγκος των δεδομένων που θα αποσταλούν στο διακομιστή Τεχνικής υποστήριξης, εάν το καθορισμένο αρχείο περιλαμβάνεται στην αναφορά. Το Kaspersky Total Security περιλαμβάνει το αρχείο στην αναφορά εάν είναι επιλεγμένο το πλαίσιο ελέγχου στη γραμμή του αρχείου.

Εκτέλεση δέσμης ενεργειών

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κείμενο δέσμης ενεργειών για εκτέλεση 🖻</u>

Κείμενο δέσμης ενεργειών που λήφθηκε από την Τεχνική υποστήριξη.

Οι ειδικοί της Kaspersky συνιστούν να μην αλλάξετε το κείμενο της δέσμης ενεργειών.

<u>Εκτέλεση</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ξεκινά η εκτέλεση της δέσμης ενεργειών.

Εκτέλεση δεσμών ενεργειών AVZ

Αυτό το παράθυρο εμφανίζει την πρόοδο εκτέλεσης της δέσμης ενεργειών AVZ. Η εκτέλεση της δέσμης ενεργειών ενδέχεται να διαρκέσει αρκετή ώρα.

Αποτέλεσμα εκτέλεσης δέσμης ενεργειών

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Σφάλμα</u> ?

Μήνυμα σφάλματος. Εμφανίζεται σε περίπτωση εντοπισμού σφαλμάτων στη δέσμη ενεργειών AVZ. Ο Οδηγός εκτέλεσης δεσμών ενεργειών AVZ διακόπτεται.

<u>Ολοκληρώθηκε</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, κλείνει ο Οδηγός εκτέλεσης δέσμης ενεργειών AVZ.

Αποτέλεσμα εκτέλεσης δέσμης ενεργειών

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κλείσιμο</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, κλείνει ο Οδηγός εκτέλεσης δέσμης ενεργειών AVZ.

<u>Επεξεργασία</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, μπορείτε να προσθέσετε τη δέσμη ενεργειών και να επαναλάβετε την εκτέλεση της δέσμης ενεργειών.

Παράθυρο Τρωτές εφαρμογές

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Τρωτές εφαρμογές</u> ?

Εμφανίζει τα τρωτά σημεία που βρέθηκαν σε εφαρμογές.

Εξαιτίας της συμπεριφοράς ορισμένων υπηρεσιών ενημέρωσης, τα τρωτά σημεία κάποιων εφαρμογών ίσως να εντοπιστούν περισσότερες από μία φορές.

Για κάθε τρωτό σημείο υπάρχουν διαθέσιμα τα ακόλουθα κουμπιά:

• Λεπτομέρειες

Εάν κάνετε κλικ σε αυτό το κουμπί, θα μεταβείτε στον δικτυακό τόπο Τεχνικής υποστήριξης όπου θα βρείτε την περιγραφή της απειλής. Στον δικτυακό τόπο, μπορείτε να κάνετε λήψη απαιτούμενων ενημερώσεων για τη δική σας έκδοση της εφαρμογής και να τις εγκαταστήσετε.

• Προσθήκη στις εξαιρέσεις

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security μετακινεί την εφαρμογή στην αξιόπιστη ζώνη.

Επιλέξτε ένα αρχείο ΖΙΡ ή έναν φάκελο

Τα προσαρμοσμένα θέματα σχεδίασης δεν διατίθενται σε όλες τις περιοχές.

Όταν επιλέγετε ένα θέμα, λάβετε υπόψη τους παρακάτω περιορισμούς:

- Δεν θα είναι δυνατή η χρήση του επιλεγμένου θέματος από το Kaspersky Total Security στις εξής περιπτώσεις:
 - Τα αρχεία εντός της αρχειοθήκης έχουν διαφορετικό όνομα ή διαδρομή εντός της δομής του φακέλου σε σύγκριση με το προεπιλεγμένο θέμα.
 - Τα αρχειοθετημένα αρχεία, που είναι υπεύθυνα για τα κείμενα στα παράθυρα της εφαρμογής, είναι κατεστραμμένα.
- Τα θέματα είναι σχεδιασμένα για μια συγκεκριμένη έκδοση του Kaspersky Total Security και δεν υπάρχει δυνατότητα εφαρμογής τους σε άλλες εκδόσεις ή άλλες εφαρμογές. Όταν γίνεται αναβάθμιση της εφαρμογής σε μια νέα έκδοση ή εγκατάσταση άλλης εφαρμογής πάνω σε αυτήν, το θέμα αλλάζει στο προεπιλεγμένο θέμα.

Αν αντιμετωπίζετε προβλήματα κατά την επιλογή ενός εναλλακτικού θέματος και δεν μπορείτε να εγκαταστήσετε το προεπιλεγμένο θέμα μέσω της προβλεπόμενης μεθόδου (για παράδειγμα, δεν μπορείτε να καταργήσετε την επιλογή του πλαισίου ελέγχου **Χρήση προσαρμοσμένου θέματος σχεδίασης** στο παράθυρο **Ρυθμίσεις εμφάνισης του Kaspersky Total Security** επειδή γίνεται συγχώνευση της γραμματοσειράς με το παρασκήνιο και τα απαραίτητα στοιχεία διαχείρισης δεν είναι ευδιάκριτα), σας συνιστούμε να προχωρήσετε σε επανεγκατάσταση του Kaspersky Total Security.

Παράθυρο Προσθήκη / Επεξεργασία εξαίρεσης για το πληκτρολόγιο υπολογιστή

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Μάσκα διεύθυνσης web</u> ?

Η διεύθυνση web ενός δικτυακού τόπου τον οποίο θέλετε να προσθέσετε στη λίστα. Μπορείτε να ορίσετε μια διεύθυνση web ή μια μάσκα διεύθυνσης.

Στην ενότητα **Πεδίο**, μπορείτε να προσδιορίσετε την περιοχή για την οποία θα ισχύει ο κανόνας εξαίρεσης για την Καταχώρηση σε ασφαλές πληκτρολόγιο.

Εφαρμογή σε ολόκληρη την τοποθεσία web 💿

Η Καταχώρηση σε ασφαλές πληκτρολόγιο ενεργοποιείται για όλες τις σελίδες του δικτυακού τόπου που καθορίζονται στο πεδίο **Μάσκα διεύθυνσης web**.

<u>Εφαρμογή στην καθορισμένη σελίδα</u> ?

Η Καταχώρηση σε ασφαλές πληκτρολόγιο ενεργοποιείται μόνο για την ιστοσελίδα που καθορίζεται στο πεδίο **Μάσκα διεύθυνσης web**.

Στην ενότητα **Καταχώρηση σε ασφαλές πληκτρολόγιο**, μπορείτε να προσδιορίσετε κατά πόσο το Kaspersky Total Security θα προστατεύει την καταχώρηση δεδομένων από το πληκτρολόγιο υπολογιστή για τον επιλεγμένο δικτυακό τόπο ή ιστοσελίδα.

<u>Προστασία</u> ?

To Kaspersky Total Security προστατεύει την εισαγωγή δεδομένων από το πληκτρολόγιο του υπολογιστή για τον επιλεγμένο δικτυακό τόπο ή ιστοσελίδα.

To Kaspersky Total Security δεν προστατεύει τα δεδομένα που καταχωρούνται από το πληκτρολόγιο του υπολογιστή για τον επιλεγμένο δικτυακό τόπο ή ιστοσελίδα.

Παράθυρο Προσθήκη / Επεξεργασία εξαίρεσης για το Πληκτρολόγιο οθόνης

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Μάσκα διεύθυνσης web</u> ?

Η διεύθυνση web ενός δικτυακού τόπου τον οποίο θέλετε να προσθέσετε στη λίστα. Μπορείτε να ορίσετε μια διεύθυνση web ή μια μάσκα διεύθυνσης.

Στην ενότητα **Πεδίο**, μπορείτε να ορίσετε το πεδίο εφαρμογής των ρυθμίσεων εμφάνισης του εικονιδίου του Πληκτρολογίου οθόνης: ολόκληρος ο δικτυακός τόπος ή μια συγκεκριμένη σελίδα.

Εφαρμογή σε ολόκληρη την τοποθεσία web ?

Το εικονίδιο γρήγορης εκκίνησης του Πληκτρολογίου οθόνης εμφανίζεται στα πεδία εισαγωγής σε όλες τις ιστοσελίδες του δικτυακού τόπου που καθορίζεται στο πεδίο **Μάσκα διεύθυνσης web**.

<u>Εφαρμογή στην καθορισμένη σελίδα ?</u>

Το εικονίδιο γρήγορης εκκίνησης του Πληκτρολογίου οθόνης εμφανίζεται στα πεδία εισαγωγής μόνο στην ιστοσελίδα που καθορίζεται στο πεδίο **Μάσκα διεύθυνσης web**.

Στην ενότητα **Εικονίδιο για το Πληκτρολόγιο οθόνης**, μπορείτε να καθορίσετε εάν η εφαρμογή θα εμφανίζει ή όχι το εικονίδιο του Πληκτρολογίου οθόνης στις σελίδες που ταιριάζουν με την καθορισμένη μάσκα διεύθυνσης web.

<u>Εμφάνιση εικονιδίου στο παράθυρο του προγράμματος περιήγησης</u> ව

Το Kaspersky Total Security εμφανίζει το εικονίδιο γρήγορης εκκίνησης για το Πληκτρολόγιο οθόνης στα πεδία εισαγωγής.

Να μην εμφανίζεται το εικονίδιο στο παράθυρο του προγράμματος περιήγησης 🖻

Το Kaspersky Total Security δεν εμφανίζει το εικονίδιο γρήγορης εκκίνησης για το Πληκτρολόγιο οθόνης στα πεδία εισαγωγής.

Ρυθμίσεις Αναφορών και Καραντίνας

Ανάπτυξη όλων | Σύμπτυξη όλων

Στην ενότητα **Αναφορές**, μπορείτε να διαμορφώσετε τις ρυθμίσεις για τη δημιουργία και αποθήκευση αναφορών.

<u>Αποθήκευση αναφορών όχι περισσότερο από 💿</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την επιλογή που καθορίζει τον περιορισμό της διάρκειας αποθήκευσης των αναφορών. Οι αναφορές μπορούν να αποθηκεύονται για μία ημέρα, μία εβδομάδα, ένα ή έξι μήνες ή ένα έτος.

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, οι αναφορές αποθηκεύονται για το χρονικό διάστημα που επιλέγεται στην αναπτυσσόμενη λίστα δίπλα από το πλαίσιο ελέγχου. Όταν παρέλθει αυτό το χρονικό διάστημα, το Kaspersky Total Security διαγράφει την αναφορά.

Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, δεν υπάρχει περιορισμός ως προς τη διάρκεια αποθήκευσης των αναφορών.

<u>Περιορισμός του μεγέθους του αρχείου της αναφοράς σε</u> 🖻

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την επιλογή περιορισμού του μέγιστου μεγέθους των αρχείων αναφορών. Το μέγιστο μέγεθος αρχείου καθορίζεται σε megabyte.

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το προεπιλεγμένο μέγιστο μέγεθος αναφοράς είναι 1024 MB. Όταν γίνει υπέρβαση του μέγιστου μεγέθους αρχείου, οι παλιότερες αναφορές καταργούνται από το αρχείο καθώς προστίθενται νέες.

Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, δεν υπάρχει περιορισμός ως προς το μέγεθος του αρχείου αναφοράς.

<u>Εκκαθάριση</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security διαγράφει τα δεδομένα από τον φάκελο αναφορών.

Από προεπιλογή, το Kaspersky Total Security διαγράφει τις αναφορές των εργασιών σάρωσης, τις αναφορές εργασιών ενημέρωσης, τις αναφορές σχετικά με την εφαρμογή των κανόνων του Τείχους προστασίας και τις αναφορές του Γονικού ελέγχου.

Στην ενότητα **Καραντίνα**, μπορείτε να τροποποιήσετε τις ρυθμίσεις Καραντίνας.

Αποθήκευση αντικειμένων όχι περισσότερο από 💿

Το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την επιλογή για τον περιορισμό της περιόδου αποθήκευσης για τα αντικείμενα σε Καραντίνα. Οι αναφορές μπορούν να αποθηκεύονται για μία ημέρα, μία εβδομάδα, ένα ή έξι μήνες ή ένα έτος.

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, τα αντικείμενα αποθηκεύονται για το χρονικό διάστημα που επιλέγεται στην αναπτυσσόμενη λίστα δίπλα από το πλαίσιο ελέγχου.

Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, δεν υπάρχει περιορισμός ως προς τη διάρκεια αποθήκευσης των αντικειμένων.

<u>Περιορισμός του μεγέθους της Καραντίνας σε</u> ව

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την επιλογή που καθορίζει το μέγεστο μέγεθος της Καραντίνας. Το μέγεθος της Καραντίνας καθορίζεται σε megabyte.

Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, το προεπιλεγμένο μέγιστο μέγεθος του χώρου αποθήκευσης είναι 100 MB. Όταν γίνει υπέρβαση του μέγιστου μεγέθους, τα παλιότερα αντικείμενα καταργούνται από τον χώρο αποθήκευσης ενώ προστίθενται νέα αντικείμενα.

Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, δεν υπάρχει περιορισμός ως προς το μέγεθος του χώρου αποθήκευσης.

Ρυθμίσεις αυτοάμυνας

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Ενεργοποίηση αυτοάμυνας</u> 🖓

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί ένα μηχανισμό του Kaspersky Total Security που προστατεύει την εφαρμογή από την αλλαγή ή τη διαγραφή των αρχείων του από τον σκληρό δίσκο, τις διεργασίες της μνήμης και τις εγγραφές του μητρώου συστήματος.

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, η δυνατότητα εκτέλεσης εξωτερικού ελέγχου της υπηρεσίας του συστήματος είναι επίσης απενεργοποιημένη. Όταν ο εξωτερικός έλεγχος της υπηρεσίας του συστήματος είναι απενεργοποιημένος, το Kaspersky Total Security αποκλείει όλες τις προσπάθειες απομακρυσμένης διαχείρισης των υπηρεσιών των εφαρμογών. Αν εντοπιστεί μια απόπειρα απομακρυσμένης διαχείρισης της εφαρμογής, εμφανίζεται μια ειδοποίηση πάνω από το εικονίδιο του Kaspersky Total Security στην περιοχή ειδοποιήσεων της γραμμής εργασιών των Microsoft Windows (εφόσον δεν έχουν απενεργοποιηθεί οι ειδοποιήσεις).

Να επιτρέπεται η διαχείριση των ρυθμίσεων του Kaspersky Total Security μέσω εφαρμογών απομακρυσμένου ελέγχου ?

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, οι αξιόπιστες εφαρμογές απομακρυσμένης διαχείρισης (όπως το TeamViewer, το LogMeIn Pro και το Remotely Anywhere) μπορούν να αλλάξουν τις ρυθμίσεις του Kaspersky Total Security.

Δεν θα επιτρέπεται η αλλαγή των ρυθμίσεων του Kaspersky Total Security από μη αξιόπιστες εφαρμογές απομακρυσμένου ελέγχου, ακόμα και αν είναι επιλεγμένο το πλαίσιο ελέγχου.

Ρυθμίσεις διακομιστή μεσολάβησης

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Να μην χρησιμοποιείται διακομιστής μεσολάβησης 🖻</u>

Αυτό το κουμπί ενεργοποιεί / απενεργοποιεί τη χρήση διακομιστή μεσολάβησης για συνδέσεις στο Διαδίκτυο. Απαιτείται σύνδεση στο Διαδίκτυο για τη λειτουργία ορισμένων στοιχείων προστασίας στο Kaspersky Total Security, καθώς και για την ενημέρωση των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής.

Αυτόματος εντοπισμός των ρυθμίσεων του διακομιστή μεσολάβησης ව

Το Kaspersky Total Security εντοπίζει τις ρυθμίσεις του διακομιστή μεσολάβησης αυτόματα με χρήση του WPAD (Πρωτόκολλο αυτόματου εντοπισμού διακομιστή μεσολάβησης ιστού).

Εάν αυτό το πρωτόκολλο δεν μπορεί να καθορίσει τη διεύθυνση, το Kaspersky Total Security θα χρησιμοποιήσει τις ρυθμίσεις του διακομιστή μεσολάβησης που έχουν καθοριστεί στο πρόγραμμα περιήγησης Microsoft Edge που βασίζεται στο Chromium. Το Kaspersky Total Security δεν λαμβάνει υπόψη τις ρυθμίσεις των διακομιστών μεσολάβησης που έχουν καθοριστεί για άλλα προγράμματα περιήγησης τα οποία είναι εγκατεστημένα στον υπολογιστή του χρήστη.

Χρήση καθορισμένων ρυθμίσεων διακομιστή μεσολάβησης 🖓

Το Kaspersky Total Security χρησιμοποιεί διαφορετικό διακομιστή μεσολάβησης από αυτόν που καθορίστηκε στις ρυθμίσεις σύνδεσης του προγράμματος περιήγησης.

<u>Διεύθυνση</u> ?

Περιέχει τη διεύθυνση IP ή τη συμβολική ονομασία (διεύθυνση URL) ενός διακομιστή μεσολάβησης.

Η επεξεργασία του πεδίου είναι δυνατή εάν έχει επιλεγεί η ρύθμιση **Χρήση** καθορισμένων ρυθμίσεων διακομιστή μεσολάβησης (για παράδειγμα, IP 192.168.0.1).

<u> Θύρα</u> ?

Η θύρα του διακομιστή μεσολάβησης.

Αυτό το πεδίο είναι διαθέσιμο εάν έχει επιλεγεί η ρύθμιση **Χρήση καθορισμένων ρυθμίσεων διακομιστή μεσολάβησης**.

<u>Χρήση ελέγχου ταυτότητας διακομιστή μεσολάβησης</u> ?

Έλεγχος ταυτότητας είναι η επαλήθευση των στοιχείων σύνδεσης ενός χρήστη.

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί τη χρήση του ελέγχου ταυτότητας στο διακομιστή μεσολάβησης.

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security επιχειρεί να εκτελέσει πρώτα τον έλεγχο ταυτότητας NTLM και κατόπιν τον ΒΑΣΙΚΟ έλεγχο ταυτότητας.

Εάν αυτό το πλαίσιο ελέγχου είναι αποεπιλεγμένο ή δεν έχουν καθοριστεί οι ρυθμίσεις του διακομιστή μεσολάβησης, το Kaspersky Total Security θα επιχειρήσει να εκτελέσει τον έλεγχο ταυτότητας NTLM με χρήση του λογαριασμού από τον οποίο εκτελείται η εργασία (για παράδειγμα, μια εργασία ενημέρωσης).

Εάν ο διακομιστής μεσολάβησης απαιτεί έλεγχο ταυτότητας και δεν έχει εισαχθεί όνομα χρήστη και κωδικός πρόσβασης ή εάν τα καθορισμένα δεδομένα απορρίφθηκαν από το διακομιστή μεσολάβησης, θα εμφανιστεί ένα παράθυρο που θα ζητά το όνομα χρήστη και τον κωδικό πρόσβασης. Εάν ο έλεγχος ταυτότητας είναι επιτυχής, το Kaspersky Total Security θα χρησιμοποιεί στο μέλλον το καθορισμένο όνομα χρήστη και τον κωδικό πρόσβασης. Διαφορετικά, το Kaspersky Total Security θα σας ζητήσει ξανά να προσδιορίσετε τις ρυθμίσεις ελέγχου ταυτότητας.

<u>Όνομα χρήστη </u>

Το όνομα χρήστη που χρησιμοποιείται για τον έλεγχο ταυτότητας στο διακομιστή μεσολάβησης.

<u>Κωδικός πρόσβασης </u>

Ο κωδικός πρόσβασης για το καθορισμένο όνομα χρήστη.

<u>Παράκαμψη διακομιστή μεσολάβησης για τοπικές διευθύνσεις </u>?

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security δεν χρησιμοποιεί διακομιστή μεσολάβησης κατά την ενημέρωση των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής από έναν τοπικό φάκελο ή φάκελο δικτύου.

Εάν αυτό το πλαίσιο ελέγχου είναι αποεπιλεγμένο, το Kaspersky Total Security χρησιμοποιεί διακομιστή μεσολάβησης κατά την ενημέρωση των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής από έναν τοπικό φάκελο ή φάκελο δικτύου.

Ρυθμίσεις ειδοποιήσεων

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την εμφάνιση ειδοποιήσεων για συμβάντα.

Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security δεν σας ειδοποιεί για συμβάντα που προκύπτουν κατά τη λειτουργία του, αλλά καταγράφει πληροφορίες σχετικά με αυτά σε μια αναφορά.

Οι ειδοποιήσεις μπορούν να παρέχονται με τις ακόλουθες μεθόδους:

- Αναδυόμενα μηνύματα πάνω από το εικονίδιο του Kaspersky Total Security στην περιοχή ειδοποιήσεων της γραμμής εργασιών
- Ηχητικές ειδοποιήσεις

Επαναφορά όλων των κρυμμένων ειδοποιήσεων 💿

Κάνοντας κλικ σε αυτή τη σύνδεση σας επιτρέπει να επαναφέρετε τις προεπιλεγμένες τιμές ρύθμισης για την εμφάνιση των ειδοποιήσεων. Εάν αποκλείσατε προηγουμένως την εμφάνιση των ειδοποιήσεων, η εμφάνιση αυτών των ειδοποιήσεων θα συνεχιστεί.

Η σύνδεση αυτή δεν είναι διαθέσιμη, εάν δεν υπάρχουν κρυφές κοινοποιήσεις.

<u>Ενεργοποίηση ηχητικών ειδοποιήσεων</u> ?

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί τις ηχητικές ειδοποιήσεις.

Από προεπιλογή, οι ειδοποιήσεις για κρίσιμα συμβάντα (για παράδειγμα, κατά τον εντοπισμό κακόβουλου λογισμικού) συνοδεύονται από ηχητικό σήμα.

Για να αλλάξετε το προεπιλεγμένο ηχητικό σήμα σε "ήχο γουρουνιού", πληκτρολογήστε **ΙDKFA** στο παράθυρο **Σχετικά με**.

Τα ηχητικά σήματα ειδοποιήσεων δεν αναπαράγονται στα Microsoft Windows 10.

<u>Λήψη ενημερωτικών μηνυμάτων και διαφημίσεων από την Kaspersky</u> ව

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί τις ειδοποιήσεις για νέα που δεν έχουν αναγνωσθεί στην περιοχή ειδοποιήσεων της γραμμής εργασιών.

Εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security συνεχίζει να λαμβάνει ενημερωτικά μηνύματα και διαφημίσεις από την Kaspersky αλλά δεν εμφανίζει ειδοποιήσεις σχετικά με αυτά. Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την επιλογή που επιτρέπει την εμφάνιση ή απόκρυψη πληροφοριών σχετικά με το λογισμικό και τις ειδικές προσφορές στους δικτυακούς τόπους της Kaspersky και των συνεργαζόμενων εταιρειών της.

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, στους συγκεκριμένους δικτυακούς τόπους θα εμφανίζονται ειδικές προσφορές για τη αγορά λογισμικού, οι οποίες επιλέγονται ειδικά για εσάς με βάση τις άδειες για τις εφαρμογές της Kaspersky που έχετε ήδη αγοράσει.

Εάν αυτό το πλαίσιο ελέγχου δεν είναι επιλεγμένο, οι δικτυακοί τόποι θα εμφανίζουν τυπικές προσφορές για την αγορά εφαρμογών.

<u>Λήψη ειδικών προσφορών για χρήστες κοινωνικών δικτύων 💿</u>

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security καθορίζει εάν είστε χρήστης κοινωνικών δικτύων και εμφανίζει πληροφορίες σχετικά με τις δραστηριότητες της Kaspersky στις τροφοδοσίες ειδήσεων των κοινωνικών δικτύων.

Εάν αυτό το πλαίσιο ελέγχου είναι απενεργοποιημένο, το Kaspersky Total Security εμφανίζει ένα τυποποιημένο σύνολο ειδήσεων της Kaspersky.

<u>Λήψη ενημερωτικών μηνυμάτων και διαφημίσεων μετά τη λήξη της τρέχουσας άδειας χρήσης</u>

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, η εφαρμογή συνεχίζει να λαμβάνει και να εμφανίζει νέα προωθητικά μηνύματα και προσφορές ακόμη και μετά τη λήξη της άδειας χρήσης.

Εάν αυτό το πλαίσιο ελέγχου δεν είναι επιλεγμένο, δεν λαμβάνονται νέα προωθητικά μηνύματα και προσφορές. Η εφαρμογή εμφανίζει μηνύματα που είχαν ληφθεί πριν τη λήξη της άδειας χρήσης.

Ενότητα προστασίας

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κατάλογος στοιχείων προστασίας 🖓</u>

Η λίστα αυτή περιλαμβάνει στοιχεία προστασίας που έχουν σχεδιαστεί για την προστασία από διάφορους τύπους ψηφιακών απειλών.

Κάθε τύπος απειλής διαχειρίζεται από ένα ειδικό στοιχείο προστασίας. Τα στοιχεία μπορούν να ενεργοποιηθούν ή να απενεργοποιηθούν ανεξάρτητα το ένα από το άλλο και οι ρυθμίσεις τους μπορούν να προσαρμοστούν.

Ρυθμίσεις Προστασίας της Webcam

Ανάπτυξη όλων | Σύμπτυξη όλων

Ενεργοποίηση / απενεργοποίηση της Προστασίας της Webcam ව

Αυτό το κουμπί ενεργοποιεί / απενεργοποιεί το στοιχείο Προστασία της Webcam.

<u>Αποκλεισμός πρόσβασης στην webcam για όλες τις εφαρμογές </u>

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, αποκλείεται η πρόσβαση στην webcam για όλες τις εφαρμογές που είναι εγκατεστημένες στον υπολογιστή σας.

Εάν το πλαίσιο ελέγχου είναι αποεπιλεγμένο, το Kaspersky Total Security παρακολουθεί την πρόσβαση εφαρμογών στην webcam ανάλογα με την ομάδα αξιοπιστίας στην οποία ανήκει η κάθε εφαρμογή:

- **Αξιόπιστες** η πρόσβαση στην webcam επιτρέπεται.
- Χαμηλού περιορισμού όταν πραγματοποιείται απόπειρα πρόσβασης στην webcam, το Kaspersky Total Security εμφανίζει ένα παράθυρο που σας ζητά να επιτρέψετε σε αυτήν την εφαρμογή να αποκτήσει πρόσβαση στην webcam.
- Υψηλού περιορισμού και Μη αξιόπιστες η πρόσβαση στην webcam αποκλείεται.

<u>Εμφάνιση ειδοποίησης όταν η webcam χρησιμοποιείται από μια εφαρμογή στην οποία</u> επιτρέπεται η πρόσβαση στην webcam 🕜

Εάν αυτό πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security εμφανίζει μια ειδοποίηση όταν μια εφαρμογή για την οποία επιτρέπεται η πρόσβαση, χρησιμοποιεί την webcam. Στο παράθυρο της ειδοποίησης μπορείτε να επεξεργαστείτε τις ρυθμίσεις της πρόσβασης εφαρμογών στην webcam ή να επιλέξετε να μην εμφανίζονται πλέον σχετικές ειδοποιήσεις.

Εάν αυτό το πλαίσιο ελέγχου δεν είναι επιλεγμένο, η ειδοποίηση δεν εμφανίζεται.

Αυτό το πλαίσιο ελέγχου είναι διαθέσιμο εάν το πλαίσιο ελέγχου **Αποκλεισμός πρόσβασης στην webcam για όλες τις εφαρμογές** είναι αποεπιλεγμένο.

Εντοπισμός ύποπτης ανακατεύθυνσης

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Διαγραφή εγγραφών </u>?

Το Kaspersky Total Security διαγράφει όλες τις ύποπτες εγγραφές του αρχείου φιλοξενίας.

<u>Παράλειψη</u> 🕐

Το Kaspersky Total Security δεν διαγράφει τις ύποπτες εγγραφές, εάν παρέχονται στη λίστα, από το αρχείο φιλοξενίας.

<u>Λίστα ύποπτων αρχείων</u> 🖓

Η λίστα αυτή περιέχει τις διευθύνσεις των κακόβουλων ή άγνωστων διακομιστών web στους οποίους ανακατευθύνεστε όταν η εφαρμογή επιχειρεί να συνδεθεί στους διακομιστές της Kaspersky.

Συνιστάται να διαγράφετε τις ύποπτες εγγραφές από το αρχείο φιλοξενίας.

Παράθυρο Καταχώρηση κωδικού πρόσβασης

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

<u>Τρέχων κωδικός πρόσβασης</u> 🖓

Ο ισχύων κωδικός πρόσβασης που χρησιμοποιείται για τη διαχείριση του Kaspersky Total Security.

<u>Αποθήκευση κωδικού για την περίοδο λειτουργίας 🖓</u>

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security διατηρεί στη μνήμη τον κωδικό πρόσβασης που εισάγεται και δεν εμφανίζει πλέον σχετική ερώτηση κατά τη διάρκεια της τρέχουσας περιόδου λειτουργίας.

Το παράθυρο Προστασία με χρήση κωδικού πρόσβασης

Ανάπτυξη όλων | Σύμπτυξη όλων

Ο σύνδεσμος **Αλλαγή ή κατάργηση κωδικού πρόσβασης** είναι διαθέσιμος εάν έχει οριστεί προηγουμένως κωδικός πρόσβασης για την προστασία της πρόσβασης στις λειτουργίες του Kaspersky Total Security.

<u>Αλλαγή ή κατάργηση κωδικού πρόσβασης 🖻</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, καθίστανται διαθέσιμα πεδία εισαγωγής για τον ορισμό νέου κωδικού πρόσβασης και την επιβεβαίωσή του.

Νέος κωδικός πρόσβασης ?

Κωδικός πρόσβασης για τη διαχείριση του Kaspersky Total Security.

<u>Επιβεβαίωση κωδικού πρόσβασης</u> 🖓

Πληκτρολογήστε πάλι τον κωδικό πρόσβασης που εισαγάγατε στο πεδίο **Νέος κωδικός πρόσβασης**.

Στην ενότητα **Ισχύς κωδικού πρόσβασης**, μπορείτε να καθορίσετε ποια τμήματα της διαχείρισης της εφαρμογής θέλετε να προστατεύονται με κωδικό πρόσβασης.

<u>Διαμόρφωση ρυθμίσεων εφαρμογής 💽</u>

Το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την εμφάνιση της ειδοποίησης κωδικού πρόσβασης όταν ένας χρήστης επιχειρεί να αποθηκεύσει αλλαγές στις ρυθμίσεις της εφαρμογής.

Το πλαίσιο ελέγχου αυτό είναι επιλεγμένο και ανενεργό εάν έχει επιλεγεί το πλαίσιο ελέγχου **Διαχείριση Γονικού ελέγχου**.

<u>Διαχείριση Γονικού ελέγχου 🖓</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την εμφάνιση της ειδοποίησης κωδικού πρόσβασης όταν ένας χρήστης επιχειρεί να ανοίξει το παράθυρο του Γονικού ελέγχου.

<u>Διαχείριση δημιουργίας αντιγράφων ασφαλείας 🖻</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την επιλογή που ζητά από τον χρήστη τον κωδικό πρόσβασης για το άνοιγμα του παραθύρου **Δημιουργία αντιγράφων ασφαλείας**.

Έξοδος από την εφαρμογή ?

Το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την εμφάνιση της ειδοποίησης κωδικού πρόσβασης όταν ο χρήστης επιχειρεί να κλείσει την εφαρμογή.

Το πλαίσιο ελέγχου αυτό είναι επιλεγμένο και ανενεργό εάν έχει επιλεγεί το πλαίσιο ελέγχου **Διαχείριση Γονικού ελέγχου**.

<u>Κατάργηση της εφαρμογής</u> ?

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την εμφάνιση της ειδοποίησης κωδικού πρόσβασης όταν ένας χρήστης επιχειρεί να καταργήσει την εφαρμογή.

Το πλαίσιο ελέγχου αυτό είναι επιλεγμένο και ανενεργό εάν έχει επιλεγεί το πλαίσιο ελέγχου **Διαχείριση Γονικού ελέγχου**.

Ρυθμίσεις σάρωσης

Ο πίνακας περιγράφει τις ρυθμίσεις που ελέγχουν τους ακόλουθους τύπους σαρώσεων: Πλήρης σάρωση, Γρήγορη σάρωση, Επιλεκτική σάρωση και Σάρωση μενού περιβάλλοντος.

Ρυθμίσεις	Περιγραφή
Επίπεδο ασφαλείας	Το Kaspersky Total Security χρησιμοποιεί διάφορα σύνολα ρυθμίσεων για σάρωση. Τα σύνολα ρυθμίσεων που αποθηκεύονται στην εφαρμογή ονομάζονται <i>Επίπεδα ασφαλείας</i> :
	 Μέγιστο. Το Kaspersky Total Security σαρώνει όλους τους τύπους αρχείων. Κατά τη σάρωση σύνθετων αρχείων, το Kaspersky Total Security σαρώνει επίσης τα αρχεία με μορφή email.

 Βέλτιστο. Το Kaspersky Total Security σαρώνει μόνο καθορισμένες μορφές αρχείων σε όλους τους σκληρούς δίσκους, τις μονάδες δίσκου δικτύου, τα αφαιρούμενα μέσα αποθήκευσης του υπολογιστή και τα ενσωματωμένα αντικείμενα OLE. Το Kaspersky Total Security δεν σαρώνει αρχεία και πακέτα εγκατάστασης.
 Χαμηλό. Το Kaspersky Total Security σαρώνει μόνο νέα και τροποποιημένα αρχεία με συγκεκριμένες επεκτάσεις αρχείων σε όλους τους σκληρούς δίσκους του υπολογιστή, τις αφαιρούμενες μονάδες δίσκου και τις μονάδες δίσκου δικτύου. Το Kaspersky Total Security δεν σαρώνει σύνθετα αρχεία.
 Προτροπή χρήστη. Εάν το Kaspersky Total Security εντοπίσει ένα μολυσμένο ή πιθανώς μολυσμένο στοιχείο κατά τη διάρκεια σάρωσης, σας ενημερώνει άμεσα για το συμβάν και σας ρωτά σχετικά με την ενέργεια που θα εφαρμοστεί στο στοιχείο που εντοπίστηκε.
Αυτή η επιλογή είναι διαθέσιμη εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στην περιοχή Ρυθμίσεις → Γενικά .
 Επιλογή ενέργειας αυτόματα. Όταν εντοπίζονται μολυσμένα ή πιθανώς μολυσμένα αντικείμενα, το Kaspersky Total Security εκτελεί την ενέργεια που συνιστάται από τους ειδικούς της Kaspersky.
 Το Kaspersky Total Security προσπαθεί πρώτα να απολυμάνει ένα μολυσμένο αντικείμενο. Εάν αποτύχει η απολύμανση, διαγράφει το αρχείο.
 Το Kaspersky Total Security διαγράφει ένα πιθανώς μολυσμένο αντικείμενο, εάν είναι επιλεγμένο το πλαίσιο ελέγχου Διαγραφή κακόβουλων εργαλείων, προγραμμάτων adware, λογισμικού αυτόματων κλήσεων και ύποπτων πακέτων. Εάν το πλαίσιο ελέγχου δεν είναι επιλεγμένο, το Kaspersky Total Security δεν διαγράφει ένα πιθανώς μολυσμένο αντικείμενο. Αντ' αυτού, εμφανίζεται μια ειδοποίηση σχετικά με τον

ειδοποιήσεων (κάντε κλικ στο κουμπί **Λεπτομέρειες** στο κύριο παράθυρο της εφαρμογής για να το ανοίξετε).

Αυτή η επιλογή είναι διαθέσιμη εάν είναι επιλεγμένο το πλαίσιο ελέγχου **Αυτόματη εκτέλεση των συνιστώμενων** ενεργειών στην περιοχή **Ρυθμίσεις** → **Γενικά**.

- Απολύμανση, εάν η απολύμανση αποτύχει, τότε διαγραφή. Εάν ενεργοποιηθεί αυτή η επιλογή, το Kaspersky Total Security επιχειρεί αυτόματα να απολυμάνει όλα τα μολυσμένα αρχεία που εντοπίζονται. Εάν αποτύχει η απολύμανση, το Kaspersky Total Security διαγράφει τα αντικείμενα.
- Απολύμανση, εάν η απολύμανση αποτύχει, τότε αποκλεισμός. Εάν επιλέξετε αυτήν την ενέργεια, τότε το Kaspersky Total Security θα προσπαθήσει αυτόματα να απολυμάνει όλα τα μολυσμένα αρχεία που εντοπίζει. Εάν η απολύμανση αποτύχει, το Kaspersky Total Security θα προσθέσει πληροφορίες σχετικά με τα μολυσμένα αρχεία που εντοπίζει στη λίστα των εντοπισμένων αντικειμένων.
- Ειδοποίηση. Εάν ενεργοποιηθεί αυτή η επιλογή, το Kaspersky Total Security θα προσθέσει πληροφορίες σχετικά με τα μολυσμένα αρχεία που εντοπίζει στη λίστα των εντοπισμένων αντικειμένων.

Πριν επιχειρήσει να απολυμάνει ή να διαγράψει ένα μολυσμένο αρχείο, το Kaspersky Total Security δημιουργεί ένα αντίγραφο ασφαλείας σε περίπτωση που χρειαστεί στη συνέχεια να επαναφέρετε το αρχείο ή να είναι δυνατή η απολύμανσή του αργότερα.

Επεξεργασία εύρους σάρωσης	Κάνοντας κλικ στη σύνδεση ανοίγει ένα παράθυρο με μια λίστα αντικειμένων που μπορεί να σαρώσει το Kaspersky Total Security. Ανάλογα με τον τύπο σάρωσης (Πλήρης σάρωση, Γρήγορη σάρωση ή Επιλεκτική σάρωση), διάφορα αντικείμενα θα συμπεριλαμβάνονται από προεπιλογή στη λίστα.
	Μπορείτε να προσθέσετε αντικείμενα στη λίστα ή να διαγράψετε τα αντικείμενα που προσθέτετε.

(δεν είναι διαθέσιμη στις Ρυθμίσεις σάρωσης του μενού περιβάλλοντος)	Για να καταργήσετε ένα αντικείμενο από τη σάρωση, δεν χρειάζεται να διαγράψετε το αντικείμενο από τη λίστα. Το μόνο που χρειάζεται να κάνετε είναι να αποεπιλέξετε το πλαίσιο δίπλα στο όνομα του αντικειμένου.
Χρονοδιάγραμμα σάρωσης (δεν είναι διαθέσιμη στις Ρυθμίσεις σάρωσης του μενού περιβάλλοντος)	Χειροκίνητα . Λειτουργία εκτέλεσης στην οποία μπορείτε να ξεκινήσετε τη σάρωση χειροκίνητα κατά τη στιγμή που σας εξυπηρετεί. Βάσει προγράμματος . Λειτουργία εκτέλεσης σάρωσης κατά την οποία το Kaspersky Total Security εκτελεί την εργασία σάρωσης σύμφωνα με το χρονοδιάγραμμα που έχετε δημιουργήσει. Εάν επιλέξετε αυτήν τη λειτουργία σάρωσης, μπορείτε επίσης να εκτελέσετε την εργασία σάρωσης χειροκίνητα.
Εκτέλεση σάρωσης	Κάνοντας κλικ στη σύνδεση ανοίγει ένα παράθυρο στο οποίο μπορείτε να επιλέξετε να εκτελέσετε τη σάρωση με δικαιώματα ενός συγκεκριμένου χρήστη. Από προεπιλογή, η εργασία σάρωσης εκτελείται στο όνομα του χρήστη με τα δικαιώματα του οποίου είστε εγγεγραμμένοι στο λειτουργικό σύστημα. Το πεδίο προστασίας μπορεί να περιλαμβάνει μονάδες δίσκου δικτύου ή άλλα αντικείμενα που απαιτούν ειδικά δικαιώματα πρόσβασης. Μπορείτε να καθορίσετε έναν χρήστη που διαθέτει τα απαιτούμενα δικαιώματα στις ρυθμίσεις του Kaspersky Total Security και να εκτελέσετε την εργασία σάρωσης εκ μέρους του συγκεκριμένου χρήστη.
Τύποι αρχείου	Το Kaspersky Total Security αντιμετωπίζει τα αρχεία χωρίς επεκτάσεις ως εκτελέσιμα. Το Kaspersky Total Security τα σαρώνει πάντα, ανεξάρτητα από τους τύπους αρχείων που έχετε επιλέξει για σάρωση. Όλα τα αρχεία. Εάν είναι ενεργοποιημένη αυτή η ρύθμιση, το Kaspersky Total Security σαρώνει όλα τα αρχεία χωρίς εξαίρεση (οποιασδήποτε μορφής και με οποιαδήποτε επέκταση).

	Σάρωση αρχείων κατά μορφή. Εάν επιλέξετε αυτήν τη ρύθμιση, το Kaspersky Total Security θα σαρώνει μόνο Δυνητικά επικίνδυνα για μόλυνση αρχεία <table-cell>. Πριν από την αναζήτηση για κακόβουλο κώδικα σε ένα αρχείο, θα αναλυθεί η εσωτερική κεφαλίδα του ώστε να προσδιοριστεί η μορφή του αρχείου (για παράδειγμα, TXT, DOC, EXE). Η σάρωση αναζητά επίσης αρχεία με συγκεκριμένες επεκτάσεις αρχείων.</table-cell>
	Σάρωση αρχείων κατά επέκταση . Εάν επιλέξετε αυτήν τη ρύθμιση, το Kaspersky Total Security θα σαρώνει μόνο <u>Δυνητικά</u> επικίνδυνα για μόλυνση αρχεία 🕜. Η μορφή του αρχείου προσδιορίζεται με βάση την επέκτασή του.
Σάρωση μόνο νέων και τροποποιημένων αρχείων	Σαρώνει μόνο νέα αρχεία και εκείνα τα αρχεία που έχουν τροποποιηθεί από την τελευταία φορά που σαρώθηκαν. Αυτό θα σας επιτρέψει να εξοικονομήσετε χρόνο κατά τη σάρωση. Αυτή η λειτουργία σάρωσης ισχύει για απλά, αλλά και για σύνθετα αρχεία.
Παράλειψη αρχείων που σαρώνονται για περισσότερο από	Περιορίζει τη διάρκεια σάρωσης ενός μεμονωμένου αντικειμένου. Αφού παρέλθει το καθορισμένο χρονικό διάστημα, το Kaspersky Total Security θα σταματήσει τη σάρωση του αρχείου. Αυτό θα σας επιτρέψει να εξοικονομήσετε χρόνο κατά τη σάρωση.
Σάρωση αρχειοθηκών	Σαρώνει αρχεία με τις ακόλουθες μορφές: RAR, ARJ, ZIP, CAB, LHA, JAR και ICE.
Πακέτα διανομής σάρωσης	Το πλαίσιο ελέγχου ενεργοποιεί/απενεργοποιεί τη σάρωση πακέτων διανομής τρίτου μέρους.
Σάρωση αρχείων με μορφές Microsoft Office	Σαρώνει αρχεία του Microsoft Office (DOC, DOCX, XLS, PPT και άλλες επεκτάσεις της Microsoft). Τα αρχεία μορφής Office περιλαμβάνουν επίσης αντικείμενα OLE.
Ανάλυση μορφών email	Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί στο Kaspersky Total Security την επιλογή σάρωσης αρχείων σε μορφές email και σε βάσεις δεδομένων email.
	Η εφαρμογή σαρώνει πλήρως μόνο τις μορφές αρχείων αλληλογραφίας Microsoft Outlook, Windows Mail/Microsoft Outlook Express και EML και μόνο εάν ο υπολογιστής διαθέτει πρόγραμμα-πελάτη αλληλογραφίας Microsoft Outlook x86.
	Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security αναλύει το αρχείο μορφής email και αναλύει κάθε στοιχείο (κυρίως σώμα, συνημμένα) για ιούς.

	Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security σαρώνει το αρχείο μορφής email ως ενιαίο αντικείμενο.
Σάρωση αρχείων φύλαξης που προστατεύονται με κωδικό πρόσβασης	Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security σαρώνει αρχεία φύλαξης που προστατεύονται με κωδικό πρόσβασης. Πριν από τη σάρωση των αρχείων που περιέχονται στην αρχειοθήκη, θα εμφανιστεί στην οθόνη ένα αίτημα για κωδικό πρόσβασης.
	Εάν το πλαίσιο ελέγχου δεν είναι επιλεγμένο, το Kaspersky Total Security παραβλέπει τη σάρωση αρχείων φύλαξης που προστατεύονται με κωδικό πρόσβασης.
Να μην αποσυμπιέζονται σύνθετα αρχεία	Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, τότε το Kaspersky Total Security δεν σαρώνει σύνθετα αρχεία που είναι μεγαλύτερα από την καθορισμένη τιμή.
μεγαλου μεγέθους Μέγιστο μέγεθος αρχείου	Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security σαρώνει τα σύνθετα αρχεία οποιουδήποτε μεγέθους.
	Το Kaspersky Total Security σαρώνει μεγάλα αρχεία που εξάγονται από αρχειοθήκες ανεξάρτητα από το εάν το πλαίσιο ελέγχου είναι επιλεγμένο ή όχι.
Ευρετική ανάλυση	Μια τεχνική για τον εντοπισμό απειλών που δεν μπορούν να προσδιοριστούν χρησιμοποιώντας την τρέχουσα έκδοση των βάσεων δεδομένων της εφαρμογής Kaspersky. Σας επιτρέπει να βρείτε αρχεία που ενδέχεται να περιέχουν άγνωστο κακόβουλο λογισμικό ή μια νέα τροποποίηση γνωστού προγράμματος με κακόβουλο λογισμικό.
	Κατά τη σάρωση αρχείων για κακόβουλο κώδικα, η ευρετική ανάλυση εκτελεί οδηγίες στα εκτελέσιμα αρχεία. Ο αριθμός των οδηγιών που εκτελούνται από την ευρετική ανάλυση εξαρτώνται από το επίπεδο που καθορίζεται για την ευρετική ανάλυση. Το επίπεδο της ευρετικής ανάλυσης ορίζει την ισορροπία μεταξύ της πληρότητας αναζήτησης για νέες απειλές, το φορτίο στους πόρους του λειτουργικού συστήματος και τον χρόνο που απαιτείται για την ευρετική ανάλυση.
Τεχνολογία iSwift	Αυτή η τεχνολογία αποτελεί εξέλιξη της τεχνολογίας iChecker για υπολογιστές που χρησιμοποιούν το σύστημα αρχείων NTFS.

	Η τεχνολογία iSwift έχει περιορισμούς: δεσμεύεται σε μια συγκεκριμένη θέση αρχείου στο σύστημα αρχείων και λειτουργεί μόνο σε αντικείμενα στο σύστημα αρχείων NTFS.
Τεχνολογία iChecker	Αυτή η τεχνολογία καθιστά εφικτή την αύξηση της ταχύτητας σάρωσης, εξαιρώντας συγκεκριμένα αρχεία από τη σάρωση. Η εξαίρεση αρχείων από τη σάρωση γίνεται με βάση έναν ειδικό αλγόριθμο, ο οποίος λαμβάνει υπόψη την ημερομηνία έκδοσης των βάσεων δεδομένων του Kaspersky Total Security, την ημερομηνία της πιο πρόσφατης σάρωσης του αρχείου και τυχόν τροποποιήσεις που έχουν πραγματοποιηθεί στις ρυθμίσεις σάρωσης. Η τεχνολογία iChecker έχει περιορισμούς: δεν λειτουργεί με μεγάλα αρχεία και εφαρμόζεται μόνο στα αρχεία με δομή που αναγνωρίζει η εφαρμογή (για παράδειγμα, ΕΧΕ, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP και RAR).

Ρυθμίσεις σάρωσης αφαιρούμενων μονάδων δίσκου

Ρυθμίσεις	Περιγραφή
Ενέργεια όταν συνδέεται μια αφαιρούμενη μονάδα δίσκου	 Γρήγορη σάρωση. Εάν ενεργοποιηθεί αυτή η επιλογή, όταν συνδέεται μια εξωτερική συσκευή, το Kaspersky Total Security θα σαρώσει μόνο αρχεία με συγκεκριμένες μορφές που είναι τα πιο ευαίσθητα σε μόλυνση και βρίσκονται στον ριζικό φάκελο της συνδεδεμένης συσκευής. Επίσης, η Γρήγορη σάρωση δεν περιλαμβάνει αποσυμπίεση και σάρωση αρχείων. Λεπτομερής σάρωση. Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, τότε, αφού συνδέσετε μια εξωτερική συσκευή, το Kaspersky Total Security θα σαρώσει όλα τα αρχεία που βρίσκονται σε κάθε φάκελο της εξωτερικής συσκευής. Επίσης, αποσυμπιέζει και σαρώνει αρχεία, εκτός από αυτά που προστατεύονται με κωδικό πρόσβασης.
Μέγιστο μέγεθος αφαιρούμενης μονάδας δίσκου	Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, τότε το Kaspersky Total Security θα σαρώνει όλες τις εξωτερικές συσκευές που δεν υπερβαίνουν το καθορισμένο μέγιστο μέγεθος. Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security σαρώνει εξωτερικές συσκευές οποιουδήποτε μεγέθους
Προβολή εξέλιξης	Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total
- , , - , - , - , - , - , - , -	security δειχνει την προοδο της σαρωσης των εξωτερικών συσκεύων

σάρωσης	σε ξεχωριστό παράθυρο και στο παράθυρο της σάρωσης που εκτελείται.
Αποκλεισμός της διακοπής της εργασίας σάρωσης	Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το κουμπί Διακοπή δεν είναι διαθέσιμο για τη σάρωση εξωτερικών συσκευών στο τρέχον παράθυρο σάρωσης.

Ρυθμίσεις σάρωσης παρασκηνίου

Αν η σάρωση παρασκηνίου είναι ενεργοποιημένη, το Kaspersky Total Security θα πραγματοποιήσει σάρωση παρασκηνίου. Η σάρωση παρασκηνίου είναι μια λειτουργία αυτόματης σάρωσης του Kaspersky Total Security που δεν εμφανίζει ειδοποιήσεις. Αυτή η σάρωση απαιτεί λιγότερους πόρους υπολογιστή σε σχέση με άλλους τύπους σαρώσεων (για παράδειγμα, Πλήρης σάρωση). Σε αυτή την κατάσταση, το Kaspersky Total Security σαρώνει τη μνήμη συστήματος, τους όγκους συστήματος, τους τομείς εκκίνησης και τα αντικείμενα εκκίνησης και πραγματοποιεί αναζητήσεις για rootkit.

Εάν ο υπολογιστής λειτουργεί με τροφοδοσία μέσω μπαταρίας, το Kaspersky Total Security δεν θα εκτελέσει σαρώσεις παρασκηνίου όταν ο υπολογιστής είναι σε αδράνεια.

Ρυθμίσεις σάρωσης για τρωτά σημεία

Ρυθμίσεις	Περιγραφή
Επεξεργασία εύρους σάρωσης	Κάνοντας κλικ στη σύνδεση ανοίγει το παράθυρο Εύρος σάρωσης για τρωτά σημεία με μια λίστα αντικειμένων που το Kaspersky Total Security σαρώνει για τρωτά σημεία.
	Μπορείτε να προσθέσετε αντικείμενα στη λίστα ή να διαγράψετε τα αντικείμενα που προσθέτετε.
	Για να καταργήσετε ένα αντικείμενο από τη σάρωση, δεν χρειάζεται να διαγράψετε το αντικείμενο από τη λίστα. Το μόνο που χρειάζεται να κάνετε είναι να αποεπιλέξετε το πλαίσιο δίπλα στο όνομα του αντικειμένου.
Χρονοδιάγραμμα σάρωσης	Χειροκίνητα . Λειτουργία εκτέλεσης στην οποία μπορείτε να ξεκινήσετε τη σάρωση για τρωτά σημεία χειροκίνητα κατά τη στιγμή που σας εξυπηρετεί.
	Βάσει προγράμματος . Λειτουργία εκτέλεσης σάρωσης κατά την οποία το Kaspersky Total Security εκτελεί την εργασία σάρωσης σύμφωνα με το χρονοδιάγραμμα που έχετε δημιουργήσει. Εάν επιλέξετε αυτήν τη λειτουργία σάρωσης, μπορείτε επίσης να εκτελέσετε την εργασία σάρωσης χειροκίνητα.

Ρυθμίσεις λογαριασμού χρήστη

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Εκτέλεση εργασιών σάρωσης ως 🖓</u>

Επιλέξτε ένα λογαριασμό τα δικαιώματα του οποίου θα χρησιμοποιούνται από το Kaspersky Total Security για την εκτέλεση εργασιών σάρωσης. Η λειτουργία αυτή είναι διαθέσιμη για την εκτέλεση τόσο των χειροκίνητων όσο και των προγραμματισμένων σαρώσεων του Kaspersky Total Security.

Είναι διαθέσιμες οι παρακάτω επιλογές:

- Τρέχων χρήστης. Οι εργασίες σάρωσης θα εκτελούνται με τα δικαιώματα του τρέχοντος λογαριασμού.
- Άλλος χρήστης. Ο συγκεκριμένος λογαριασμός χρήστη θα χρησιμοποιηθεί για την εκτέλεση των εργασιών σάρωσης. Εάν κάνετε αυτή την επιλογή, πληκτρολογήστε το όνομα του λογαριασμού και τον κωδικό πρόσβασης στα πεδία Λογαριασμός χρήστη και Κωδικός πρόσβασης αντίστοιχα.

Ρυθμίσεις του Προγράμματος Anti-Banner

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Ενεργοποίηση / απενεργοποίηση του Προγράμματος Anti-Banner 🖓</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί το Πρόγραμμα Anti-Banner.

Εάν το κουμπί είναι πράσινο, το Πρόγραμμα Anti-Banner αποκλείει την προβολή των διαφημιστικών πλαισίων που εμφανίζονται στους δικτυακούς τόπους που επισκέπτεστε και στο περιβάλλον εργασίας ορισμένων εφαρμογών. Από προεπιλογή, το Πρόγραμμα Anti-Banner αποκλείει τα διαφημιστικά πλαίσια δικτυακών τόπων από τη λίστα των γνωστών διαφημιστικών πλαισίων. Αυτή η λίστα περιλαμβάνεται στις βάσεις δεδομένων του Kaspersky Total Security.

<u>Λίστα φίλτρων</u> 🕐

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Λίστα φίλτρων** στο οποίο μπορείτε να χρησιμοποιήσετε ειδικά φίλτρα για να καθορίσετε με μεγαλύτερη ακρίβεια τα διαφημιστικά πλαίσια που πρέπει να αποκλείονται.

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο με μια λίστα δικτυακών τόπων στους οποίους έχετε επιτρέψει την εμφάνιση των διαφημιστικών πλαισίων.

Αποκλεισμένα διαφημιστικά πλαίσια 💿

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Αποκλεισμένα** διαφημιστικά πλαίσια. Μπορείτε να χρησιμοποιήσετε αυτό το παράθυρο για να δημιουργήσετε μια λίστα με διαφημιστικά πλαίσια προς αποκλεισμό.

Επιτρεπόμενα διαφημιστικά πλαίσια 🖓

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Επιτρεπόμενα διαφημιστικά πλαίσια**. Μπορείτε να χρησιμοποιήσετε αυτό το παράθυρο για να δημιουργήσετε μια λίστα με διαφημιστικά πλαίσια που θα επιτρέπονται.

<u>Να επιτρέπονται τα διαφημιστικά πλαίσια στις τοποθεσίες web της Kaspersky</u> ව

Εάν επιλεγεί το πλαίσιο ελέγχου, το Πρόγραμμα Anti-Banner δεν αποκλείει τα διαφημιστικά πλαίσια στις τοποθεσίες web της Kaspersky ή των συνεργατών της οι οποίοι φιλοξενούν τις διαφημίσεις της Kaspersky. Μια λίστα αυτών των δικτυακών τόπων διατίθεται μέσω της σύνδεσης **Τοποθεσίες web της Kaspersky**.

Τοποθεσίες web της Kaspersky 🖓

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο με μια λίστα των δικτυακών τόπων της Kaspersky.

Η σύνδεση είναι διαθέσιμη, εάν το πλαίσιο ελέγχου **Να επιτρέπονται τα** διαφημιστικά πλαίσια στις τοποθεσίες web της Kaspersky είναι επιλεγμένο.

Παράθυρο Προσθήκη / Επεξεργασία διαφημιστικού πλαισίου

Ανάπτυξη όλων | Σύμπτυξη όλων

Διεύθυνση IP, διεύθυνση web (URL) ή μάσκα διεύθυνσης web.

Κατά την καταχώριση μιας μάσκας διεύθυνσης web, μπορείτε να χρησιμοποιήσετε τους χαρακτήρες μπαλαντέρ * και ?, όπου το σύμβολο * αναπαριστά οποιαδήποτε σειρά χαρακτήρων, ενώ το σύμβολο ? αναπαριστά οποιονδήποτε μεμονωμένο χαρακτήρα.

<u>Κατάσταση</u> ?

Στην ενότητα **Κατάσταση**, μπορείτε να προσδιορίσετε εάν το Πρόγραμμα Anti-Banner θα χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

Είναι διαθέσιμες οι παρακάτω επιλογές:

- **Ενεργό**. Το Πρόγραμμα Anti-Banner χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.
- Ανενεργό. Το Πρόγραμμα Anti-Banner δεν χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

Παράθυρο Προσθήκη / Επεξεργασία δικτυακού τόπου

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Τοποθεσία web</u> ?

Διεύθυνση web (URL) του δικτυακού τόπου.

<u>Κατάσταση</u> 🕐

Η ενότητα **Κατάσταση** σας επιτρέπει να καθορίσετε εάν το Πρόγραμμα Anti-Banner πρέπει να επιτρέπει ή όχι την εμφάνιση διαφημιστικών πλαισίων στον καθορισμένο δικτυακό τόπο.

Είναι διαθέσιμες οι παρακάτω επιλογές:

- **Ενεργό**. Το Πρόγραμμα Anti-Banner επιτρέπει την εμφάνιση διαφημιστικών πλαισίων στον καθορισμένο δικτυακό τόπο.
- Ανενεργό. Το Πρόγραμμα Anti-Banner δεν επιτρέπει την εμφάνιση διαφημιστικών πλαισίων στον καθορισμένο δικτυακό τόπο.

Το παράθυρο Αποκλεισμένα διαφημιστικά πλαίσια

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κουμπί</u> 🛛 🗗

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα μενού με τα ακόλουθα στοιχεία:

- Εισαγωγή και προσθήκη στα υπάρχοντα. Ενεργοποιώντας αυτό το στοιχείο, ανοίγει ένα παράθυρο που επιτρέπει την εισαγωγή μιας λίστας αποκλεισμένων διευθύνσεων από ένα αρχείο CSV. Οι τρέχουσες διευθύνσεις δεν διαγράφονται.
- Εισαγωγή και αντικατάσταση υπαρχόντων. Ενεργοποιώντας αυτό το στοιχείο, ανοίγει ένα παράθυρο που επιτρέπει την εισαγωγή μιας λίστας αποκλεισμένων διευθύνσεων από ένα αρχείο CSV. Οι τρέχουσες διευθύνσεις διαγράφονται.
- Εξαγωγή. Ενεργοποιώντας αυτό το στοιχείο, ανοίγει ένα παράθυρο που επιτρέπει την εξαγωγή μιας λίστας αποκλεισμένων διευθύνσεων σε ένα αρχείο CSV.

<u>Λίστα αποκλεισμένων διαφημιστικών πλαισίων 💿</u>

Αποθηκεύει τις διευθύνσεις ή τις μάσκες διευθύνσεων των αποκλεισμένων διαφημιστικών πλαισίων. Το πρόγραμμα Anti-Banner αποκλείει ένα διαφημιστικό πλαίσιο εάν η διεύθυνσή του βρίσκεται στη λίστα αποκλεισμένων διαφημιστικών πλαισίων.

Μπορείτε να προσθέσετε μια διεύθυνση ή μια μάσκα διεύθυνσης στη λίστα.

Εάν οριστεί η τιμή *Ενεργό* στη γραμμή διεύθυνσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Banner χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

Εάν οριστεί η τιμή *Ανενεργό* στη γραμμή διεύθυνσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Banner δεν χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

<u>Μάσκα διεύθυνσης web (URL)</u> ?

Αυτή η στήλη εμφανίζει τη διεύθυνση ή μάσκα διεύθυνσης για το αποκλεισμένο διαφημιστικό πλαίσιο.
Αυτή η στήλη δείχνει αν το Πρόγραμμα Anti-Banner χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

Εάν οριστεί η τιμή *Ενεργό* στη γραμμή διεύθυνσης, το Πρόγραμμα Anti-Banner χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

Εάν στη γραμμή διεύθυνσης οριστεί η τιμή *Ανενεργό*, το Πρόγραμμα Anti-Banner δεν χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

<u>Επεξεργασία</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο για την αλλαγή της διεύθυνσης ή της μάσκας διεύθυνσης ενός διαφημιστικού πλαισίου στη λίστα αποκλεισμένων διαφημιστικών πλαισίων.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Πρόγραμμα Anti-Banner διαγράφει την επιλεγμένη διεύθυνση/μάσκα διεύθυνσης ενός διαφημιστικού πλαισίου από τη λίστα.

<u>Προσθήκη</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο για την προσθήκη της διεύθυνσης ή μάσκας διεύθυνσης ενός διαφημιστικού πλαισίου στη λίστα αποκλεισμένων διαφημιστικών πλαισίων.

Το παράθυρο Επιτρεπόμενα διαφημιστικά πλαίσια

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κουμπί</u> 🛯 🔂

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα μενού με τα ακόλουθα στοιχεία:

 Εισαγωγή και προσθήκη στα υπάρχοντα. Ενεργοποιώντας αυτό το στοιχείο, έχετε τη δυνατότητα εισαγωγής μιας λίστας επιτρεπόμενων διευθύνσεων από ένα αρχείο CSV. Οι τρέχουσες διευθύνσεις δεν διαγράφονται.

- Εισαγωγή και αντικατάσταση υπαρχόντων. Ενεργοποιώντας αυτό το στοιχείο, έχετε τη δυνατότητα εισαγωγής μιας λίστας επιτρεπόμενων διευθύνσεων από ένα αρχείο CSV. Οι τρέχουσες διευθύνσεις διαγράφονται.
- Εξαγωγή. Ενεργοποιώντας αυτό το στοιχείο, έχετε τη δυνατότητα εξαγωγής μιας λίστας διευθύνσεων σε ένα αρχείο CSV. Μπορείτε να εξάγετε ολόκληρη τη λίστα διευθύνσεων ή μεμονωμένες διευθύνσεις που έχετε επιλέξει από τη λίστα.

Λίστα επιτρεπόμενων διαφημιστικών πλαισίων 💿

Αποθηκεύει τις διευθύνσεις ή τις μάσκες διευθύνσεων των επιτρεπόμενων διαφημιστικών πλαισίων. Το πρόγραμμα Anti-Banner δεν αποκλείει ένα διαφημιστικό πλαίσιο εάν η διεύθυνσή του βρίσκεται στη λίστα επιτρεπόμενων διευθύνσεων.

Μπορείτε να προσθέσετε μια διεύθυνση ή μια μάσκα διεύθυνσης στη λίστα.

Εάν οριστεί η τιμή *Ενεργό* στη γραμμή διεύθυνσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Banner χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

Εάν οριστεί η τιμή *Ανενεργό* στη γραμμή διεύθυνσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Banner δεν χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

<u>Μάσκα διεύθυνσης web (URL)</u> 🖓

Αυτή η στήλη εμφανίζει τη διεύθυνση ή μάσκα διεύθυνσης για το επιτρεπόμενο διαφημιστικό πλαίσιο.

<u>Κατάσταση</u> 🕐

Αυτή η στήλη δείχνει αν το Πρόγραμμα Anti-Banner χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

Εάν οριστεί η τιμή *Ενεργό* στη γραμμή διεύθυνσης, το Πρόγραμμα Anti-Banner χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

Εάν στη γραμμή διεύθυνσης οριστεί η τιμή *Ανενεργό*, το Πρόγραμμα Anti-Banner δεν χρησιμοποιεί αυτή τη διεύθυνση κατά τη σάρωση διαφημιστικών πλαισίων.

<u>Επεξεργασία</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο για την αλλαγή της διεύθυνσης ή της μάσκας διεύθυνσης ενός διαφημιστικού πλαισίου στη λίστα επιτρεπόμενων διαφημιστικών πλαισίων.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Πρόγραμμα Anti-Banner διαγράφει την επιλεγμένη διεύθυνση/μάσκα διεύθυνσης ενός διαφημιστικού πλαισίου από τη λίστα επιτρεπόμενων διαφημιστικών πλαισίων.

<u>Προσθήκη</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο για την προσθήκη της διεύθυνσης ή της μάσκας διεύθυνσης ενός διαφημιστικού πλαισίου στη λίστα επιτρεπόμενων διευθύνσεων.

Παράθυρο Δικτυακοί τόποι με επιτρεπόμενα διαφημιστικά πλαίσια

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κουμπί</u> 🛛 🗗

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα μενού με τα ακόλουθα στοιχεία:

- Εισαγωγή και προσθήκη στα υπάρχοντα. Ενεργοποιώντας αυτό το στοιχείο, έχετε τη δυνατότητα εισαγωγής μιας λίστας επιτρεπόμενων διευθύνσεων από ένα αρχείο CSV. Οι τρέχουσες διευθύνσεις δεν διαγράφονται.
- Εισαγωγή και αντικατάσταση υπαρχόντων. Ενεργοποιώντας αυτό το στοιχείο, έχετε τη δυνατότητα εισαγωγής μιας λίστας επιτρεπόμενων διευθύνσεων από ένα αρχείο CSV. Οι τρέχουσες διευθύνσεις διαγράφονται.
- Εξαγωγή. Ενεργοποιώντας αυτό το στοιχείο, έχετε τη δυνατότητα εξαγωγής μιας λίστας διευθύνσεων σε ένα αρχείο CSV. Μπορείτε να εξάγετε ολόκληρη τη λίστα διευθύνσεων ή μεμονωμένες διευθύνσεις που έχετε επιλέξει από τη λίστα.

Περιέχει τις διευθύνσεις των δικτυακών τόπων για τους οποίους έχετε επιτρέψει να εμφανίζονται διαφημιστικά πλαίσια. Το Πρόγραμμα Anti-Banner δεν αποκλείει τα διαφημιστικά πλαίσια σε έναν δικτυακό τόπο εάν η διεύθυνσή του περιλαμβάνεται στη λίστα.

Εάν οριστεί η τιμή *Ενεργό* στη γραμμή διεύθυνσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Banner επιτρέπει την εμφάνιση διαφημιστικών πλαισίων σε αυτόν τον δικτυακό τόπο.

Εάν οριστεί η τιμή *Ανενεργό* στη γραμμή διεύθυνσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Banner αποκλείει την εμφάνιση διαφημιστικών πλαισίων σε αυτόν τον δικτυακό τόπο.

<u>Επεξεργασία</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο για την αλλαγή της διεύθυνσης που έχει επιλεγεί στη λίστα.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Πρόγραμμα Anti-Banner καταργεί την επιλεγμένη διεύθυνση τοποθεσίας web από τη λίστα.

<u>Προσθήκη</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο για την προσθήκη μιας διεύθυνσης τοποθεσίας web στη λίστα.

Παράθυρο δικτυακών τόπων της Kaspersky

Αυτό το παράθυρο εμφανίζει μια λίστα με τους δικτυακούς τόπους της Kaspersky και των συνεργατών της οι οποίοι φιλοξενούν τις διαφημίσεις της Kaspersky.

Αυτή η λίστα αναπτύσσεται και ενημερώνεται από ειδικούς της Kaspersky. Στην εφαρμογή, η λίστα ενημερώνεται αυτόματα κατά τη διάρκεια ενημέρωσης των βάσεων δεδομένων και των λειτουργικών μονάδων εφαρμογής.

Ρυθμίσεις του Προγράμματος Anti-Spam

Ανάπτυξη όλων | Σύμπτυξη όλων

Ενεργοποίηση / απενεργοποίηση του Προγράμματος Anti-Spam ව

Με αυτό το κουμπί, μπορείτε να ενεργοποιήσετε / απενεργοποιήσετε το Πρόγραμμα Anti-Spam.

Εάν αυτό το κουμπί είναι ενεργοποιημένο, το Πρόγραμμα Anti-Spam εντοπίζει την ανεπιθύμητη αλληλογραφία (spam) και την επεξεργάζεται σύμφωνα με τους κανόνες του προγράμματος-πελάτη ηλ. αλληλογραφίας που χρησιμοποιείτε.

<u>Επίπεδο ασφαλείας ?</u>

Στην ενότητα **Επίπεδο ασφαλείας**, μπορείτε να επιλέξετε μία από τις προκαθορισμένες συλλογές ρυθμίσεων (επίπεδα ασφάλειας) για το Πρόγραμμα Anti-Spam. Η απόφαση για το επίπεδο ασφάλειας που πρέπει να επιλέξετε εξαρτάται από τις συνθήκες εργασίας και την τρέχουσα κατάσταση.

Είναι διαθέσιμα τα παρακάτω επίπεδα ασφάλειας:

• **Υψηλό**. Σε αυτό το επίπεδο ασφάλειας το Πρόγραμμα Anti-Spam εφαρμόζει τον πιο αυστηρό έλεγχο στο φιλτράρισμα της ανεπιθύμητης αλληλογραφίας.

Συνιστάται να επιλέξετε το υψηλό επίπεδο ασφάλειας κατά την εργασία σε επικίνδυνο περιβάλλον (για παράδειγμα, κατά τη χρήση δωρεάν υπηρεσιών ηλ. αλληλογραφίας).

Η ρύθμιση ενός υψηλού επιπέδου ασφάλειας μπορεί να έχει ως αποτέλεσμα να εμφανίζεται συχνότερα το φαινόμενο της ταξινόμησης μη spam μηνυμάτων ως spam.

- Συνιστάται. Αυτό το επίπεδο ασφάλειας διασφαλίζει τη βέλτιστη ισορροπία μεταξύ επιδόσεων και ασφάλειας. Αυτό το επίπεδο είναι κατάλληλο για τις περισσότερες καταστάσεις.
- Χαμηλό. Σε αυτό το επίπεδο ασφάλειας το Πρόγραμμα Anti-Spam εφαρμόζει το ελάχιστο επίπεδο φιλτραρίσματος ανεπιθύμητης αλληλογραφίας.

Συνιστάται να ορίσετε το χαμηλό επίπεδο ασφάλειας κατά την εργασία σε ασφαλές περιβάλλον (για παράδειγμα, κατά τη χρήση κρυπτογραφημένων εταιρικών υπηρεσιών ηλ. αλληλογραφίας).

Η ρύθμιση ενός χαμηλού επιπέδου ασφάλειας μπορεί να έχει ως αποτέλεσμα να εμφανίζεται λιγότερα συχνά το φαινόμενο της ταξινόμησης μη ανεπιθύμητων μηνυμάτων ως spam ή πιθανό μήνυμα spam.

Κάνοντας κλικ στη σύνδεση οδηγεί το Kaspersky Total Security στο να εφαρμόζει το επίπεδο ασφάλειας **Συνιστάται**. Η σύνδεση εμφανίζεται εάν έχετε τροποποιήσει τις ρυθμίσεις στο παράθυρο **Ρυθμίσεις για προχωρημένους για το Πρόγραμμα Anti-Spam** στην ενότητα **Να γίνει ταξινόμηση ενός μηνύματος ως spam**.

<u>Ρυθμίσεις για προχωρημένους</u> ව

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο Ρυθμίσεις για προχωρημένους για το πρόγραμμα Anti-Spam.

Ρυθμίσεις για προχωρημένους για το πρόγραμμα Anti-Spam

Ανάπτυξη όλων | Σύμπτυξη όλων

Στην ενότητα **Να γίνει ταξινόμηση ενός μηνύματος ως spam** μπορείτε να ορίσετε προϋποθέσεις για το φιλτράρισμα email, τις οποίες χρησιμοποιεί το Πρόγραμμα Anti-Spam για την αναγνώριση της ανεπιθύμητης αλληλογραφίας.

<u>Αν περιέχει στοιχεία phishing </u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί τον έλεγχο μηνυμάτων email για στοιχεία ηλεκτρονικού "ψαρέματος" στο κείμενο ή για διευθύνσεις URL που περιλαμβάνονται στη λίστα διευθύνσεων phishing web.

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Πρόγραμμα Anti-Spam θα θεωρεί ως spam τα μηνύματα που περιέχουν διευθύνσεις URL που βρίσκονται στη λίστα διευθύνσεων phishing web.

Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Πρόγραμμα Anti-Spam δεν θα ελέγχει τις διευθύνσεις URL στα μηνύματα με βάση τη λίστα διευθύνσεων phishing web.

Αν περιέχει διευθύνσεις URL από τη βάση δεδομένων κακόβουλων διευθύνσεων URL 🖓

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί τον έλεγχο του εάν οι σύνδεσμοι, που περιλαμβάνονται σε άμεσα μηνύματα, περιέχονται και στη λίστα κακόβουλων διευθύνσεων URL.

<u>Αν είναι από αποκλεισμένο αποστολέα 🖻</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την επιλογή φιλτραρίσματος αλληλογραφίας με χρήση της λίστας αποκλεισμένων αποστολέων. Το Πρόγραμμα Anti-Spam θα κατατάσσει τα μηνύματα από αυτούς τους αποστολείς ως spam.

<u>Επιλογή</u> ?

Κάνοντας κλικ σε αυτήν τη σύνδεση, ανοίγει το παράθυρο **Αποκλεισμένοι αποστολείς**, στο οποίο μπορείτε να δημιουργήσετε μια λίστα αποκλεισμένων αποστολέων.

Όταν δημιουργείτε τη λίστα, μπορείτε να καθορίσετε τόσο μεμονωμένες διευθύνσεις όσο και μάσκες διευθύνσεων των αποκλεισμένων αποστολέων.

Η σύνδεση αυτή είναι διαθέσιμη εάν έχει επιλεγεί το πλαίσιο ελέγχου **Αν είναι από** αποκλεισμένο αποστολέα.

<u>Αν περιέχει αποκλεισμένες φράσεις ?</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί το φιλτράρισμα μηνυμάτων με βάση τη λίστα αποκλεισμένων φράσεων, η παρουσία των οποίων υποδεικνύει ότι το μήνυμα είναι spam.

<u>Επιλογή</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο **Αποκλεισμένες φράσεις**, στο οποίο μπορείτε να δημιουργήσετε μια λίστα απαγορευμένων φράσεων.

Όταν δημιουργείτε τη λίστα, μπορείτε να καθορίσετε αποκλεισμένες φράσεις και μάσκες φράσεων.

Ο σύνδεσμος αυτός είναι διαθέσιμος εάν έχει επιλεγεί το πλαίσιο ελέγχου **Αν περιέχει αποκλεισμένες φράσεις**.

<u>Αν περιέχει άσεμνες λέξεις </u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Άσεμνη γλώσσα**. Σε αυτό το παράθυρο μπορείτε να δημιουργήσετε μια λίστα άσεμνων λέξεων. Η παρουσία τέτοιων λέξεων σε ένα μήνυμα υποδεικνύει ότι το μήνυμα είναι spam.

Η σύνδεση αυτή είναι διαθέσιμη εάν έχει επιλεγεί το πλαίσιο ελέγχου **Αν περιέχει** άσεμνες λέξεις.

Στην ενότητα **Να μην γίνει ταξινόμηση ενός μηνύματος ως spam**, μπορείτε να ορίσετε τις ενδείξεις που χρησιμοποιεί το Πρόγραμμα Anti-Spam για την αναγνώριση μη ανεπιθύμητων μηνυμάτων.

<u>Αν είναι από επιτρεπόμενο αποστολέα 🖓</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί τον έλεγχο συμπερίληψης της διεύθυνσης ενός αποστολέα στη λίστα επιτρεπόμενων αποστολέων.

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Πρόγραμμα Anti-Spam κατατάσσει ως μη spam τα μηνύματα που προέρχονται από επιτρεπόμενους αποστολείς.

Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Πρόγραμμα Anti-Spam δεν κατατάσσει ως μη spam τα μηνύματα που προέρχονται από επιτρεπόμενους αποστολείς. Τα μηνύματα που αποστέλλονται από αποστολείς της λίστας επιτρεπόμενων αποστολέων δεν φιλτράρονται.

<u>Επιλογή</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Επιτρεπόμενοι αποστολείς**, στο οποίο μπορείτε να δημιουργήσετε μια λίστα επιτρεπόμενων αποστολέων.

Όταν δημιουργείτε τη λίστα, μπορείτε να καθορίσετε διευθύνσεις επιτρεπόμενων αποστολέων ή μάσκες διευθύνσεων.

Ο σύνδεσμος αυτός είναι διαθέσιμος εάν έχει επιλεγεί το πλαίσιο ελέγχου **Αν είναι από** επιτρεπόμενο αποστολέα.

<u>Αν περιέχει επιτρεπόμενες φράσεις 🖓</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί τον έλεγχο ενός μηνύματος με βάση τη λίστα επιτρεπόμενων φράσεων.

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Πρόγραμμα Anti-Spam κατατάσσει ως μη spam τα μηνύματα που περιέχουν φράσεις από τη λίστα αυτή.

Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Πρόγραμμα Anti-Spam δεν χρησιμοποιεί τη λίστα επιτρεπόμενων φράσεων για το φιλτράρισμα των μηνυμάτων και δεν κατατάσσει ως μη ανεπιθύμητα τα μηνύματα που περιέχουν εκφράσεις από τη λίστα.

<u>Επιλογή</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Επιτρεπόμενες φράσεις**, στο οποίο μπορείτε να δημιουργήσετε μια λίστα επιτρεπόμενων φράσεων.

Όταν δημιουργείτε τη λίστα, μπορείτε να καθορίσετε μεμονωμένες φράσεις και μάσκες επιτρεπόμενων φράσεων.

Ο σύνδεσμος αυτός είναι διαθέσιμος εάν έχει επιλεγεί το πλαίσιο ελέγχου **Αν περιέχει** επιτρεπόμενες φράσεις.

Στην ενότητα **Ενέργειες με μηνύματα**, μπορείτε να καθορίσετε τις ετικέτες που πρέπει να προστίθενται στη γραμμή θέματος των μηνυμάτων που κατατάσσονται ως *Spam* ή *Πιθανό* μήνυμα spam από το Πρόγραμμα Anti-Spam.

<u>Προσθήκη ετικέτας [!! SPAM] στο θέμα του μηνύματος που έχει καταταχθεί ως spam</u> ව

Αυτόματη προσθήκη ετικέτας στο θέμα μηνυμάτων, τα οποία το Πρόγραμμα Anti-Spam αναγνωρίζει ως *Spam*.

Το κείμενο της ετικέτας εμφανίζεται στο πεδίο δίπλα στο πλαίσιο ελέγχου. Από προεπιλογή, το Πρόγραμμα Anti-Spam προσθέτει την ετικέτα **[!! SPAM]**.

<u>Προσθήκη ετικέτας [?? Probable SPAM] στο θέμα του μηνύματος που έχει κατηγοριοποιηθεί ως</u> <u>πιθανό spam</u> ?

Αυτόματη προσθήκη ετικέτας στο θέμα μηνυμάτων, τα οποία το Πρόγραμμα Anti-Spam αναγνωρίζει ως *Πιθανό μήνυμα spam*.

Το κείμενο της ετικέτας εμφανίζεται στο πεδίο δίπλα στο πλαίσιο ελέγχου. Από προεπιλογή, το Πρόγραμμα Anti-Spam προσθέτει την ετικέτα **[?? Probable SPAM]**.

Παράθυρο Προσθήκη / Επεξεργασία αποκλεισμένων φράσεων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Μάσκα φράσης</u> 🕐

Φράση ή μάσκα φράσης, η οποία θεωρείται ως ένδειξη spam όταν εντοπίζεται σε ένα μήνυμα.

<u>Συντελεστής στάθμισης φράσης ?</u>

Μια αριθμητική τιμή που υποδεικνύει την πιθανότητα ένα μήνυμα που περιέχει μια αποκλεισμένη φράση να είναι spam. Όσο μεγαλύτερος είναι ο συντελεστής στάθμισης, τόσο υψηλότερη η πιθανότητα να είναι spam το μήνυμα που περιέχει μια αποκλεισμένη φράση.

Το Πρόγραμμα Anti-Spam κατατάσσει ένα μήνυμα ως ανεπιθύμητη αλληλογραφία αν το άθροισμα των συντελεστών αξιολόγησης των αποκλεισμένων φράσεων που περιέχει υπερβαίνει την καθορισμένη τιμή.

<u>Κατάσταση</u> ?

Στην ενότητα **Κατάσταση**, μπορείτε να καθορίσετε εάν θέλετε το Πρόγραμμα Anti-Spam να ελέγχει τα μηνύματα για αποκλεισμένες φράσεις:

- **Ενεργό**. Το Πρόγραμμα Anti-Spam σαρώνει τα μηνύματα για να ελέγξει εάν περιλαμβάνουν αποκλεισμένες φράσεις.
- Ανενεργό. Το Πρόγραμμα Anti-Spam δεν σαρώνει τα μηνύματα για να ελέγξει αν περιέχουν αποκλεισμένες φράσεις.

Το παράθυρο Αποκλεισμένοι αποστολείς

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κουμπί</u> 🛛 🗗

Κάνοντας κλικ στο κουμπί, ανοίγει ένα μενού όπου μπορείτε να επιλέξετε μία από τις παρακάτω ενέργειες:

- Εισαγωγή και προσθήκη στα υπάρχοντα. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εισαγωγής μιας λίστας αποκλεισμένων αποστολέων από ένα αρχείο CSV. Η τρέχουσα λίστα αποστολέων δεν διαγράφεται.
- Εισαγωγή και αντικατάσταση υπαρχόντων. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εισαγωγής μιας λίστας αποκλεισμένων αποστολέων από ένα αρχείο CSV. Η τρέχουσα λίστα αποστολέων διαγράφεται.
- **Εξαγωγή**. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εξαγωγής μιας λίστας αποκλεισμένων αποστολέων σε ένα αρχείο CSV.

Περιέχει μια λίστα διευθύνσεων, τις οποίες το Πρόγραμμα Anti-Spam κατατάσσει ως πηγές ανεπιθύμητης αλληλογραφίας.

Μπορείτε να προσθέσετε μια διεύθυνση ή μια μάσκα διεύθυνσης στη λίστα.

Εάν έχει οριστεί η τιμή *Ενεργό* στη γραμμή διεύθυνσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Spam κατηγοριοποιεί τη διεύθυνση ως αποκλεισμένη.

Εάν έχει οριστεί η τιμή *Ανενεργό* στη γραμμή διεύθυνσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Spam εξαιρεί τη διεύθυνση από τη λίστα.

<u>Διεύθυνση αποστολέα</u> ?

Αυτή η στήλη εμφανίζει τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή τη μάσκα διεύθυνσης email του αποκλεισμένου αποστολέα.

<u>Κατάσταση</u> ?

Αυτή η στήλη δείχνει αν το Πρόγραμμα Anti-Spam κατηγοριοποιεί τα μηνύματα που λαμβάνονται από αυτή τη διεύθυνση ως spam.

Εάν έχει οριστεί η τιμή *Ενεργό* στη γραμμή διεύθυνσης, το Πρόγραμμα Anti-Spam κατηγοριοποιεί τα μηνύματα που λαμβάνονται από αυτή τη διεύθυνση ως spam.

Εάν έχει οριστεί η τιμή *Ανενεργό* στη γραμμή διεύθυνσης, το Πρόγραμμα Anti-Spam εξαιρεί την επιλεγμένη διεύθυνση από τη λίστα.

<u>Επεξεργασία</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο για την αλλαγή της διεύθυνσης URL ή της μάσκας διεύθυνσης URL που έχει επιλεγεί στη λίστα.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Πρόγραμμα Anti-Spam καταργεί την επιλεγμένη διεύθυνση ή μάσκα διεύθυνσης από τη λίστα.

<u>Προσθήκη</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο για την προσθήκη διεύθυνσης URL ή μάσκας διεύθυνσης URL στη λίστα.

Το παράθυρο Αποκλεισμένες φράσεις

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κουμπί 🛛 🗗</u>

Κάνοντας κλικ στο κουμπί, ανοίγει ένα μενού όπου μπορείτε να επιλέξετε μία από τις παρακάτω ενέργειες:

- Εισαγωγή και προσθήκη στα υπάρχοντα. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εισαγωγής μιας λίστας αποκλεισμένων φράσεων από ένα αρχείο CSV. Οι τρέχουσες φράσεις δεν διαγράφονται.
- Εισαγωγή και αντικατάσταση υπαρχόντων. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εισαγωγής μιας λίστας αποκλεισμένων φράσεων από ένα αρχείο CSV. Οι τρέχουσες φράσεις διαγράφονται.
- Εξαγωγή. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εξαγωγής μιας λίστας αποκλεισμένων φράσεων σε ένα αρχείο CSV.

<u>Λίστα αποκλεισμένων φράσεων</u> ව

Περιέχει φράσεις-κλειδιά που δηλώνουν ότι το μήνυμα στο οποίο περιέχονται είναι spam.

Μπορείτε να προσθέσετε στη λίστα μια φράση ή μια μάσκα φράσης.

Εάν οριστεί η τιμή *Ενεργό* στη γραμμή φράσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Spam χρησιμοποιεί αυτή τη φράση κατά το φιλτράρισμα των μηνυμάτων.

Εάν οριστεί η τιμή *Ανενεργό* στη γραμμή φράσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Spam εξαιρεί τη φράση από τη λίστα και δεν τη χρησιμοποιεί κατά το φιλτράρισμα των μηνυμάτων.

<u>Επεξεργασία</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο, στο οποίο μπορείτε να αλλάξετε μια φράση ή μια μάσκα φράσης που θα επιλέξετε στη λίστα.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Πρόγραμμα Anti-Spam καταργεί την επιλεγμένη φράση ή μάσκα φράσης από τη λίστα.

<u>Προσθήκη</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο, στο οποίο μπορείτε να προσθέσετε μια φράση ή μια μάσκα φράσης στη λίστα.

Παράθυρο Προσθήκη / Επεξεργασία διεύθυνσης email

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Μάσκα διεύθυνσης email</u> ?

Σε αυτό το παράθυρο, μπορείτε να καθορίσετε μια διεύθυνση ηλ. αλληλογραφίας ή μια μάσκα διεύθυνσης ηλ. αλληλογραφίας.

Κατά την καταχώριση μιας μάσκας, μπορείτε να χρησιμοποιήσετε τους χαρακτήρες μπαλαντέρ * και ?, όπου το σύμβολο * αναπαριστά οποιαδήποτε σειρά χαρακτήρων, ενώ το σύμβολο ? αναπαριστά οποιονδήποτε μεμονωμένο χαρακτήρα.

<u>Κατάσταση</u> 🕐

Στην ενότητα **Κατάσταση**, μπορείτε να προσδιορίσετε εάν θέλετε το Πρόγραμμα Anti-Spam να αποκλείει τα μηνύματα που αποστέλλονται από αυτή τη διεύθυνση κατά τη σάρωση των μηνυμάτων σύμφωνα με τη λίστα επιτρεπόμενων / αποκλεισμένων αποστολέων.

- Ενεργό. Το Πρόγραμμα Anti-Spam αποκλείει τα μηνύματα που αποστέλλονται από αυτή τη διεύθυνση.
- Ανενεργό. Το Πρόγραμμα Anti-Spam δεν αποκλείει τα μηνύματα που αποστέλλονται από αυτή τη διεύθυνση.

Παράθυρο Προσθήκη / Επεξεργασία επιτρεπόμενων φράσεων

<u>Μάσκα φράσης</u> 🕐

Μια φράση, ή μάσκα φράσης, η παρουσία της οποίας σε ένα μήνυμα υποδεικνύει ότι το μήνυμα δεν είναι spam.

<u>Συντελεστής στάθμισης φράσης</u> 🖓

Μια αριθμητική τιμή που υποδεικνύει την πιθανότητα ένα μήνυμα που περιέχει επιτρεπόμενη φράση να μην είναι spam. Όσο μεγαλύτερος είναι ο συντελεστής στάθμισης, τόσο υψηλότερη η πιθανότητα να μην είναι spam το μήνυμα που περιέχει μια επιτρεπόμενη φράση.

Το Πρόγραμμα Anti-Spam δεν κατατάσσει ένα μήνυμα ως spam αν το άθροισμα των συντελεστών στάθμισης των επιτρεπόμενων φράσεων που περιέχει υπερβαίνει την καθορισμένη τιμή.

<u>Κατάσταση</u> 🕐

Στην ενότητα **Κατάσταση**, μπορείτε να προσδιορίσετε εάν το Πρόγραμμα Anti-Spam θα σαρώνει τα μηνύματα για να ελέγξει αν περιλαμβάνουν μια συγκεκριμένη επιτρεπόμενη φράση.

- Ενεργό. Το Πρόγραμμα Anti-Spam σαρώνει τα μηνύματα για να ελέγξει αν περιλαμβάνουν την επιτρεπόμενη φράση.
- Ανενεργό. Το Πρόγραμμα Anti-Spam δεν σαρώνει τα μηνύματα για να ελέγξει αν περιλαμβάνουν την επιτρεπόμενη φράση.

Το παράθυρο Επιτρεπόμενοι αποστολείς

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κουμπί</u> 🛽 🔁

Κάνοντας κλικ στο κουμπί, ανοίγει ένα μενού όπου μπορείτε να επιλέξετε μία από τις παρακάτω ενέργειες:

Εισαγωγή και προσθήκη στα υπάρχοντα. Ενεργοποιώντας αυτή την επιλογή,
 έχετε τη δυνατότητα εισαγωγής μιας λίστας επιτρεπόμενων αποστολέων από ένα

αρχείο CSV. Η τρέχουσα λίστα αποστολέων δεν διαγράφεται.

- Εισαγωγή και αντικατάσταση υπαρχόντων. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εισαγωγής μιας λίστας επιτρεπόμενων αποστολέων από ένα αρχείο CSV. Η τρέχουσα λίστα αποστολέων διαγράφεται.
- Εξαγωγή. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εξαγωγής μιας λίστας επιτρεπόμενων αποστολέων σε ένα αρχείο CSV.

Η λίστα Επιτρεπόμενοι αποστολείς 🖓

Περιέχει μια λίστα διευθύνσεων αποστολέων, των οποίων τα μηνύματα κατατάσσονται από το Πρόγραμμα Anti-Spam ως μη spam.

Μπορείτε να προσθέσετε μια διεύθυνση ή μια μάσκα διεύθυνσης στη λίστα.

Εάν έχει οριστεί η τιμή *Ενεργό* στη γραμμή διευθύνσεων στη στήλη **Κατάσταση**, το Πρόγραμμα Anti-Spam κατατάσσει κάθε μήνυμα από αυτόν τον αποστολέα ως μη spam.

Εάν έχει οριστεί η τιμή *Ανενεργό* στη γραμμή διευθύνσεων της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Spam δεν κατατάσσει όλα τα μηνύματα από αυτόν τον αποστολέα ως μη spam και τα σαρώνει χρησιμοποιώντας τυπικές μεθόδους σάρωσης.

Διεύθυνση αποστολέα ?

Αυτή η στήλη εμφανίζει τη διεύθυνση ηλεκτρονικού ταχυδρομείου ή τη μάσκα διεύθυνσης email του επιτρεπόμενου αποστολέα.

<u>Κατάσταση</u> 🕐

Αυτή η στήλη δείχνει αν το Πρόγραμμα Anti-Spam κατατάσσει τα μηνύματα που λαμβάνονται από αυτή τη διεύθυνση ως μη spam.

Εάν έχει οριστεί η τιμή *Ενεργό* στη γραμμή διεύθυνσης, το Πρόγραμμα Anti-Spam κατατάσσει τα μηνύματα που λαμβάνονται από αυτή τη διεύθυνση ως μη spam.

Εάν έχει οριστεί η τιμή *Ανενεργό* στη γραμμή διεύθυνσης, το Πρόγραμμα Anti-Spam εξαιρεί την επιλεγμένη διεύθυνση από τη λίστα.

<u>Επεξεργασία</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο, στο οποίο μπορείτε να αλλάξετε μια διεύθυνση URL ή μάσκα διεύθυνσης URL στη λίστα των επιτρεπόμενων αποστολέων.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Πρόγραμμα Anti-Spam καταργεί την επιλεγμένη διεύθυνση ή μάσκα διεύθυνσης από τη λίστα.

<u>Προσθήκη</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο, στο οποίο μπορείτε να προσθέσετε μια διεύθυνση URL ή μάσκα διεύθυνσης URL στη λίστα των επιτρεπόμενων αποστολέων.

<u>Προσθήκη των παραληπτών των μηνυμάτων email μου στους επιτρεπόμενους αποστολείς</u>

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, η εφαρμογή προσθέτει παραλήπτες email στη λίστα επιτρεπόμενων αποστολέων που διαθέτετε.

Το παράθυρο Επιτρεπόμενες φράσεις

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κουμπί 🛛 🗗</u>

Κάνοντας κλικ στο κουμπί, ανοίγει ένα μενού όπου μπορείτε να επιλέξετε μία από τις παρακάτω ενέργειες:

- Εισαγωγή και προσθήκη στα υπάρχοντα. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εισαγωγής μιας λίστας επιτρεπόμενων φράσεων από ένα αρχείο CSV. Οι τρέχουσες φράσεις δεν διαγράφονται.
- Εισαγωγή και αντικατάσταση υπαρχόντων. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εισαγωγής μιας λίστας επιτρεπόμενων φράσεων από ένα αρχείο CSV. Οι τρέχουσες φράσεις διαγράφονται.

• **Εξαγωγή**. Ενεργοποιώντας αυτή την επιλογή, έχετε τη δυνατότητα εξαγωγής μιας λίστας επιτρεπόμενων φράσεων σε ένα αρχείο CSV.

<u>Λίστα επιτρεπόμενων φράσεων</u> ව

Περιέχει βασικές εκφράσεις, των οποίων η παρουσία σε ένα μήνυμα υποδεικνύει ότι το μήνυμα δεν είναι spam.

Μπορείτε να προσθέσετε στη λίστα μια φράση ή μια μάσκα φράσης.

Εάν οριστεί η τιμή *Ενεργό* στη γραμμή φράσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Spam χρησιμοποιεί αυτή τη φράση κατά το φιλτράρισμα των μηνυμάτων.

Εάν οριστεί η τιμή *Ανενεργό* στη γραμμή φράσης της στήλης **Κατάσταση**, το Πρόγραμμα Anti-Spam δεν χρησιμοποιεί αυτή τη φράση κατά το φιλτράρισμα των μηνυμάτων.

<u>Επεξεργασία</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο, στο οποίο μπορείτε να αλλάξετε τη φράση ή τη μάσκα φράσης που θα επιλέξετε στη λίστα.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Πρόγραμμα Anti-Spam καταργεί την επιλεγμένη φράση ή μάσκα φράσης από τη λίστα.

<u>Προσθήκη</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο, στο οποίο μπορείτε να προσθέσετε μια φράση ή μια μάσκα φράσης στη λίστα.

Ρυθμίσεις Προγράμματος Ασφαλείς τραπεζικές συναλλαγές

Ανάπτυξη όλων | Σύμπτυξη όλων

Ενεργοποίηση / απενεργοποίηση Προγράμματος Ασφαλείς τραπεζικές συναλλαγές 🖓

Αυτό το κουμπί ενεργοποιεί / απενεργοποιεί το πρόγραμμα Ασφαλείς τραπεζικές συναλλαγές.

Εάν το κουμπί είναι πράσινο, το Kaspersky Total Security παρακολουθεί όλες τις απόπειρες πρόσβασης σε δικτυακούς τόπους τραπεζών ή συστημάτων πληρωμής και εκτελεί την ενέργεια που έχει οριστεί ως προεπιλογή ή που καθορίζεται από τον χρήστη. Από προεπιλογή, στη λειτουργία Ασφαλών τραπεζικών συναλλαγών, το Kaspersky Total Security ζητά από τον χρήστη επιβεβαίωση για την εκκίνηση του Προστατευμένου προγράμματος περιήγησης.

Αν το κουμπί είναι κόκκινο, το Kaspersky Total Security επιτρέπει την επίσκεψη σε δικτυακούς τόπους τραπεζών ή συστημάτων πληρωμών μέσω ενός κοινού προγράμματος περιήγησης.

Μάθετε περισσότερα ?

Κάνοντας κλικ σε αυτήν τη σύνδεση, ανοίγει μια σελίδα με λεπτομέρειες του στοιχείου σε ένα παράθυρο του προγράμματος περιήγησης.

Στην ενότητα **Κατά την πρώτη πρόσβαση σε τοποθεσίες web τραπεζών και συστημάτων πληρωμής**, μπορείτε να επιλέξετε μια ενέργεια που θα εκτελεί το Kaspersky Total Security όταν επισκέπτεστε δικτυακούς τόπους τραπεζών ή συστημάτων πληρωμής για πρώτη φορά.

<u>Εκτέλεση Προστατευμένου προγράμματος περιήγησης 🕐</u>

Εάν το Kaspersky Total Security εντοπίσει μια προσπάθεια πρόσβασης στον συγκεκριμένο δικτυακό τόπο, ανοίγει τον δικτυακό τόπο χρησιμοποιώντας το Προστατευμένο πρόγραμμα περιήγησης. Το τυπικό πρόγραμμα περιήγησης που χρησιμοποιείται για την πρόσβαση στον δικτυακό τόπο εμφανίζει ένα μήνυμα που σας ενημερώνει για την εκκίνηση του Προστατευμένου προγράμματος περιήγησης.

<u>Προτροπή χρήστη </u>

Εάν το Kaspersky Total Security εντοπίσει μια προσπάθεια πρόσβασης στον συγκεκριμένο δικτυακό τόπο, σας ειδοποιεί να εκκινήσετε ένα Προστατευμένο πρόγραμμα περιήγησης ή να ανοίξετε τον δικτυακό τόπο με το τυπικό πρόγραμμα περιήγησης. Όταν επιχειρείτε να αποκτήσετε πρόσβαση στον συγκεκριμένο δικτυακό τόπο, το Kaspersky Total Security δεν χρησιμοποιεί το Προστατευμένο πρόγραμμα περιήγησης. Ο δικτυακός τόπος ανοίγει στο τυπικό πρόγραμμα περιήγησης.

Στην ενότητα **Πρόσθετα**, μπορείτε να διαμορφώσετε πρόσθετες ρυθμίσεις για τις Ασφαλείς τραπεζικές συναλλαγές.

<u>Για μετάβαση σε τοποθεσίες web από το παράθυρο της λειτουργίας Ασφαλείς τραπεζικές</u> συναλλαγές, να χρησιμοποιηθεί <πρόγραμμα περιήγησης> 🖓

Από την αναπτυσσόμενη λίστα, μπορείτε να επιλέξετε ένα πρόγραμμα περιήγησης με το οποίο το Kaspersky Total Security θα ανοίγει τους δικτυακούς τόπους τραπεζών ή συστημάτων πληρωμής που επιλέγονται στο παράθυρο Ασφαλείς τραπεζικές συναλλαγές.

Η λειτουργία Ασφαλών τραπεζικών συναλλαγών είναι διαθέσιμοι στους χρήστες με τα ακόλουθα προγράμματα περιήγησης: Microsoft Internet Explorer, Microsoft Edge που βασίζεται στο Chromium, Mozilla Firefox, Google Chrome και Yandex.Browser.

Από προεπιλογή, η λειτουργία Ασφαλών τραπεζικών συναλλαγών χρησιμοποιεί το πρόγραμμα περιήγησης που είναι προεπιλεγμένο πρόγραμμα περιήγησης στο λειτουργικό σύστημα.

<u>Δημιουργία συντόμευσης για τις Ασφαλείς τραπεζικές συναλλαγές 🖻</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, δημιουργείται μια συντόμευση επιφάνειας εργασίας για εκκίνηση του προγράμματος Ασφαλείς τραπεζικές συναλλαγές. Αυτή η συντόμευση επιτρέπει το άνοιγμα ενός παραθύρου που περιέχει μια λίστα δικτυακών τόπων τραπεζών ή συστημάτων πληρωμής, για την πρόσβαση στους οποίους χρησιμοποιείται το Προστατευμένο πρόγραμμα περιήγησης.

Στις εκδόσεις 64 bit των Windows 8, των Windows 8.1 και των Windows 10, η αναπαράσταση υλικού χρησιμοποιείται για την προστασία του προγράμματος περιήγησης.

Ρυθμίσεις Προστασίας από ιούς στο Web

Ρυθμίσεις

Περιγραφή

Επίπεδο ασφαλείας	Το Kaspersky Total Security χρησιμοποιεί διάφορα σύνολα ρυθμίσεων για την εκτέλεση της Προστασίας από ιούς στο Web. Τα σύνολα ρυθμίσεων που αποθηκεύονται στην εφαρμογή ονομάζονται <i>Επίπεδα ασφαλείας</i> :
	 Υψηλό. Το επίπεδο ασφαλείας της κυκλοφορίας web που χρησιμοποιεί η Προστασία από ιούς στο Web για να σαρώσει διεξοδικά την κυκλοφορία web που λαμβάνεται από τον υπολογιστή μέσω των πρωτοκόλλων HTTP και FTP. Η προστασία από ιούς στο Web εκτελεί μια λεπτομερή σάρωση όλων των αντικειμένων κυκλοφορίας web χρησιμοποιώντας το πλήρες σύνολο βάσεων δεδομένων εφαρμογών και εκτελεί επίσης τη βαθύτερη ευρετική ανάλυση ?
	 Συνιστάται. Το επίπεδο ασφαλείας κυκλοφορίας web που επιτυγχάνει τη βέλτιστη ισορροπία μεταξύ της απόδοσης του Kaspersky Total Security και της ασφάλειας της κυκλοφορίας web. Η Προστασία από ιούς στο Web εκτελεί ευρετική ανάλυση σε μεσαίο επίπεδο. Αυτό το επίπεδο ασφαλείας κυκλοφορίας web συνιστάται από ειδικούς της Kaspersky.
	 Χαμηλό. Το επίπεδο ασφαλείας κυκλοφορίας web του οποίου οι ρυθμίσεις διασφαλίζουν τη μέγιστη ταχύτητα σάρωσης της κυκλοφορίας web. Η Προστασία από ιούς στο Web εκτελεί ελαφριά ευρετική ανάλυση.
Ενέργεια σε εντοπισμό απειλών	 Προτροπή χρήστη. Η Προστασία από ιούς στο Web σάς ενημερώνει για τον εντοπισμό ενός μολυσμένου ή πιθανώς μολυσμένου αντικειμένου και σας ειδοποιεί για την ενέργεια που θα πραγματοποιήσει.
	Αυτή η επιλογή είναι διαθέσιμη εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στην περιοχή Ρυθμίσεις → Γενικά .
	 Επιλογή ενέργειας αυτόματα Η Προστασία από ιούς στο Web επιλέγει μια ενέργεια αυτόματα με βάση τις τρέχουσες ρυθμίσεις. Εάν ένας πόρος Ιστού περιλαμβάνεται ως εξαίρεση ή δεν περιέχει μολυσμένα ή πιθανώς μολυσμένα αντικείμενα, η Προστασία από ιούς

στο Web σάς επιτρέπει να αποκτήσετε πρόσβαση σε
αυτόν. Εάν η σάρωση που πραγματοποιείται από την
Προστασία από ιούς στο Web εντοπίσει μολυσμένο ή
πιθανώς μολυσμένο αντικείμενο στον πόρο web, η
πρόσβαση προς τον πόρο web θα αποκλειστεί.

Αυτή η επιλογή είναι διαθέσιμη εάν είναι επιλεγμένο το πλαίσιο ελέγχου **Αυτόματη εκτέλεση των** συνιστώμενων ενεργειών στην περιοχή **Ρυθμίσεις** → Γενικά.

- Αποκλεισμός της λήψης. Εάν ορίσετε αυτήν την επιλογή, τότε εάν εντοπιστεί ένα μολυσμένο αντικείμενο στην κυκλοφορία web, η Προστασία από ιούς στο Web αποκλείει την πρόσβαση σε αυτό το αντικείμενο και εμφανίζει ένα μήνυμα στο πρόγραμμα περιήγησης.
- Ειδοποίηση. Εάν αυτή η επιλογή είναι ενεργοποιημένη και εντοπιστεί ένα μολυσμένο αντικείμενο στην κυκλοφορία ιστού, το Kaspersky Total Security επιτρέπει τη λήψη αυτού του αντικειμένου στον υπολογιστή, αλλά προσθέτει πληροφορίες σχετικά με το μολυσμένο αντικείμενο στη λίστα των εντοπισμένων αντικειμένων.

Έλεγχος της διεύθυνσης URL έναντι της βάσης δεδομένων κακόβουλων διευθύνσεων URL	Η σάρωση των συνδέσεων για να προσδιοριστεί εάν περιλαμβάνονται στη βάση δεδομένων κακόβουλων συνδέσεων σας επιτρέπει να παρακολουθείτε τοποθεσίες web που έχουν προστεθεί στη λίστα μη επιτρεπόμενων στοιχείων. Η βάση δεδομένων των κακόβουλων συνδέσεων δημιουργείται από ειδικούς της Kaspersky. Αποτελεί μέρος του κιτ διανομής λογισμικού και ενημερώνεται μαζί με τη βάση δεδομένων του Kaspersky Total Security.
Έλεγχος της διεύθυνσης URL έναντι της βάσης δεδομένων διευθύνσεων URL που περιέχουν πρόγραμμα adware	Ένα παράδειγμα είναι λογισμικό που ανακατευθύνει το ερώτημα της αναζήτησής σας στο Διαδίκτυο σε μια τοποθεσία web διαφημίσεων. Έτσι, λαμβάνετε μια τοποθεσία web διαφημίσεων αντί για τον πόρο web που έχει μεγαλύτερη σχέση με το ερώτημα της αναζήτησής σας.
Έλεγχος της διεύθυνσης URL έναντι της βάσης	Ένα παράδειγμα αυτής της κατηγορίας είναι ένα εργαλείο απομακρυσμένης αντιμετώπισης προβλημάτων που χρησιμοποιούν νόμιμα οι διαχειριστές συστημάτων. Ένας

δεδομένων διευθύνσεων URL που περιέχουν νόμιμες εφαρμογές οι οποίες μπορούν να χρησιμοποιηθούν από εγκληματίες για την καταστροφή του υπολογιστή σας ή των προσωπικών δεδομένων σας	εγκληματίας μπορεί να εγκαταστήσει ένα τέτοιο εργαλείο στον υπολογιστή σας χωρίς να το γνωρίζετε, για να αποκτήσει πρόσβαση στον υπολογιστή σας και να τον χρησιμοποιήσει για εγκληματικούς σκοπούς.
Χρήση ευρετικής ανάλυσης	Μια τεχνική για τον εντοπισμό απειλών που δεν μπορούν να προσδιοριστούν χρησιμοποιώντας την τρέχουσα έκδοση των βάσεων δεδομένων της εφαρμογής Kaspersky. Σας επιτρέπει να βρείτε αρχεία που ενδέχεται να περιέχουν άγνωστο κακόβουλο λογισμικό ή μια νέα τροποποίηση γνωστού προγράμματος με κακόβουλο λογισμικό.
	Όταν η κυκλοφορία web σαρώνεται για ιούς και άλλες εφαρμογές που αποτελούν απειλή, το πρόγραμμα ευρετικής ανάλυσης εκτελεί οδηγίες στα εκτελέσιμα αρχεία. Ο αριθμός των οδηγιών που εκτελούνται από την ευρετική ανάλυση εξαρτώνται από το επίπεδο που καθορίζεται για την ευρετική ανάλυση. Το επίπεδο της ευρετικής ανάλυσης ορίζει την ισορροπία μεταξύ της πληρότητας αναζήτησης για νέες απειλές, το φορτίο στους πόρους του λειτουργικού συστήματος και τον χρόνο που απαιτείται για την ευρετική ανάλυση.
Έλεγχος της διεύθυνσης URL έναντι της βάσης δεδομένων διευθύνσεων phishing URL	Τα περιεχόμενα της βάσης δεδομένων συνδέσεων phishing περιλαμβάνουν τις διευθύνσεις web των γνωστών τοποθεσιών web τη δεδομένη στιγμή που χρησιμοποιούνται για επιθέσεις phishing. Η Kaspersky συμπληρώνει αυτήν τη βάση δεδομένων συνδέσεων phishing με διευθύνσεις που λαμβάνονται από τον διεθνή οργανισμό Anti-Phishing Working Group (Ομάδα εργασίας για την καταπολέμηση του phishing). Η βάση δεδομένων των συνδέσεων phishing αποτελεί μέρος του κιτ διανομής λογισμικού και ενημερώνεται μαζί με τη βάση δεδομένων του Kaspersky Total Security.
Κατά του phishing Χρήση ευρετικής ανάλυσης	Μια τεχνική για τον εντοπισμό απειλών που δεν μπορούν να προσδιοριστούν χρησιμοποιώντας την τρέχουσα έκδοση των βάσεων δεδομένων της εφαρμογής Kaspersky. Αυτό επιτρέπει τον εντοπισμό ενεργειών phishing, ακόμη και αν η

	διεύθυνση URL δεν βρίσκεται στη βάση δεδομένων των διευθύνσεων web phishing.
Έλεγχος URL	Το στοιχείο "Σύμβουλος URL" ελέγχει τις συνδέσεις στις ιστοσελίδες που ανοίγουν στον Microsoft Edge που βασίζεται στο Chromium, το Google Chrome ή το Mozilla Firefox. Το Kaspersky Total Security εμφανίζει ένα από τα παρακάτω εικονίδια δίπλα σε κάθε σύνδεση που έχει ελεγχθεί:
	🥑 – αν ο συνδεδεμένος δικτυακός τόπος είναι ασφαλής σύμφωνα με την Kaspersky
	ον δεν υπάρχουν πληροφορίες σχετικά με την κατάσταση ασφαλείας του συνδεδεμένου δικτυακού τόπου
	eáv μια ιστοσελίδα που ανοίχθηκε από σύνδεση μπορεί να χρησιμοποιηθεί από εγκληματίες για την καταστροφή του υπολογιστή σας ή των προσωπικών δεδομένων σας, σύμφωνα με την Kaspersky
	• αν ο συνδεδεμένος δικτυακός τόπος είναι επικίνδυνος σύμφωνα με την Kaspersky Για να προβάλετε ένα αναπτυσσόμενο παράθυρο με περισσότερες λεπτομέρειες σχετικά με τη σύνδεση, μετακινήστε το δείκτη του ποντικιού στο αντίστοιχο εικονίδιο.
Σε όλες τις τοποθεσίες web εκτός από τις καθορισμένες Διαχείριση εξαιρέσεων	Όταν είναι ενεργοποιημένη αυτή η επιλογή, το Kaspersky Total Security σαρώνει συνδέσεις σε όλες τις τοποθεσίες web, εκτός από αυτές που αναφέρονται στο παράθυρο Εξαιρέσεις . Το παράθυρο Εξαιρέσεις ανοίνει κάνοντας κλικ στη σύνδεση
- ,	Διαχείριση εξαιρέσεων.
Μόνο στις καθορισμένες τοποθεσίες web Ρύθμιση παραμέτρων	Όταν είναι ενεργοποιημένη αυτή η επιλογή, το Kaspersky Total Security σαρώνει συνδέσεις μόνο σε αυτές τις τοποθεσίες web που αναφέρονται στο παράθυρο Ελεγμένες τοποθεσίες web .
ελεγμένων τοποθεσιών web	Το παράθυρο Ελεγμένες τοποθεσίες web ανοίγει κάνοντας κλικ στη σύνδεση Ρύθμιση παραμέτρων ελεγμένων τοποθεσιών web .
Ρύθμιση παραμέτρων	 Όλες οι διευθύνσεις URL. Το Kaspersky Total Security

Συμβούλου URL	σαρώνει συνδέσεις σε όλους τους τύπους τοποθεσιών web. • Μόνο διευθύνσεις URL στα αποτελέσματα αναζήτησης . Το Kaspersky Total Security σαρώνει συνδέσεις σε τοποθεσίες web που περιέχουν αποτελέσματα αναζήτησης που λαμβάνονται από μηχανές αναζήτησης.
Κατηγορίες τοποθεσιών web	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου Εμφάνιση πληροφοριών σχετικά με τις κατηγορίες περιεχομένου των τοποθεσιών web, το Kaspersky Total Security προσθέτει τα σχόλια της σύνδεσης για να υποδείξει εάν η τοποθεσία web ανήκει σε μία από τις αναφερόμενες κατηγορίες (για παράδειγμα, Βία ή Περιεχόμενο για ενήλικες). Μπορείτε να καταργήσετε τα πλαίσια ελέγχου δίπλα στις κατηγορίες που δεν απαιτούν προειδοποιήσεις.
Να μην γίνεται σάρωση κυκλοφορίας web που προέρχεται από αξιόπιστες διευθύνσεις web	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, η Προστασία από ιούς στο Web δεν σαρώνει το περιεχόμενο ιστοσελίδων/ τοποθεσιών web των οποίων οι διευθύνσεις περιλαμβάνονται στη λίστα αξιόπιστων διευθύνσεων web. Μπορείτε να προσθέσετε και συγκεκριμένες ιστοσελίδες/ διευθύνσεις τοποθεσιών web καθώς και μάσκες διευθύνσεων ιστοσελίδας/τοποθεσίας web στη λίστα αξιόπιστων διευθύνσεων web. Η λίστα των αξιόπιστων διευθύνσεων web είναι διαθέσιμη στο παράθυρο Αξιόπιστες διευθύνσεις URL , το οποίο μπορεί να ανοίξει κάνοντας κλικ στη σύνδεση από τις Αξιόπιστες διευθύνσεις URL .

Παράθυρο Δικτυακοί τόποι της Kaspersky και των συνεργατών της

Αυτό το παράθυρο εμφανίζει τη λίστα δικτυακών τόπων της Kaspersky και των συνεργατών της.

Αυτή η λίστα αναπτύσσεται και ενημερώνεται από ειδικούς της Kaspersky. Στην εφαρμογή, η λίστα ενημερώνεται αυτόματα κατά τη διάρκεια ενημέρωσης των βάσεων δεδομένων και των λειτουργικών μονάδων εφαρμογής.

Ρυθμίσεις Αποκλεισμού επιθέσεων δικτύου

Ο Αποκλεισμός επιθέσεων δικτύου φορτώνεται κατά την εκκίνηση του λειτουργικού συστήματος και σαρώνει την εισερχόμενη κυκλοφορία δικτύου για δραστηριότητες που είναι χαρακτηριστικές των επιθέσεων δικτύου. Όταν το Kaspersky Total Security εντοπίζει μια απόπειρα επίθεσης δικτύου στον υπολογιστή ενός χρήστη, αποκλείει τη σύνδεση δικτύου με τον επιτιθέμενο υπολογιστή.

Οι περιγραφές των γνωστών τύπων επιθέσεων δικτύου τη δεδομένη στιγμή και οι μέθοδοι εξουδετέρωσής τους καθορίζονται στις βάσεις δεδομένων του Kaspersky Total Security. Η λίστα επιθέσεων δικτύου που είναι ανιχνεύσιμες από τον Αποκλεισμό επιθέσεων δικτύου ενημερώνεται όταν ενημερώνονται οι βάσεις δεδομένων και οι λειτουργικές μονάδες της εφαρμογής.

Ρυθμίσεις Αποκλεισμού επιθέσεων δικτύου

Ρυθμίσεις	Περιγραφή
Αντιμετωπίστε τη σάρωση θυρών και την υπερφόρτωση δικτύου ως επιθέσεις	Η Υπερφόρτωση δικτύου είναι μια επίθεση στους πόρους δικτύου του οργανισμού (για παράδειγμα, διακομιστές web). Αυτή η επίθεση συνίσταται στην αποστολή τεράστιου όγκου κυκλοφορίας για την εξάντληση της χωρητικότητας κυκλοφορίας ενός δικτύου. Ως αποτέλεσμα, οι χρήστες δεν έχουν πρόσβαση στους πόρους δικτύου του οργανισμού.
	<i>Η επίθεση σάρωσης θυρών</i> συνίσταται στην σάρωση θυρών UDP και TCP, καθώς και υπηρεσιών δικτύου στον υπολογιστή. Αυτή η επίθεση επιτρέπει τον προσδιορισμό του επιπέδου ύπαρξης τρωτών σημείων στον υπολογιστή πριν από ακόμη πιο επικίνδυνους τύπους επιθέσεων δικτύου. Η σάρωση θύρας επιτρέπει επίσης στους εισβολείς να προσδιορίσουν το λειτουργικό σύστημα του υπολογιστή και να επιλέξουν συγκεκριμένες επιθέσεις για αυτό.
	Εάν η εναλλαγή είναι ενεργοποιημένη, το στοιχείο Αποκλεισμός επιθέσεων δικτύου αποκλείει τη σάρωση θύρας και την πλημμύρα δικτύου.
Προσθήκη επιτιθέμενου υπολογιστή στη λίστα των αποκλεισμένων υπολογιστών για Ν λεπτά	Εάν η εναλλαγή είναι ενεργοποιημένη, τότε ο Αποκλεισμός επιθέσεων δικτύου θα προσθέσει τον επιτιθέμενο υπολογιστή στη λίστα αποκλεισμένων. Αυτό σημαίνει ότι ο Αποκλεισμός επιθέσεων δικτύου, θα αποκλείσει τη σύνδεση δικτύου με τον επιτιθέμενο υπολογιστή μετά την πρώτη προσπάθεια επίθεσης δικτύου κατά τη διάρκεια της καθορισμένης χρονικής περιόδου, προκειμένου να προστατεύσει αυτόματα τον υπολογιστή του χρήστη από τυχόν μελλοντικές επιθέσεις δικτύου από την ίδια διεύθυνση.

Διαχείριση εξαιρέσεων Η λίστα περιέχει διευθύνσεις ΙΡ από τις οποίες ο Αποκλεισμός επιθέσεων δικτύου δεν αποκλείει επιθέσεις δικτύου.

Το Kaspersky Total Security δεν αναφέρει πληροφορίες σχετικά με επιθέσεις δικτύου από διευθύνσεις ΙΡ που περιλαμβάνονται στη λίστα εξαιρέσεων.

Ρυθμίσεις Ελέγχου εφαρμογών

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Ενεργοποίηση / απενεργοποίηση Ελέγχου εφαρμογών 🤊</u>

Με αυτό το κουμπί, μπορείτε να ενεργοποιήσετε / απενεργοποιήσετε τον Έλεγχο εφαρμογών.

Μάθετε περισσότερα ?

Κάνοντας κλικ σε αυτήν τη σύνδεση, ανοίγει μια σελίδα με λεπτομέρειες του στοιχείου σε ένα παράθυρο του προγράμματος περιήγησης.

Να θεωρούνται αξιόπιστες οι εφαρμογές με ψηφιακή υπογραφή 🖻

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, ο Έλεγχος εφαρμογών κατατάσσει τις εφαρμογές που έχουν ψηφιακές υπογραφές ως αξιόπιστες. Ο Έλεγχος εφαρμογών μετακινεί αυτές τις εφαρμογές στην ομάδα **Αξιόπιστες** και δεν ελέγχει τη δραστηριότητά τους.

Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, ο Έλεγχος εφαρμογών δεν κατατάσσει τις εφαρμογές που έχουν ψηφιακές υπογραφές ως αξιόπιστες και ελέγχει τις δραστηριότητές τους. Ο Έλεγχος εφαρμογών ταξινομεί τις εφαρμογές αξιόπιστων προμηθευτών λογισμικού (για παράδειγμα της Microsoft) ως αξιόπιστες, είτε είναι επιλεγμένο αυτό το πλαίσιο ελέγχου είτε όχι.

<u>Φόρτωση κανόνων για εφαρμογές από το Kaspersky Security Network (KSN)</u> ව

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, ο Έλεγχος εφαρμογών στέλνει ένα αίτημα στη βάση δεδομένων του Kaspersky Security Network με σκοπό να ορίσει την ομάδα μιας εφαρμογής. Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, ο Έλεγχος εφαρμογών δεν κάνει αναζήτηση για πληροφορίες στη βάση δεδομένων του Kaspersky Security Network με σκοπό να ορίσει την ομάδα αξιοπιστίας της εφαρμογής.

<u>Ομάδα αξιοπιστίας για εφαρμογές που δεν ήταν δυνατόν να προστεθούν στις υπάρχουσες</u> ομάδες 🕜

Η σύνδεση ανοίγει το παράθυρο **Ομάδα αξιοπιστίας για εφαρμογές που δεν ήταν δυνατόν να προστεθούν στις υπάρχουσες ομάδες**. Σε αυτό το παράθυρο μπορείτε να επιλέξετε την <u>ομάδα αξιοπιστίας</u> στην οποία θα εκχωρούνται οι άγνωστες εφαρμογές. Μπορείτε να επιλέξετε μία από τις παρακάτω επιλογές:

- Αξιόπιστες
- Χαμηλού Περιορισμού
- Υψηλού Περιορισμού
- Μη αξιόπιστες

<u>Αλλαγή ομάδας αξιοπιστίας για εφαρμογές που εκκινούνται πριν από την εκκίνηση του</u> <u>Kaspersky Total Security</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Ομάδα αξιοπιστίας για τις** εφαρμογές που εκκινήθηκαν πριν την εκκίνηση του Kaspersky Total Security. Σε αυτό το παράθυρο, μπορείτε να αλλάξετε την ομάδα αξιοπιστίας ? για τις εφαρμογές που ξεκίνησαν πριν από την εκκίνηση του Kaspersky Total Security. Η δραστηριότητα δικτύου των εφαρμογών που εκκινούνται πριν από την εκκίνηση του Kaspersky Total Security ελέγχεται σύμφωνα με τους κανόνες της επιλεγμένης ομάδας αξιοπιστίας.

Από προεπιλογή, οι εφαρμογές που εκκινούνται πριν από την εκκίνηση του Kaspersky Total Security εκχωρούνται σε μία από τις ομάδες αξιοπιστίας σύμφωνα με τους κανόνες που έχει δημιουργήσει η Kaspersky.

<u>Διαχείριση εφαρμογών </u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Διαχείριση εφαρμογών**. Σε αυτό το παράθυρο, μπορείτε να επεξεργαστείτε τη λίστα κανόνων για εφαρμογές.

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Διαχείριση πόρων**. Σε αυτό το παράθυρο, μπορείτε να δημιουργήσετε μια λίστα των προσωπικών δεδομένων και μια λίστα με τις ρυθμίσεις και τους πόρους του λειτουργικού συστήματος. Η πρόσβαση σε αυτά τα στοιχεία ελέγχεται από τον Έλεγχο εφαρμογών.

Παράθυρο Εικόνες συλλογής στατιστικών στοιχείων

Αυτό το παράθυρο εμφανίζει μια λίστα με τις εικόνες συλλογής στατιστικών στοιχείων.

Αυτή η λίστα αναπτύσσεται και ενημερώνεται από ειδικούς της Kaspersky. Στην εφαρμογή, η λίστα ενημερώνεται αυτόματα κατά τη διάρκεια ενημέρωσης των βάσεων δεδομένων και των λειτουργικών μονάδων εφαρμογής.

Ιδιωτική περιήγηση. Κατηγορίες και εξαιρέσεις

Ανάπτυξη όλων | Σύμπτυξη όλων

Υπηρεσίες ανάλυσης δικτύου 🖓

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, το στοιχείο Ιδιωτική περιήγηση αποκλείει τις υπηρεσίες ανάλυσης δικτύου που παρακολουθούν και αναλύουν την online δραστηριότητά σας.

Κάνοντας κλικ στη σύνδεση **Προβολή λίστας**, ανοίγει ένα παράθυρο που περιέχει μια λίστα υπηρεσιών ανάλυσης δικτύου που χρησιμοποιούν την παρακολούθηση δραστηριοτήτων για να αναλύσουν την online δραστηριότητά σας.

<u>Διαφημιστικά πρακτορεία</u> 🖓

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, το στοιχείο Ιδιωτική περιήγηση εμποδίζει την παρακολούθηση της online δραστηριότητάς σας από διαφημιστικά πρακτορεία για σκοπούς μάρκετινγκ.

Κάνοντας κλικ στη σύνδεση **Προβολή λίστας**, ανοίγει ένα παράθυρο που περιέχει μια λίστα διαφημιστικών πρακτορείων που παρακολουθούν την online δραστηριότητά σας για σκοπούς μάρκετινγκ. Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, το στοιχείο Ιδιωτική περιήγηση εμποδίζει την παρακολούθηση της online δραστηριότητάς σας μέσω εικόνων συλλογής στατιστικών στοιχείων. Οι εικόνες συλλογής στατιστικών στοιχείων είναι αντικείμενα που ενσωματώνονται σε δικτυακούς τόπους και δεν είναι ορατές στους χρήστες.

Κάνοντας κλικ στη σύνδεση **Προβολή λίστας**, ανοίγει ένα παράθυρο με τη λίστα των εικόνων συλλογής στατιστικών στοιχείων.

Μέσα κοινωνικής δικτύωσης 🖓

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, το στοιχείο Ιδιωτική περιήγηση αποκλείει τη συλλογή δεδομένων όταν επισκέπτεστε κοινωνικά δίκτυα, με εξαίρεση τη συλλογή δεδομένων που εκτελείται από τα ίδια τα κοινωνικά δίκτυα. Ο αποκλεισμός της συλλογής δεδομένων δεν σας εμποδίζει από το να χρησιμοποιήσετε λειτουργίες όπως "Μου αρέσει", "+1" και παρόμοιες λειτουργίες.

Τα πλαίσια ελέγχου με τα ονόματα των κοινωνικών δικτύων σάς δίνουν τη δυνατότητα να προσδιορίσετε τα κοινωνικά δίκτυα στους δικτυακούς τόπους των οποίων η εφαρμογή θα αποκλείει τη συλλογή δεδομένων.

<u>Εξαιρέσεις</u> 🕐

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο στο οποίο μπορείτε να καθορίσετε τους δικτυακούς τόπους στους οποίους θα επιτρέπεται η παρακολούθηση της online δραστηριότητάς σας.

Παράθυρο Μη συμβατοί δικτυακοί τόποι

Αυτό το παράθυρο εμφανίζει μια λίστα των δικτυακών τόπων που μπορεί να καταστούν μη λειτουργικοί ως αποτέλεσμα του αποκλεισμού της συλλογής δεδομένων, σύμφωνα με τις πληροφορίες που είναι στη διάθεση της Kaspersky.

Αυτή η λίστα αναπτύσσεται και ενημερώνεται από ειδικούς της Kaspersky. Στην εφαρμογή, η λίστα ενημερώνεται αυτόματα κατά τη διάρκεια ενημέρωσης των βάσεων δεδομένων και των λειτουργικών μονάδων εφαρμογής.

Παράθυρο ρυθμίσεων ιδιωτικής περιήγησης

Εάν ο διακόπτης εναλλαγής είναι ενεργοποιημένος, όταν είστε online το στοιχείο Ιδιωτική περιήγηση εντοπίζει τις προσπάθειες συλλογής δεδομένων από υπηρεσίες παρακολούθησης. Οι υπηρεσίες παρακολούθησης χρησιμοποιούν τις πληροφορίες που λαμβάνουν για να αναλύσουν τη δραστηριότητά σας και μπορούν να χρησιμοποιήσουν τα αποτελέσματα αυτής της ανάλυσης για να σας εμφανίσουν σχετικές διαφημίσεις.

<u>Μόνο συλλογή στατιστικών στοιχείων</u> ව

Όταν αυτή η επιλογή είναι ενεργοποιημένη, το στοιχείο Ιδιωτική περιήγηση βρίσκεται σε *λειτουργία εντοπισμού*, δίνοντάς σας τη δυνατότητα να βλέπετε αναφορές για εντοπισμένες προσπάθειες συλλογής δεδομένων.

Να αποκλειστεί η συλλογή δεδομένων 🖓

Όταν αυτή η επιλογή είναι ενεργοποιημένη, το στοιχείο Ιδιωτική περιήγηση βρίσκεται σε *λειτουργία αποκλεισμού*, εντοπίζοντας και αποκλείοντας προσπάθειες συλλογής δεδομένων. Πληροφορίες σχετικά με αυτές τις προσπάθειες καταγράφονται σε μια αναφορά.

<u>Κατηγορίες και εξαιρέσεις </u>?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο στο οποίο μπορείτε να ορίσετε τις κατηγορίες υπηρεσιών παρακολούθησης για τις οποίες θέλετε να αποκλειστεί ή να επιτραπεί η συλλογή δεδομένων. Από αυτό το παράθυρο μπορείτε να προχωρήσετε στη δημιουργία μιας λίστας δικτυακών τόπων στους οποίους θέλετε να επιτρέπεται η παρακολούθηση.

<u>Αποκλεισμός παρακολούθησης</u> 🖓

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο και η λειτουργία αποκλεισμού ενεργοποιημένη, κάθε φορά που επισκέπτεστε έναν δικτυακό τόπο, το πρόγραμμα περιήγησης στέλνει την κεφαλίδα HTTP "Χωρίς παρακολούθηση" στον δικτυακό τόπο, κάτι που σημαίνει ότι δεν επιτρέπεται η παρακολούθηση της δραστηριότητάς σας. Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security επιτρέπει τη συλλογή δεδομένων στους δικτυακούς τόπους της Kaspersky και των συνεργατών της.

<u>Τοποθεσίες web της Kaspersky και των συνεργατών της</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο με τη λίστα δικτυακών τόπων της Kaspersky και των συνεργατών της.

<u>Να επιτρέπεται η συλλογή δεδομένων σχετικά με μη συμβατές τοποθεσίες web</u> ව

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security επιτρέπει τη συλλογή δεδομένων σε δικτυακούς τόπους που μπορεί να καταστούν μη λειτουργικοί ως αποτέλεσμα αποκλεισμού της συλλογής δεδομένων.

<u>Μη συμβατές τοποθεσίες web</u> 🖓

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο με μια λίστα δικτυακών τόπων που μπορεί να καταστούν μη λειτουργικοί ως αποτέλεσμα αποκλεισμού της συλλογής δεδομένων.

Παράθυρο Διαφημιστικά πρακτορεία

Αυτό το παράθυρο εμφανίζει μια λίστα διαφημιστικών πρακτορείων που παρακολουθούν την online δραστηριότητά σας για σκοπούς μάρκετινγκ.

Αυτή η λίστα αναπτύσσεται και ενημερώνεται από ειδικούς της Kaspersky. Στην εφαρμογή, η λίστα ενημερώνεται αυτόματα κατά τη διάρκεια ενημέρωσης των βάσεων δεδομένων και των λειτουργικών μονάδων εφαρμογής.

Παράθυρο Υπηρεσίες ανάλυσης δικτύου

Αυτό το παράθυρο εμφανίζει μια λίστα υπηρεσιών ανάλυσης δικτύου που παρακολουθούν και αναλύουν την online δραστηριότητά σας.

Αυτή η λίστα αναπτύσσεται και ενημερώνεται από ειδικούς της Kaspersky. Στην εφαρμογή, η λίστα ενημερώνεται αυτόματα κατά τη διάρκεια ενημέρωσης των βάσεων δεδομένων και των λειτουργικών μονάδων εφαρμογής.

Ρυθμίσεις Προστασίας email από ιούς

Ρυθμίσεις	Περιγραφή
Επίπεδο ασφαλείας	Το Kaspersky Total Security χρησιμοποιεί διάφορα σύνολα ρυθμίσεων για την εκτέλεση της Προστασίας email από ιούς. Τα σύνολα ρυθμίσεων που αποθηκεύονται στην εφαρμογή ονομάζονται <i>Επίπεδα ασφαλείας</i> :
	 Υψηλό. Εάν επιλεγεί αυτό το επίπεδο ασφάλειας αλληλογραφίας, η Προστασία email από ιούς εφαρμόζει τον πιο αυστηρό έλεγχο στα μηνύματα. Η Προστασία email από ιούς σαρώνει εισερχόμενα και εξερχόμενα μηνύματα αλληλογραφίας και εκτελεί επίσης μια βαθιά ευρετική ανάλυση. Σας συνιστούμε να χρησιμοποιείτε το Υψηλό επίπεδο ασφαλείας αλληλογραφίας σε επικίνδυνο περιβάλλον. Ένα παράδειγμα τέτοιου περιβάλλοντος είναι μια σύνδεση σε δωρεάν υπηρεσία email από οικιακό δίκτυο που δεν φυλάσσεται από κεντρική προστασία email.
	 Συνιστάται. Το επίπεδο ασφαλείας αλληλογραφίας που επιτυγχάνει τη βέλτιστη ισορροπία μεταξύ της απόδοσης του Kaspersky Total Security και της ασφάλειας αλληλογραφίας. Η Προστασία email από ιούς σαρώνει εισερχόμενα και εξερχόμενα μηνύματα αλληλογραφίας και εκτελεί επίσης μια ευρετική ανάλυση μεσαίου επιπέδου. Αυτό το επίπεδο ασφαλείας αλληλογραφίας συνιστάται από ειδικούς της Kaspersky.
	 Χαμηλό. Αυτό είναι το επίπεδο ασφαλείας αλληλογραφίας που χρησιμοποιεί η Προστασία email από ιούς μόνο για τη σάρωση εισερχόμενων μηνυμάτων αλληλογραφίας καθώς και για την εκτέλεση επιφανειακής ευρετικής ανάλυσης. Δεν χρησιμοποιεί αυτό το επίπεδο για τη σάρωση αρχειοθηκών που είναι συνημμένες σε μηνύματα. Όταν επιλεγεί αυτό το επίπεδο ασφαλείας αλληλογραφίας, το στοιχείο Προστασία email από ιούς σαρώνει τα μηνύματα email όσο το δυνατόν γρηγορότερα και καταναλώνει την ελάχιστη ποσότητα πόρων του λειτουργικού συστήματος. Το επίπεδο ασφαλείας αλληλογραφίας Χαμηλό χρησιμοποιείται κατά την εργασία σε αξιόπιστα προστατευμένο περιβάλλον. Ένα παράδειγμα τέτοιου περιβάλλοντος μπορεί να είναι ένα τοπικό δίκτυο με κεντρική ασφάλεια email.

Ενέργεια σε εντοπισμό απειλών

 Προτροπή χρήστη. Η Προστασία email από ιούς σας ενημερώνει για την ανίχνευση ενός μολυσμένου ή πιθανώς μολυσμένου αντικείμενο και σας ειδοποιεί για τις περαιτέρω ενέργειες που θα εκτελεστούν σε αυτό το αντικείμενο.

Αυτή η επιλογή είναι διαθέσιμη εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου **Αυτόματη εκτέλεση των συνιστώμενων** ενεργειών στην περιοχή **Ρυθμίσεις** → **Γενικά**.

 Επιλογή ενέργειας αυτόματα. Όταν εντοπίζονται μολυσμένα ή πιθανώς μολυσμένα αντικείμενα, η Προστασία email από ιούς εκτελεί αυτόματα την ενέργεια που συνιστάται από τους ειδικούς της Kaspersky. Για μολυσμένα αντικείμενα, η ενέργεια είναι Απολύμανση. Αυτή η τιμή είναι επιλεγμένη από προεπιλογή.

Πριν επιχειρηθεί η απολύμανση ή διαγραφή ενός μολυσμένου αντικειμένου, η Προστασία email από ιούς δημιουργεί ένα αντίγραφο ασφαλείας σε περίπτωση που χρειαστεί αργότερα να αποκατασταθεί το αντικείμενο ή υπάρχει η πιθανότητα απολύμανσής του.

Αυτή η επιλογή είναι διαθέσιμη εάν είναι επιλεγμένο το πλαίσιο ελέγχου **Αυτόματη εκτέλεση των συνιστώμενων** ενεργειών στην περιοχή **Ρυθμίσεις** → **Γενικά**.

- Απολύμανση, εάν η απολύμανση αποτύχει, τότε διαγραφή. Εάν εντοπιστεί ένα μολυσμένο αντικείμενο σε ένα εισερχόμενο ή εξερχόμενο μήνυμα, το Kaspersky Total Security προσπαθεί να απολυμάνει το αντικείμενο που εντοπίστηκε. Ο χρήστης θα μπορεί να αποκτήσει πρόσβαση σε ένα μήνυμα με ασφαλές συνημμένο. Ωστόσο, εάν το Kaspersky Total Security δεν είναι σε θέση να απολυμάνει το αντικείμενο, τότε θα το διαγράψει. Το Kaspersky Total Security προσθέτει πληροφορίες σχετικά με την εκτελούμενη ενέργεια στο θέμα του μηνύματος: [Το μολυσμένο αντικείμενο διαγράφηκε] <θέμα μηνύματος>.
- Απολύμανση, εάν η απολύμανση αποτύχει, τότε αποκλεισμός. Εάν εντοπιστεί ένα μολυσμένο αντικείμενο σε ένα εισερχόμενο μήνυμα, το Kaspersky Total Security προσπαθεί να απολυμάνει το αντικείμενο που εντοπίστηκε. Ο χρήστης θα μπορεί να αποκτήσει πρόσβαση σε ένα μήνυμα με ασφαλές συνημμένο. Εάν το αντικείμενο δεν μπορεί να

	 απολυμανθεί, το Kaspersky Total Security προσθέτει μια προειδοποίηση στο θέμα του μηνύματος: [Μολυσμένο μήνυμα] <θέμα μηνύματος>. Ο χρήστης θα μπορεί να αποκτήσει πρόσβαση στο μήνυμα με το αρχικό συνημμένο. Εάν εντοπιστεί ένα μολυσμένο αντικείμενο σε ένα εξερχόμενο μήνυμα, το Kaspersky Total Security θα προσπαθήσει να απολυμάνει το αντικείμενο που εντοπίστηκε. Εάν το Kaspersky Total Security δεν είναι σε θέση να απολυμάνει το αντικείμενο, θα αποκλείσει την αποστολή του μηνύματος και το πρόγραμμα email θα εμφανίσει ένα μολυσμένο αντικείμενο σε ένα είσερχόμενο μήνυμα, το Kaspersky Total Security δεν είναι σε θέση να απολυμάνει το αντικείμενο, θα αποκλείσει την αποστολή του μηνύματος και το πρόγραμμα email θα εμφανίσει ένα μολυσμένο αντικείμενο σε ένα εισερχόμενο μήνυμα, το Kaspersky Total Security θα προσθέσει μια προειδοποίηση στο θέμα του μηνύματος: [Μολυσμένο μήνυμα] <θέμα μηνύματος>. Ο χρήστης θα μπορεί να αποκτήσει πρόσβαση στο μήνυμα με το αρχικό συνημμένο. Εάν εντοπιστεί ένα μολυσμένο αντικείμενο σε ένα εξερχόμενο μήνυμα, το Kaspersky Total Security θα αποκλείσει την αποστολή του μηνύματος και το πρόγραμμα email θα εμφανίσει ένα μολυσμένο αντικείμενο σε ένα εξερχόμενο μήνυμα, το Kaspersky Total Security θα αποκλείσει την αποστολή του μηνύματος και το πρόγραμμα email θα εμφανίσει ένα μολυσμένο αντικείμενο σε ένα εξερχόμενο μήνυμα, το Kaspersky Total Security θα αποκλείσει την αποστολή του μηνύματος και το πρόγραμμα
Ισχύς προστασίας	Η <i>Ισχύς προστασίας</i> περιλαμβάνει αντικείμενα που ελέγχει το στοιχείο κατά την εκτέλεσή του: Εισερχόμενα και εξερχόμενα μηνύματα ή Εισερχόμενα μηνύματα μόνο . Για να προστατεύσετε τους υπολογιστές σας, χρειάζεστε σάρωση μόνο των εισερχόμενων μηνυμάτων. Μπορείτε να ενεργοποιήσετε τη σάρωση για εξερχόμενα μηνύματα για να αποτρέψετε την αποστολή μολυσμένων αρχείων σε αρχειοθήκες. Μπορείτε επίσης να ενεργοποιήσετε τη σάρωση εξερχόμενων μηνυμάτων εάν θέλετε να αποτρέψετε την αποστολή αρχείων συγκεκριμένης μορφής, όπως για παράδειγμα, αρχείων ήχου και βίντεο.
Σάρωση κίνησης POP3, SMTP, NNTP και IMAP	Αυτό το πλαίσιο ελέγχου ενεργοποιεί/απενεργοποιεί τη σάρωση από την Προστασία email από ιούς της επισκεψιμότητας αλληλογραφίας που αποστέλλεται μέσω των πρωτοκόλλων POP3, SMTP, NNTP και IMAP.
Σύνδεση πρόσθετου Microsoft Outlook	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, τα μηνύματα email που αποστέλλονται μέσω των πρωτοκόλλων POP3, SMTP, NNTP και IMAP θα σαρώνονται χρησιμοποιώντας την επέκταση που είναι ενσωματωμένη στο Microsoft Office Outlook.

	Εάν σαρωθεί το email χρησιμοποιώντας την επέκταση για το Microsoft Outlook, συνιστάται η χρήση της λειτουργίας Cached Exchange. Μπορείτε να βρείτε περισσότερες λεπτομέρειες σχετικά με τη λειτουργία Cached Exchange και προτάσεις για τον τρόπο χρήσης της στη <u>Γνωσιακή βάση της Microsoft</u> .
Ευρετική ανάλυση	Μια τεχνική για τον εντοπισμό απειλών που δεν μπορούν να προσδιοριστούν χρησιμοποιώντας την τρέχουσα έκδοση των βάσεων δεδομένων της εφαρμογής Kaspersky. Σας επιτρέπει να βρείτε αρχεία που ενδέχεται να περιέχουν άγνωστο κακόβουλο λογισμικό ή μια νέα τροποποίηση γνωστού προγράμματος με κακόβουλο λογισμικό.
	Κατά τη σάρωση αρχείων για κακόβουλο κώδικα, η ευρετική ανάλυση εκτελεί οδηγίες στα εκτελέσιμα αρχεία. Ο αριθμός των οδηγιών που εκτελούνται από την ευρετική ανάλυση εξαρτώνται από το επίπεδο που καθορίζεται για την ευρετική ανάλυση. Το επίπεδο της ευρετικής ανάλυσης ορίζει την ισορροπία μεταξύ της πληρότητας αναζήτησης για νέες απειλές, το φορτίο στους πόρους του λειτουργικού συστήματος και τον χρόνο που απαιτείται για την ευρετική ανάλυση.
Σάρωση επισυναπτόμενων αρχείων μορφών Microsoft Office	Σαρώνει αρχεία του Microsoft Office (DOC, DOCX, XLS, PPT και άλλες επεκτάσεις της Microsoft). Τα αρχεία μορφής Office περιλαμβάνουν επίσης αντικείμενα OLE.
Σάρωση συνημμένων αρχειοθηκών	Σαρώνει αρχεία με τις ακόλουθες μορφές: RAR, ARJ, ZIP, CAB, LHA, JAR και ICE.
Να μην πραγματοποιείται σάρωση σε αρχεία μεγαλύτερα από	Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, η Προστασία email από ιούς εξαιρεί αρχειοθήκες που είναι συνημμένες σε μηνύματα email από τη σάρωση εάν το μέγεθός τους υπερβαίνει την τιμή που έχετε καθορίσει. Εάν το πλαίσιο ελέγχου δεν είναι επιλεγμένο, η Προστασία email από ιούς σαρώνει αρχεία οποιουδήποτε μεγέθους που είναι συνημμένα σε μηνύματα email.
Περιορισμός του χρόνου σάρωσης	Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, τότε ο χρόνος που απαιτείται για τη σάρωση αρχείων που επισυνάπτονται σε μηνύματα email θα περιοριστεί στο καθορισμένο χρονικό
αρχείων σε	διάστημα.

Το φίλτρο συνημμένων δεν λειτουργεί για εξερχόμενα μηνύματα email.

Απενεργοποίηση φιλτραρίσματος. Εάν ορίσετε αυτήν την επιλογή, η Προστασία email από ιούς δεν θα φιλτράρει αρχεία που είναι συνημμένα σε μηνύματα email.

Μετονομασία συνημμένων των επιλεγμένων τύπων. Εάν ορίσετε αυτήν την επιλογή, η Προστασία email από ιούς θα αντικαταστήσει τον τελευταίο χαρακτήρα της επέκτασης στα συνημμένα αρχεία των καθορισμένων τύπων με τον χαρακτήρα υπογράμμισης (για παράδειγμα, attachment.doc_). Έτσι, προκειμένου να ανοίξει το αρχείο, ο χρήστης θα πρέπει να το μετονομάσει.

Διαγραφή συνημμένων των επιλεγμένων τύπων. Εάν ορίσετε αυτήν την επιλογή, η Προστασία email από ιούς θα διαγράψει αρχεία των καθορισμένων τύπων που είναι συνημμένα σε μηνύματα email.

Μπορείτε να προσδιορίσετε τους τύπους των συνημμένων αρχείων που πρέπει να μετονομάσετε ή να διαγράψετε από τα Μηνύματα email στη λίστα μασκών αρχείων.

Παράθυρο Ιδιότητες δικτύου (προσαρμογέα)

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Όνομα</u> ?

Όνομα προσαρμογέα δικτύου.

<u>Τύπος σύνδεσης</u> 🕐

Τύπος προσαρμογέα δικτύου, για παράδειγμα, δίκτυο Ethernet, ασύρματο δίκτυο ή σύνδεση modem.

<u>Κατάσταση</u> 🕐
Τρέχουσα κατάσταση της σύνδεσης δικτύου: Συνδέθηκε ή Αποσυνδέθηκε.

Στην ενότητα **Νέες συνδέσεις**, μπορείτε να επιλέξετε την ενέργεια που θα εκτελεί το Τείχος προστασίας όταν εντοπίζεται μια νέα σύνδεση με χρήση αυτού του προσαρμογέα.

<u>Ερώτηση για ομάδα</u> ?

Εάν το Τείχος προστασίας εντοπίσει μια νέα σύνδεση δικτύου, σας ειδοποιεί και σας ζητά να επιλέξετε μια κατάσταση για το νέο δίκτυο.

Αυτόματη μετακίνηση νέων δικτύων στην ομάδα 💿

Εάν το Τείχος προστασίας εντοπίσει μια νέα σύνδεση δικτύου, εκχωρεί αυτόματα σε αυτό το δίκτυο την κατάσταση που έχει επιλεγεί στην αναπτυσσόμενη λίστα.

Στην αναπτυσσόμενη λίστα, μπορείτε να ορίσετε την κατάσταση δικτύου που θα εκχωρεί αυτόματα το Τείχος προστασίας στα νέα δίκτυα.

Ρυθμίσεις Παρακολούθησης συστημάτων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Ενεργοποίηση/απενεργοποίηση</u> ?

Με αυτό το κουμπί, μπορείτε να ενεργοποιήσετε / απενεργοποιήσετε την Παρακολούθηση συστημάτων.

Εάν αυτό το κουμπί είναι πράσινο, η Παρακολούθηση συστημάτων συλλέγει και αποθηκεύει δεδομένα για όλα τα συμβάντα που προκύπτουν στο λειτουργικό σύστημα (όπως τροποποίηση ενός αρχείου, τροποποίηση κλειδιών μητρώου, εκκίνηση προγραμμάτων οδήγησης ή απόπειρες τερματισμού του υπολογιστή). Τα δεδομένα αυτά χρησιμοποιούνται για την παρακολούθηση κακόβουλων και άλλων δραστηριοτήτων του λογισμικού (συμπεριλαμβανομένου του ransomware) και για την επαναφορά του λειτουργικού συστήματος στην κατάσταση που ήταν πριν από την εμφάνιση του λογισμικού (για επαναφορά των ενεργειών του λογισμικού). Μερικές φορές, η δραστηριότητα των εφαρμογών δεν μπορεί να αντιστραφεί, για παράδειγμα όταν εντοπίζεται εφαρμογή από το στοιχείο Έλεγχος εφαρμογών. Η Παρακολούθηση συστημάτων συλλέγει δεδομένα από διάφορες πηγές, συμπεριλαμβανομένων άλλων στοιχείων του Kaspersky Total Security. Η Παρακολούθηση συστημάτων αναλύει τη δραστηριότητα των εφαρμογών και παρέχει σε άλλα στοιχεία του Kaspersky Total Security τις πληροφορίες που συλλέγει σχετικά με τα συμβάντα.

Στην ενότητα **Αποτροπή εκμετάλλευσης**, μπορείτε να διαμορφώσετε τις ενέργειες που πραγματοποιεί η εφαρμογή σε περίπτωση εκτέλεσης εκτελέσιμων αρχείων από τρωτές εφαρμογές.

<u>Παρακολούθηση προσπαθειών εκτέλεσης μη εξουσιοδοτημένων λειτουργιών 💿</u>

Με αυτό το πλαίσιο ελέγχου, μπορείτε να ενεργοποιήσετε / απενεργοποιήσετε την Πρόληψη εκμετάλλευσης ?

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security παρακολουθεί τα εκτελέσιμα αρχεία τα οποία εκτελούνται από τρωτές εφαρμογές. Εάν το Kaspersky Total Security εντοπίσει μια προσπάθεια εκτέλεσης εκτελέσιμου αρχείου από μια τρωτή εφαρμογή, που δεν έχει εκκινηθεί από το χρήστη, η εφαρμογή εκτελεί την ενέργεια που επιλέγεται από την αναπτυσσόμενη λίστα **Σε περίπτωση εντοπισμού απειλής**.

Όταν γίνεται αναβάθμιση του Kaspersky Total Security από έκδοση παλιότερη από την έκδοση Kaspersky Total Security 2018, αυτή η ρύθμιση παίρνει την προεπιλεγμένη τιμή.

<u>Κατά την ανίχνευση απειλών</u> ?

Σε αυτήν την αναπτυσσόμενη λίστα, μπορείτε να επιλέξετε την ενέργεια που θα εκτελεί η Παρακολούθηση συστημάτων όταν εκτελείται ένα εκτελέσιμο αρχείο από μια παρακολουθούμενη τρωτή εφαρμογή.

Η λίστα αυτή παρέχει τη δυνατότητα επιλογής ανάμεσα στις εξής ενέργειες:

- Προτροπή χρήστη. Η Παρακολούθηση συστημάτων ρωτά το χρήστη για την ανάληψη δράσης. Αυτή η επιλογή είναι διαθέσιμη εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στην περιοχή Ρυθμίσεις → Γενικά.
- Επιλογή ενέργειας αυτόματα. Η Παρακολούθηση συστημάτων εκτελεί αυτόματα την ενέργεια που έχει επιλεγεί στις ρυθμίσεις εφαρμογής και προσθέτει πληροφορίες για την επιλεγμένη ενέργεια στην αναφορά. Αυτή η επιλογή είναι διαθέσιμη εάν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στην περιοχή Ρυθμίσεις → Γενικά.

- Να επιτραπεί η ενέργεια. Η Παρακολούθηση συστημάτων επιτρέπει την εκτέλεση του εκτελέσιμου αρχείου.
- Αποκλεισμός ενέργειας. Η Παρακολούθηση συστημάτων αποκλείει το εκτελέσιμο αρχείο.

<u>Ενέργεια κατά τον εντοπισμό κακόβουλης ή άλλης δραστηριότητας 🖓</u>

Στην αναπτυσσόμενη λίστα, μπορείτε να επιλέξετε την ενέργεια που θα εκτελεί η Παρακολούθηση συστημάτων όταν εντοπίζεται κακόβουλη ή άλλη δραστηριότητα με βάση τα αποτελέσματα της ανάλυσης δραστηριότητας εφαρμογών.

- Προτροπή χρήστη. Η Παρακολούθηση συστημάτων ρωτά το χρήστη για την ανάληψη δράσης. Αυτή η επιλογή είναι διαθέσιμη εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στην περιοχή Ρυθμίσεις → Γενικά.
- Επιλογή ενέργειας αυτόματα. Η Παρακολούθηση συστημάτων επιλέγει αυτόματα την ενέργεια που συνιστάται από τους ειδικούς της Kaspersky για να αντιμετωπίσει την εφαρμογή. Αυτή η επιλογή είναι διαθέσιμη εάν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στην περιοχή Ρυθμίσεις → Γενικά.
- Επιλογή ενέργειας αυτόματα. Η Παρακολούθηση συστημάτων επιλέγει αυτόματα την ενέργεια που συνιστάται από τους ειδικούς της Kaspersky για να αντιμετωπίσει την εφαρμογή.
- Διαγραφή της εφαρμογής. Η Παρακολούθηση συστημάτων διαγράφει την εφαρμογή.
- **Τερματισμός της εφαρμογής**. Η Παρακολούθηση συστημάτων τερματίζει όλες τις διεργασίες της εφαρμογής.
- Παράβλεψη. Η Παρακολούθηση συστημάτων δεν εκτελεί καμία ενέργεια επί της εφαρμογής.

Ενέργειες προς εκτέλεση εάν η κακόβουλη ή άλλη δραστηριότητα μπορεί να αντιστραφεί ?

Στην αναπτυσσόμενη λίστα, μπορείτε να επιλέξετε την ενέργεια που θα εκτελεί η Παρακολούθηση συστημάτων όταν μπορεί να αντιστραφεί η κακόβουλη ή άλλη δραστηριότητα.

- Εντολή για ενέργεια. Αν η Παρακολούθηση συστημάτων, η Προστασία αρχείων από ιούς ή τα αποτελέσματα μιας εργασίας σάρωσης για ιούς επιβεβαιώνουν ότι είναι απαραίτητο να γίνει επαναφορά, η Παρακολούθηση συστημάτων ειδοποιεί το χρήστη για την ενέργεια. Αυτή η επιλογή είναι διαθέσιμη εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στην περιοχή Ρυθμίσεις → Γενικά.
- Επιλογή ενέργειας αυτόματα. Εάν η Παρακολούθηση συστημάτων κρίνει μια εφαρμογή ως κακόβουλη, αφού αναλύσει τη δραστηριότητά της, εκτελεί επαναφορά της δραστηριότητας της εφαρμογής και ενημερώνει τον χρήστη σχετικά με αυτό το συμβάν. Αυτή η επιλογή είναι διαθέσιμη εάν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στην περιοχή Ρυθμίσεις → Γενικά.
- Επαναφορά. Η Παρακολούθηση συστημάτων εκτελεί επαναφορά της κακόβουλης ή άλλης δραστηριότητας της εφαρμογής.
- Να μην γίνει επαναφορά. Η Παρακολούθηση συστημάτων αποθηκεύει πληροφορίες σχετικά με την κακόβουλη ή άλλη δραστηριότητα αλλά δεν επαναφέρει τις ενέργειες της εφαρμογής.

Στην ενότητα **Προστασία από κακόβουλα προγράμματα κλειδώματος οθόνης**, μπορείτε να διαμορφώσετε τις ενέργειες που θα εκτελεί το Kaspersky Total Security αν εντοπιστεί δραστηριότητα κλειδώματος οθόνης. Τα κλειδώματα οθόνης είναι κακόβουλα προγράμματα που περιορίζουν τις δραστηριότητες του χρήστη σε έναν υπολογιστή, κλειδώνοντας την οθόνη και το πληκτρολόγιο ή εμποδίζοντας την πρόσβαση στη γραμμή εργασιών και τις συντομεύσεις. Τα κλειδώματα οθόνης μπορεί να επιχειρήσουν να αποσπάσουν λύτρα για την ανάκτηση της πρόσβασης στο λειτουργικό σύστημά σας. Χρησιμοποιώντας την προστασία από κακόβουλα προγράμματα κλειδώματος οθόνης, μπορείτε να κλείσετε κάθε κλείδωμα οθόνης πατώντας ένα συγκεκριμένο συνδυασμό πλήκτρων.

<u>Εντοπισμός και κλείσιμο κακόβουλων προγραμμάτων κλειδώματος οθόνης 🖓</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την προστασία από κακόβουλα προγράμματα κλειδώματος οθόνης.

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, όταν ανιχνεύεται δραστηριότητα κλειδώματος οθόνης, μπορείτε να τη σταματήσετε πατώντας το συνδυασμό πλήκτρων που προσδιορίζεται στην αναπτυσσόμενη λίστα κάτω από το πλαίσιο ελέγχου.

Όταν γίνεται αναβάθμιση του Kaspersky Total Security από έκδοση παλιότερη από την έκδοση Kaspersky Total Security 2018, αυτή η ρύθμιση παίρνει την προεπιλεγμένη τιμή.

<u>Χρησιμοποιήστε τον παρακάτω συνδυασμό πλήκτρων για να κλείσετε χειροκίνητα ένα</u> κακόβουλο πρόγραμμα κλειδώματος οθόνης 💿

Στην αναπτυσσόμενη λίστα, μπορείτε να επιλέξετε ένα πλήκτρο ή ένα συνδυασμό πλήκτρων, τα οποία, όταν χρησιμοποιούνται, ενεργοποιούν την προστασία από κλειδώματα οθόνης για την ανίχνευση και διαγραφή του κλειδώματος οθόνης.

Ο ακόλουθος συνδυασμός πλήκτρων χρησιμοποιείται από προεπιλογή: CTRL+ALT+SHIFT+F4.

Ρυθμίσεις Προστασίας αρχείων από ιούς

Ρυθμίσεις	Περιγραφή
Επίπεδο ασφαλείας	Το Kaspersky Total Security χρησιμοποιεί διάφορες ομάδες ρυθμίσεων για την εκτέλεση της Προστασίας αρχείων από ιούς. Τα σύνολα ρυθμίσεων που αποθηκεύονται στην εφαρμογή ονομάζονται <i>Επίπεδα ασφαλείας</i> :
	 Υψηλό. Όταν επιλεγεί αυτό το επίπεδο ασφαλείας αρχείου, το στοιχείο Προστασία αρχείων από ιούς εκτελεί τον αυστηρότερο έλεγχο όλων των αρχείων που έχουν ανοίξει, αποθηκευτεί και εκκινηθεί. Το στοιχείο Προστασία αρχείων από ιούς σαρώνει όλους τους τύπους σκληρών δίσκων, μονάδων δίσκου δικτύου και αφαιρούμενων μέσων αποθήκευσης του υπολογιστή. Επίσης, σαρώνει αρχειοθήκες, πακέτα εγκατάστασης και ενσωματωμένα αντικείμενα OLE.
	 Συνιστάται. Αυτό το επίπεδο ασφαλείας αρχείων συνιστάται από ειδικούς της Kaspersky Lab. Το στοιχείο Προστασίας αρχείων από ιούς σαρώνει μόνο συγκεκριμένες μορφές αρχείων σε όλους τους σκληρούς δίσκους, σε μονάδες δίσκου δικτύου και σε αφαιρούμενα μέσα αποθήκευσης του υπολογιστή και ενσωματωμένα αντικείμενα OLE. Το στοιχείο Προστασία αρχείων από ιούς δεν σαρώνει αρχεία ή πακέτα εγκατάστασης.
	 Χαμηλό. Οι ρυθμίσεις αυτού του επιπέδου ασφαλείας αρχείου διασφαλίζουν τη μέγιστη ταχύτητα σάρωσης. Το στοιχείο Προστασία αρχείων από ιούς σαρώνει μόνο αρχεία με τις καθορισμένες επεκτάσεις σε όλους τους σκληρούς δίσκους, τις μονάδες δίσκου δικτύου και τα αφαιρούμενα μέσα

	αποθήκευσης του υπολογιστή. Το στοιχείο Προστασία αρχείων από ιούς δεν σαρώνει σύνθετα αρχεία.
Ενέργεια σε εντοπισμό απειλών	 Προτροπή χρήστη. Η Προστασία αρχείων από ιούς σας ενημερώνει για την ανίχνευση ενός μολυσμένου ή πιθανώς μολυσμένου αντικειμένου και σας ειδοποιεί για την ενέργεια που θα πραγματοποιήσει.
	Αυτή η επιλογή είναι διαθέσιμη εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στην περιοχή Ρυθμίσεις → Γενικά .
	 Επιλογή ενέργειας αυτόματα. Μόλις εντοπιστούν μολυσμένα ή πιθανώς μολυσμένα στοιχεία, η Προστασία αρχείων από ιούς εκτελεί αυτόματα στο αντικείμενο την ενέργεια που συνιστάται από τους ειδικούς της Kaspersky. Για μολυσμένα αντικείμενα, η ενέργεια είναι Απολύμανση. Αυτή η τιμή είναι επιλεγμένη από προεπιλογή.
	Πριν επιχειρήσει να απολυμάνει ή να διαγράψει ένα μολυσμένο αντικείμενο, η Προστασία αρχείων από ιούς δημιουργεί το αντίγραφο ασφαλείας του για επακόλουθη επαναφορά ή απολύμανση.
	Αυτή η επιλογή είναι διαθέσιμη εάν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στην περιοχή Ρυθμίσεις → Γενικά .
	Απολύμανση, εάν η απολύμανση αποτύχει, τότε διαγραφή. Εάν επιλέξετε αυτήν την ενέργεια, τότε το Kaspersky Total Security θα προσπαθήσει αυτόματα να απολυμάνει όλα τα μολυσμένα αρχεία που εντοπίζει. Εάν αποτύχει η απολύμανση, το Kaspersky Total Security διαγράφει τα αντικείμενα.
	 Απολύμανση, εάν η απολύμανση αποτύχει, τότε αποκλεισμός. Εάν επιλέξετε αυτήν την ενέργεια, τότε το Kaspersky Total Security θα προσπαθήσει αυτόματα να

απολυμάνει όλα τα μολυσμένα αρχεία που εντοπίζει. Εάν η απολύμανση αποτύχει, το Kaspersky Total Security θα προσθέσει πληροφορίες σχετικά με τα μολυσμένα αρχεία που εντοπίζει στη λίστα των εντοπισμένων αντικειμένων.

	 Αποκλεισμός. Εάν είναι ενεργοποιημένη αυτή η επιλογή, το στοιχείο Προστασία αρχείων από ιούς αποκλείει αυτόματα όλα τα μολυσμένα αρχεία χωρίς να προσπαθεί να τα απολυμάνει.
	Πριν επιχειρήσει να απολυμάνει ή να διαγράψει ένα μολυσμένο αρχείο, το Kaspersky Total Security δημιουργεί ένα αντίγραφο ασφαλείας σε περίπτωση που χρειαστεί στη συνέχεια να επαναφέρετε το αρχείο ή να είναι δυνατή η απολύμανσή του αργότερα.
Τύποι αρχείου	Όλα τα αρχεία . Εάν είναι ενεργοποιημένη αυτή η ρύθμιση, το Kaspersky Total Security σαρώνει όλα τα αρχεία χωρίς εξαίρεση (οποιασδήποτε μορφής και με οποιαδήποτε επέκταση).
	Σάρωση αρχείων κατά μορφή . Εάν επιλέξετε αυτήν τη ρύθμιση, το Kaspersky Total Security θα σαρώνει μόνο <u>Δυνητικά επικίνδυνα</u> <u>για μόλυνση αρχεία </u> ?. Πριν από την αναζήτηση για κακόβουλο κώδικα σε ένα αρχείο, θα αναλυθεί η εσωτερική κεφαλίδα του ώστε να προσδιοριστεί η μορφή του αρχείου (για παράδειγμα, TXT, DOC, EXE). Η σάρωση αναζητά επίσης αρχεία με συγκεκριμένες επεκτάσεις αρχείων.
	Σάρωση αρχείων κατά επέκταση . Εάν επιλέξετε αυτήν τη ρύθμιση, το Kaspersky Total Security θα σαρώνει μόνο <u>Δυνητικά</u> επικίνδυνα για μόλυνση αρχεία 💿. Η μορφή του αρχείου προσδιορίζεται με βάση την επέκτασή του.
Επεξεργασία ισχύος προστασίας	Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο Ισχύς προστασίας αρχείων από ιούς , το οποίο περιέχει μια λίστα αντικειμένων που σαρώνονται από την Προστασία αρχείων από ιούς.
	Μπορείτε να προσθέσετε αντικείμενα στη λίστα ή να διαγράψετε τα αντικείμενα που προσθέτετε.
	Για να καταργήσετε ένα αντικείμενο από τη σάρωση, δεν χρειάζεται να διαγράψετε το αντικείμενο από τη λίστα. Το μόνο που χρειάζεται να κάνετε είναι να αποεπιλέξετε το πλαίσιο δίπλα στο όνομα του αντικειμένου.
Ευρετική ανάλυση	Μια τεχνική για τον εντοπισμό απειλών που δεν μπορούν να προσδιοριστούν χρησιμοποιώντας την τρέχουσα έκδοση των βάσεων δεδομένων της εφαρμογής Kaspersky. Σας επιτρέπει να

	βρείτε αρχεία που ενδέχεται να περιέχουν άγνωστο κακόβουλο λογισμικό ή μια νέα τροποποίηση γνωστού προγράμματος με κακόβουλο λογισμικό.
	Κατά τη σάρωση αρχείων για κακόβουλο κώδικα, η ευρετική ανάλυση εκτελεί οδηγίες στα εκτελέσιμα αρχεία. Ο αριθμός των οδηγιών που εκτελούνται από την ευρετική ανάλυση εξαρτώνται από το επίπεδο που καθορίζεται για την ευρετική ανάλυση. Το επίπεδο της ευρετικής ανάλυσης ορίζει την ισορροπία μεταξύ της πληρότητας αναζήτησης για νέες απειλές, το φορτίο στους πόρους του λειτουργικού συστήματος και τον χρόνο που απαιτείται για την ευρετική ανάλυση.
Σάρωση μόνο νέων και τροποποιημένων αρχείων	Σαρώνει μόνο νέα αρχεία και εκείνα τα αρχεία που έχουν τροποποιηθεί από την τελευταία φορά που σαρώθηκαν. Αυτό θα σας επιτρέψει να εξοικονομήσετε χρόνο κατά τη σάρωση. Αυτή η λειτουργία σάρωσης ισχύει για απλά, αλλά και για σύνθετα αρχεία.
Σάρωση αρχειοθηκών	Σαρώνει αρχεία με τις ακόλουθες μορφές: RAR, ARJ, ZIP, CAB, LHA, JAR και ICE.
Πακέτα διανομής σάρωσης	Το πλαίσιο ελέγχου ενεργοποιεί/απενεργοποιεί τη σάρωση πακέτων διανομής τρίτου μέρους.
Σάρωση αρχείων με μορφές Microsoft Office	Σαρώνει αρχεία του Microsoft Office (DOC, DOCX, XLS, PPT και άλλες επεκτάσεις της Microsoft). Τα αρχεία μορφής Office περιλαμβάνουν επίσης αντικείμενα OLE.
Να μην αποσυμπιέζονται σύνθετα αρχεία μεγάλου μεγέθους Μέγιστο μέγεθος αρχείου	Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, τότε το Kaspersky Total Security δεν σαρώνει σύνθετα αρχεία που είναι μεγαλύτερα από την καθορισμένη τιμή.
	Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security σαρώνει τα σύνθετα αρχεία οποιουδήποτε μεγέθους.
	Το Kaspersky Total Security σαρώνει μεγάλα αρχεία που εξάγονται από αρχειοθήκες ανεξάρτητα από το εάν το πλαίσιο ελέγχου είναι επιλεγμένο ή όχι.
Εξαγωγή σύνθετων αρχείων στο παρασκήνιο	Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security παρέχει πρόσβαση σε σύνθετα αρχεία που είναι μεγαλύτερα από την καθορισμένη τιμή πριν από τη σάρωση των συγκεκριμένων αρχείων. Σε αυτήν την περίπτωση, το Kaspersky
νιεγιστο μεγεθος αρχείου	τοται Security αποσυμπιεζει και σαρώνει συνθετά άρχεια στο παρασκήνιο.

	Το Kaspersky Total Security παρέχει πρόσβαση σε σύνθετα αρχεία που είναι μικρότερα από αυτήν την τιμή μόνο μετά την αποσυμπίεση και τη σάρωση των συγκεκριμένων αρχείων.
	Εάν έχει καταργηθεί αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security παρέχει πρόσβαση σε σύνθετα αρχεία μόνο μετά την αποσυμπίεση και τη σάρωση των αρχείων, ανεξάρτητα από το μέγεθός τους.
Λειτουργία σάρωσης	Έξυπνη λειτουργία . Σε αυτήν τη λειτουργία, η Προστασία αρχείων από ιούς σαρώνει ένα αντικείμενο βάσει της ανάλυσης των ενεργειών που εκτελούνται στο αντικείμενο. Για παράδειγμα, όταν εργάζεστε με ένα έγγραφο του Microsoft Office, το Kaspersky Total Security σαρώνει το αρχείο την πρώτη φορά που ανοίγει και την τελευταία φορά που κλείνει. Οι ενδιάμεσες λειτουργίες που αντικαθιστούν το αρχείο δεν οδηγούν σε σάρωσή του.
	γινεται αποπειρα ανοιγματος η τροποποιησης τους. Πρόσβαση . Σε αυτήν τη λειτουργία, η Προστασία αρχείων από ιούς σαρώνει αντικείμενα μόνο κατόπιν απόπειρας ανοίγματός τους
	Εκτέλεση . Σε αυτήν τη λειτουργία, η Προστασία αρχείων από ιούς σαρώνει αντικείμενα μόνο κατόπιν απόπειρας εκτέλεσής τους.
Τεχνολογία iSwift	Εκτέλεση . Σε αυτήν τη λειτουργία, η Προστασία αρχείων από ιούς σαρώνει αντικείμενα μόνο κατόπιν απόπειρας εκτέλεσής τους. Αυτή η τεχνολογία αποτελεί εξέλιξη της τεχνολογίας iChecker για υπολογιστές που χρησιμοποιούν το σύστημα αρχείων NTFS. Η τεχνολογία iSwift έχει περιορισμούς: δεσμεύεται σε μια συγκεκριμένη θέση αρχείου στο σύστημα αρχείων και λειτουργεί μόνο σε αντικείμενα στο σύστημα αρχείων NTFS.
Τεχνολογία iSwift Τεχνολογία iChecker	 Εκτέλεση. Σε αυτήν τη λειτουργία, η Προστασία αρχείων από ιούς σαρώνει αντικείμενα μόνο κατόπιν απόπειρας εκτέλεσής τους. Αυτή η τεχνολογία αποτελεί εξέλιξη της τεχνολογίας iChecker για υπολογιστές που χρησιμοποιούν το σύστημα αρχείων NTFS. Η τεχνολογία iSwift έχει περιορισμούς: δεσμεύεται σε μια συγκεκριμένη θέση αρχείου στο σύστημα αρχείων και λειτουργεί μόνο σε αντικείμενα στο σύστημα αρχείων NTFS. Αυτή η τεχνολογία καθιστά εφικτή την αύξηση της ταχύτητας σάρωσης, εξαιρώντας συγκεκριμένα αρχεία από τη σάρωση. Η εξαίρεση αρχείων από τη σάρωση γίνεται με βάση έναν ειδικό αλγόριθμο, ο οποίος λαμβάνει υπόψη την ημερομηνία έκδοσης των βάσεων δεδομένων του Kaspersky Total Security, την ημερομηνία της πιο πρόσφατης σάρωσης του αρχείου και τυχόν τροποποιήσεις που έχουν πραγματοποιηθεί στις ρυθμίσεις σάρωσης. Η τεχνολογία iChecker έχει περιορισμούς: δεν λειτουργεί με μεγάλα αρχεία και εφαρμόζεται μόνο στα αρχεία με δομή που αναγνωρίζει η εφαρμογή (για παράδειγμα, ΕΧΕ, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP και RAR).

	Για να καθορίσετε εξαιρέσεις, κάντε κλικ στη σύνδεση Διαχείριση εξαιρέσεων στο παράθυρο Εξαιρέσεις .
Παύση Προστασίας αρχείων από ιούς	Αυτή η επιλογή διακόπτει προσωρινά και αυτόματα τη λειτουργία της Προστασίας αρχείων από ιούς κατά την καθορισμένη ώρα ή κατά την εργασία με τις καθορισμένες εφαρμογές.
	Αυτή η επιλογή διαμορφώνεται κάνοντας κλικ στη σύνδεση Παύση της Προστασίας αρχείων από ιούς .

Ρυθμίσεις προστασίας AMSI

Ρυθμίσεις	Περιγραφή
Σάρωση αρχειοθηκών	Σαρώνει αρχεία με τις ακόλουθες μορφές: RAR, ARJ, ZIP, CAB, LHA, JAR και ICE.
Πακέτα διανομής σάρωσης	Το πλαίσιο ελέγχου ενεργοποιεί/απενεργοποιεί τη σάρωση πακέτων διανομής τρίτου μέρους.
Σάρωση αρχείων με μορφές Microsoft Office	Σαρώνει αρχεία του Microsoft Office (DOC, DOCX, XLS, PPT και άλλες επεκτάσεις της Microsoft). Τα αρχεία μορφής Office περιλαμβάνουν επίσης αντικείμενα OLE.
Να μην αποσυμπιέζονται σύνθετα αρχεία μενάλου μενέθους	Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, τότε το Kaspersky Total Security δεν σαρώνει σύνθετα αρχεία που είναι μεγαλύτερα από την καθορισμένη τιμή.
Μέγιστο μέγεθος αρχείου	Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security σαρώνει τα σύνθετα αρχεία οποιουδήποτε μεγέθους.
	Το Kaspersky Total Security σαρώνει μεγάλα αρχεία που εξάγονται από αρχειοθήκες ανεξάρτητα από το εάν το πλαίσιο ελέγχου είναι επιλεγμένο ή όχι.

Παράθυρο Προσθήκη / Επεξεργασία προσωπικών δεδομένων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Τύποι προσωπικών δεδομένων</u> ?

Όταν κάνετε κλικ στους συνδέσμους στο πεδίο **Όνομα πεδίου**, εμφανίζεται ο αντίστοιχος τύπος προσωπικών δεδομένων.

Περιγραφή που εμφανίζεται στη λίστα με τις εγγραφές προσωπικών δεδομένων (για παράδειγμα, *Τηλέφωνο οικίας, Τηλέφωνο εργασίας* ή *Ταχ. κωδικός*).

Μπορείτε να αντιγράψετε την περιγραφή των προσωπικών δεδομένων αυτόματα, κάνοντας κλικ στον σχετικό σύνδεσμο με τον τύπο προσωπικών δεδομένων.

<u>Τιμή</u> ?

Προσωπικά δεδομένα για τα οποία η αποστολή αποκλείεται ή επιτρέπεται.

Αναφορά για τη μεταφορά προσωπικών δεδομένων

Ανάπτυξη όλων | Σύμπτυξη όλων

Το επάνω μέρος του παραθύρου εμφανίζει το όνομα του λογαριασμού χρήστη, οι ενέργειες του οποίου αναφέρονται στο συγκεκριμένο παράθυρο.

Έλεγχος ενεργοποιημένος / απενεργοποιημένος 🛛 🔿 / 🔵

Αυτός ο διακόπτης καθιστά εφικτή την ενεργοποίηση / απενεργοποίηση των ενεργειών του χρήστη μέσω του Γονικού ελέγχου.

Ανάλογα με το εάν ο Γονικός έλεγχος παρακολουθεί τις ενέργειες του χρήστη, το κουμπί αυτό μπορεί να εμφανίζεται ως εξής:



– Ο Γονικός έλεγχος παρακολουθεί τις ενέργειες του χρήστη.

– Ο Γονικός έλεγχος δεν παρακολουθεί τις ενέργειες του χρήστη.

Η παρακολούθηση των ενεργειών του χρήστη πραγματοποιείται σύμφωνα με τις ρυθμίσεις Γονικού ελέγχου που έχουν οριστεί για τον συγκεκριμένο χρήστη.

Σε αυτό το παράθυρο, μπορείτε να δείτε πληροφορίες σχετικά με τη χρήση λέξεων-κλειδιών και τις προσπάθειες μετάδοσης προσωπικών δεδομένων από τον επιλεγμένο χρήστη.

<u>Σήμερα</u> ?

Κάνοντας κλικ σε αυτό το κουμπί ανοίγει η αναφορά σχετικά με τη δραστηριότητα του χρήστη για την τρέχουσα ημέρα.



Κάνοντας κλικ σε αυτά τα κουμπιά ανοίγουν οι αναφορές για τις προηγούμενες και επόμενες περιόδους.

Ημέρα / Εβδομάδα / Μήνας 🖓

Χρονική περίοδος για την οποία δημιουργείται μια αναφορά. Μπορείτε να δημιουργήσετε αναφορά για τις παρακάτω περιόδους: ημέρα, εβδομάδα και μήνας.

<u>Κουμπί</u> ?

Κάνοντας κλικ σε αυτό το κουμπί ανοίγει το παράθυρο ρυθμίσεων Γονικού ελέγχου, στο οποίο εμφανίζεται η ενότητα **Έλεγχος περιεχομένου**. Σε αυτή την ενότητα μπορείτε να επιβάλετε περιορισμούς στην αποστολή προσωπικών δεδομένων.

<u>Λίστα αποκλεισμένων προσωπικών δεδομένων 💿</u>

Περιέχει τη λίστα των προσωπικών δεδομένων από μηνύματα που στάλθηκαν και λήφθηκαν από τον επιλεγμένο χρήστη κατά το καθορισμένο διάστημα.

<u>Δεδομένα</u> ?

Η στήλη αυτή περιλαμβάνει προσωπικά δεδομένα από απεσταλμένα ή ληφθέντα μηνύματα.

Για τον αποκλεισμό προσωπικών δεδομένων, προσδιορίζεται ο τύπος πληροφοριών των οποίων η μεταφορά θα αποκλειστεί.

<u>Πόρος</u> ?

Αυτή η στήλη εμφανίζει την τοποθεσία web μέσω της οποίας ο χρήστης επιχείρησε να στείλει ή να λάβει ένα μήνυμα με προσωπικά δεδομένα η μεταφορά των οποίων έχει αποκλειστεί.

<u>Κατάσταση</u> 🕐

Εάν η αποστολή του μηνύματος έχει αποκλειστεί από τον Γονικό έλεγχο, η στήλη εμφανίζει την τιμή *Αποκλεισμένο*.

<u>Ημερομηνία</u> 🕐

Αυτή η στήλη εμφανίζει την ημερομηνία λήψης ή αποστολής του μηνύματος που περιέχει προσωπικά δεδομένα των οποίων η μεταφορά έχει αποκλειστεί.

Επιλογή ενός προφίλ χρήστη

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Συλλογή δεδομένων</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το προφίλ εφαρμόζεται με τις προεπιλεγμένες ρυθμίσεις στο λογαριασμό του επιλεγμένου χρήστη. Το προφίλ αυτό συλλέγει μόνο στατιστικά στοιχεία σχετικά με τις ενέργειες του επιλεγμένου χρήστη. Δεν έχουν οριστεί περιορισμοί σχετικά με τη χρήση εφαρμογών και Διαδικτύου.

<u>Προσαρμοσμένοι περιορισμοί</u> 🖓

Οι ρυθμίσεις που ορίστηκαν χειροκίνητα εφαρμόζονται στο λογαριασμό του επιλεγμένου χρήστη.

<u>Προφίλ παιδιού (4+)</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, εφαρμόζεται το προφίλ που προορίζεται για παιδιά 4 έως 12 ετών στο λογαριασμό του επιλεγμένου χρήστη. Αυτό το προφίλ παρέχει τους ακόλουθους κανόνες για τη χρήση του Διαδικτύου και των εφαρμογών:

- Επιτρέπεται χρήση του Διαδικτύου.
- Η περιήγηση επιτρέπεται μόνο σε δικτυακούς τόπους που κατατάσσονται στις κατηγορίες "Διαδικτυακή επικοινωνία" και "Παιχνίδια υπολογιστή".
- Η λήψη αρχείων όλων των τύπων είναι αποκλεισμένη.
- Η παρακολούθηση της χρήσης του υπολογιστή είναι ενεργοποιημένη. Δεν έχουν οριστεί περιορισμοί χρήσης του υπολογιστή.

- Η παρακολούθηση της χρήσης εφαρμογών είναι ενεργοποιημένη. Δεν έχουν επιβληθεί περιορισμοί στη χρήση του υπολογιστή.
- Είναι ενεργοποιημένη η παρακολούθηση της χρήσης για παιχνίδια. Οι περιορισμοί ρυθμίζονται σύμφωνα με το σύστημα αξιολόγησης.

<u>Προφίλ εφήβου (12+)</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, εφαρμόζεται το προφίλ που προορίζεται για παιδιά 12+ στο λογαριασμό του επιλεγμένου χρήστη. Αυτό το προφίλ παρέχει τους ακόλουθους κανόνες για τη χρήση του Διαδικτύου και των εφαρμογών:

- Επιτρέπεται χρήση του Διαδικτύου.
- Η περιήγηση επιτρέπεται μόνο σε δικτυακούς τόπους που κατατάσσονται στις κατηγορίες "Διαδικτυακή επικοινωνία", "Αγορές, τράπεζες, συστήματα πληρωμών" και "Παιχνίδια υπολογιστή".
- Η παρακολούθηση της χρήσης του υπολογιστή είναι ενεργοποιημένη. Δεν έχουν οριστεί περιορισμοί χρήσης του υπολογιστή.
- Η παρακολούθηση της χρήσης εφαρμογών είναι ενεργοποιημένη. Δεν έχουν επιβληθεί περιορισμοί στη χρήση του υπολογιστή.
- Είναι ενεργοποιημένη η παρακολούθηση της χρήσης για παιχνίδια. Οι περιορισμοί ρυθμίζονται σύμφωνα με το σύστημα αξιολόγησης.

Προεπιλεγμένες ρυθμίσεις 🖓

Κάνοντας κλικ σε αυτό το κουμπί, το προφίλ εφαρμόζεται με τις προεπιλεγμένες ρυθμίσεις στο λογαριασμό του επιλεγμένου χρήστη. Αυτό το προφίλ παρέχει τους ακόλουθους κανόνες για τη χρήση του Διαδικτύου και των εφαρμογών:

- Επιτρέπεται χρήση του Διαδικτύου.
- Η περιήγηση επιτρέπεται μόνο σε δικτυακούς τόπους που κατατάσσονται στις κατηγορίες "Διαδικτυακή επικοινωνία", "Αγορές, τράπεζες, συστήματα πληρωμών" και "Παιχνίδια υπολογιστή".
- Είναι ενεργοποιημένη η Ασφαλής αναζήτηση.

- Η παρακολούθηση της χρήσης του υπολογιστή είναι ενεργοποιημένη. Δεν έχουν οριστεί περιορισμοί χρήσης του υπολογιστή.
- Η παρακολούθηση της χρήσης εφαρμογών είναι ενεργοποιημένη. Δεν έχουν επιβληθεί περιορισμοί στη χρήση του υπολογιστή.
- Είναι ενεργοποιημένη η παρακολούθηση της έναρξης παιχνιδιών, δεν έχουν οριστεί περιορισμοί στην έναρξη.
- Είναι ενεργοποιημένη η παρακολούθηση κρυπτογραφημένων συνδέσεων SSL στα προγράμματα περιήγησης.

<u>Εισαγωγή</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο για την επιλογή ενός αρχείου που περιέχει τις ρυθμίσεις Γονικού ελέγχου. Αφού επιλέξετε το αρχείο, αυτές οι ρυθμίσεις εφαρμόζονται στο λογαριασμό του επιλεγμένου χρήστη.

<u>Εξαγωγή</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο για την αποθήκευση των τρεχουσών ρυθμίσεων Γονικού ελέγχου στο αρχείο.

Παράθυρο Προσθήκη / Επεξεργασία διεύθυνσης web

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Μάσκα διεύθυνσης web</u> ?

Η διεύθυνση web ή η μάσκα διεύθυνσης του δικτυακού τόπου, η πρόσβαση στην οποία θα πρέπει να αποκλειστεί ή να επιτρέπεται.

<u>Ενέργεια</u> ?

Μπορείτε να το χρησιμοποιήσετε για να αποκλείσετε ή να επιτρέψετε την πρόσβαση των χρηστών σε δικτυακούς τόπους.

Μπορείτε να επιλέξετε μία από τις παρακάτω επιλογές:

- Να επιτρέπεται. Εάν επιλέξετε αυτό το στοιχείο επιλογής, ο Γονικός έλεγχος επιτρέπει την πρόσβαση των χρηστών στο δικτυακό τόπο ακόμη κι αν ανήκει σε μια αποκλεισμένη κατηγορία ή εάν έχει ενεργοποιηθεί ο αποκλεισμός όλων των δικτυακών τόπων.
- Αποκλεισμός. Εάν επιλέξετε αυτό το στοιχείο, ο Γονικός έλεγχος αποκλείει την πρόσβαση του χρήστη στο δικτυακό τόπο, ακόμη και αν ανήκει σε επιτρεπόμενη κατηγορία.

<u>Τύπος</u> ?

Μπορείτε να προσδιορίσετε το πεδίο στο οποίο θα εφαρμοστούν οι ρυθμίσεις πρόσβασης του δικτυακού τόπου.

Μπορείτε να επιλέξετε μία από τις παρακάτω επιλογές:

 Μάσκα τοποθεσίας web. Εάν ενεργοποιήσετε αυτή την επιλογή, ο Γονικός έλεγχος επιτρέπει ή αποκλείει την πρόσβαση σε όλες τις ιστοσελίδες του καθορισμένου δικτυακού τόπου για το χρήστη.

Για παράδειγμα, εάν το πεδίο **Μάσκα διεύθυνσης web** περιέχει τη διεύθυνση example.com, ο Γονικός έλεγχος επιτρέπει ή αποκλείει την πρόσβαση σε όλους δικτυακούς τόπους του example.com, συμπεριλαμβανομένων των news.example.com, market.example.com και mail.example.com.

 Καθορισμένη διεύθυνση web. Εάν επιλέξετε αυτό το στοιχείο, ο Γονικός έλεγχος επιτρέπει ή αποκλείει την πρόσβαση μόνο στην καθορισμένη σελίδα του δικτυακού τόπου που υποδεικνύεται στο πεδίο Μάσκα διεύθυνσης web.

Για παράδειγμα, εάν καθορίσετε τη διεύθυνση URL mail.example.com/login στο πεδίο **Μάσκα διεύθυνσης web**, ο Γονικός έλεγχος επιτρέπει ή αποκλείει την πρόσβαση μόνο στην καθορισμένη σελίδα σύνδεσης που χρησιμοποιείται για τη σύνδεση στον λογαριασμό διαδικτυακού ηλεκτρονικού ταχυδρομείου. Ο κανόνας αυτός δεν θα ισχύει σε άλλες σελίδες του δικτυακού τόπου.

<u>Εφαρμογή προτύπου ?</u>

Επιτρέπει την εφαρμογή της εξαίρεσης σε ένα από τα υπάρχοντα πρότυπα με το καθορισμένο σύνολο ρυθμίσεων.

Μπορείτε να επιλέξετε μία από τις παρακάτω επιλογές:

 Ολόκληρη η τοποθεσία web – όταν αυτή η επιλογή είναι ενεργοποιημένη, ο Γονικός Έλεγχος επιτρέπει ή αποκλείει την πρόσβαση στον τομέα που έχει καθοριστεί στο πεδίο Μάσκα διεύθυνσης web. Για παράδειγμα, εάν το πεδίο **Μάσκα διεύθυνσης web** περιέχει τη διεύθυνση example.com, ο Γονικός έλεγχος θα επιτρέπει ή θα αποκλείει την πρόσβαση σε όλους δικτυακούς τόπους του τομέα example.com, συμπεριλαμβανομένων των news.example.com, market.example.com και mail.example.com.

- Καθορισμένη ιστοσελίδα όταν αυτή η επιλογή είναι ενεργοποιημένη, ο Γονικός Έλεγχος επιτρέπει ή αποκλείει την πρόσβαση στη συγκεκριμένη σελίδα που υποδεικνύεται στο πεδίο Μάσκα διεύθυνσης web και σε όλες τις διευθύνσεις web που περιέχουν τη συγκεκριμένη σελίδα. Για παράδειγμα, εάν το πεδίο Μάσκα διεύθυνσης web περιέχει τη διεύθυνση example.com/hl, ο Γονικός Έλεγχος θα επιτρέπει ή θα αποκλείει την πρόσβαση στη συγκεκριμένη σελίδα, καθώς και σε όλες τις διευθύνσεις web που την περιέχουν, όπως example.com/hl/example1.html.
- Καθορισμένη διεύθυνση web όταν αυτή η επιλογή είναι ενεργοποιημένη, ο Γονικός Έλεγχος επιτρέπει ή αποκλείει την πρόσβαση στην καθορισμένη διεύθυνση web που υποδεικνύεται στο πεδίο Μάσκα διεύθυνσης web. Για παράδειγμα, εάν καθορίσετε τη διεύθυνση URL mail.example.com/login στο πεδίο Μάσκα διεύθυνσης web, ο Γονικός έλεγχος επιτρέπει ή αποκλείει την πρόσβαση μόνο στην καθορισμένη σελίδα σύνδεσης που χρησιμοποιείται για τη σύνδεση στον λογαριασμό διαδικτυακού ηλεκτρονικού ταχυδρομείου. Ο κανόνας αυτός δεν θα ισχύει σε άλλες σελίδες του δικτυακού τόπου.

Εξαιρέσεις Γονικού ελέγχου

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

Σε αυτό το παράθυρο, μπορείτε να δημιουργήσετε μία λίστα εξαιρέσεων από τις διαμορφωμένες ρυθμίσεις Γονικού ελέγχου. Ρυθμίσεις πρόσβασης οι οποίες επηρεάζουν τους δικτυακούς τόπους που προστίθενται στη λίστα εξαιρέσεων κατά τον αποκλεισμό δικτυακών τόπων κατά κατηγορία (κουμπί **Αποκλεισμός πρόσβασης σε τοποθεσίες web** επιλεγμένων κατηγοριών) και κατά τον αποκλεισμό όλων των δικτυακών τόπων (κουμπί **Αποκλεισμός πρόσβασης σε όλες τις τοποθεσίες web**).

Για παράδειγμα, μπορείτε να επιτρέψετε την πρόσβαση σε τοποθεσίες web από την κατηγορία "Διαδικτυακή επικοινωνία", αλλά θα πρέπει να προσθέσετε το www.example.com στον κατάλογο των εξαιρέσεων για να αποκλείσετε την πρόσβαση στη συγκεκριμένη τοποθεσία web. Στην περίπτωση αυτή, ο Γονικός έλεγχος επιτρέπει την πρόσβαση σε όλα τα κοινωνικά δίκτυα, εκτός από τα μέσα κοινωνικής δικτύωσης example.com. Μπορείτε επίσης να αποκλείσετε όλους τους δικτυακούς τόπους και να προσθέσετε έναν δικτυακό τόπο διαδικτυακού ηλεκτρονικού ταχυδρομείου στη λίστα των εξαιρέσεων για να επιτρέπεται η πρόσβαση σε αυτόν. Στην περίπτωση αυτή, ο Γονικός έλεγχος επιτρέπει στο χρήστη να έχει πρόσβαση σε αυτόν.

Η λίστα περιλαμβάνει τις διευθύνσεις web, η πρόσβαση στις οποίες επιτρέπεται ή αποκλείεται ανεξάρτητα από τις ρυθμίσεις του Γονικού ελέγχου.

Από το μενού περιβάλλοντος της διεύθυνσης web στη λίστα, μπορείτε να αλλάξετε την διεύθυνση web ή να την αφαιρέσετε από τη λίστα και να επιτρέψετε ή να αποκλείσετε την πρόσβαση στον δικτυακό τόπο.

<u>Μάσκα διεύθυνσης web</u> ?

Η διεύθυνση web ή η μάσκα διεύθυνσης ενός δικτυακού τόπου στον οποίο επιτρέπεται ή αποκλείεται η πρόσβαση.

<u>Τύπος</u> ?

Η Στήλη εμφανίζει το πεδίο στο οποίο εφαρμόζονται οι ρυθμίσεις πρόσβασης του δικτυακού τόπου.

Εάν στη στήλη εμφανίζεται η επιλογή *Μάσκα δικτυακού τόπου*, επιτρέπεται ή αποκλείεται η πρόσβαση σε όλες τις ιστοσελίδες του δικτυακού τρόπου.

Εάν στη στήλη εμφανίζεται η επιλογή *Καθορισμένη διεύθυνση web*, επιτρέπεται ή αποκλείεται η πρόσβαση μόνο στη συγκεκριμένη ιστοσελίδα του δικτυακού τόπου.

<u>Ενέργεια</u> ?

Αυτή η στήλη δείχνει αν η πρόσβαση στο δικτυακό τόπο επιτρέπεται ή αποκλείεται.

Εάν στη στήλη εμφανίζεται η επιλογή *Επιτράπηκε(-αν)*, ο Γονικός έλεγχος επιτρέπει την πρόσβαση στο δικτυακό τόπο.

Εάν στη στήλη εμφανίζεται η επιλογή *Αποκλεισμένο*, ο Γονικός έλεγχος αποκλείει την πρόσβαση στο δικτυακό τόπο.

<u>Επεξεργασία</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο **Επεξεργασία** από το οποίο μπορείτε να επεξεργαστείτε τη μάσκα διεύθυνσης web ή τη διεύθυνση web του δικτυακού τόπου που έχει επιλεγεί στη λίστα εξαιρέσεων και στις ρυθμίσεις πρόσβασης στον δικτυακό τόπο. Το κουμπί είναι διαθέσιμο εάν έχει επιλεγεί μάσκα διεύθυνσης web στη λίστα εξαιρέσεων.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, η επιλεγμένη μάσκα διεύθυνσης web καταργείται από τη λίστα των εξαιρέσεων.

Το κουμπί είναι διαθέσιμο εάν έχει επιλεγεί μάσκα διεύθυνσης web στη λίστα εξαιρέσεων.

<u>Προσθήκη</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο για την προσθήκη μάσκας διεύθυνσης δικτυακού τόπου, στο οποίο μπορείτε να προσθέσετε τη διεύθυνση του δικτυακού τόπου ή τη μάσκα διεύθυνσης του δικτυακού τόπου στη λίστα εξαιρέσεων.

Παράθυρο περιορισμών χρήσης εφαρμογών

Ανάπτυξη όλων | Σύμπτυξη όλων

Σε αυτό το παράθυρο, μπορείτε να επιβάλετε περιορισμούς στο χρόνο χρήσης μιας επιλεγμένης εφαρμογής.

Στην ενότητα **Εργάσιμες**, μπορείτε να περιορίσετε το χρόνο χρήσης της εφαρμογής τις καθημερινές.

<u>Να επιτρέπεται η πρόσβαση το πολύ <N> ώρες την ημέρα 🖓</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί ένα χρονικό όριο χρήσης της εφαρμογής κατά τις καθημερινές.

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, ο Γονικός έλεγχος περιορίζει το συνολικό χρόνο χρήσης της εφαρμογής για τον επιλεγμένο χρήστη. Το χρονικό όριο για τη χρήση της εφαρμογής καθορίζεται (σε ώρες) στην αναπτυσσόμενη λίστα δίπλα στο πλαίσιο ελέγχου.

Εάν το πλαίσιο ελέγχου δεν είναι επιλεγμένο, ο Γονικός έλεγχος δεν περιορίζει τη χρήση της εφαρμογής τις καθημερινές.

Στην ενότητα **Σαββατοκύριακα**, μπορείτε να περιορίσετε το χρόνο χρήσης της εφαρμογής τα σαββατοκύριακα.

<u>Να επιτρέπεται η πρόσβαση το πολύ <N> ώρες την ημέρα</u> ?

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί ένα χρονικό όριο χρήσης της εφαρμογής κατά τα σαββατοκύριακα.

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, ο Γονικός έλεγχος περιορίζει το συνολικό χρόνο χρήσης της εφαρμογής για τον επιλεγμένο χρήστη. Το χρονικό όριο για τη χρήση της εφαρμογής καθορίζεται (σε ώρες) στην αναπτυσσόμενη λίστα δίπλα στο πλαίσιο ελέγχου.

Εάν το πλαίσιο ελέγχου δεν είναι επιλεγμένο, ο Γονικός έλεγχος δεν περιορίζει τη χρήση της εφαρμογής τα σαββατοκύριακα.

Στην ενότητα **Διαλείμματα** μπορείτε να ορίσετε τον περιοδικό αποκλεισμό της πρόσβασης στην εφαρμογή κατά τη διάρκεια της ημέρας.

<u>Διάλειμμα κάθε <N> ώρες για <N λεπτά> 🖓</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την περιοδική φραγή της εφαρμογής στο καθορισμένο χρονικό διάστημα για να διασφαλιστεί ότι ο χρήστης κάνει διάλειμμα από τη χρήση.

Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, ο Γονικός έλεγχος αποκλείει την εφαρμογή στο διάστημα που ορίζεται στην αναπτυσσόμενη λίστα **<HH:MM>**. Η διάρκεια του αποκλεισμού της πρόσβασης επιλέγεται από την αναπτυσσόμενη λίστα **<Ν λεπτά>**.

Η ενότητα **Ακριβής χρόνος χρήσης** εμφανίζει έναν πίνακα με τον χρόνο χρήσης της εφαρμογής. Χρησιμοποιώντας αυτόν τον πίνακα, μπορείτε να ορίσετε ένα ωριαίο χρονοδιάγραμμα για τη χρήση της εφαρμογής καθ' όλη τη διάρκεια της εβδομάδας.

<u>Πίνακας χρόνου χρήσης της εφαρμογής</u> ව

Μπορείτε να χρησιμοποιήσετε αυτόν τον πίνακα για να καθορίσετε τις ημέρες της εβδομάδας και τις ώρες κατά τις οποίες ο χρήστης επιτρέπεται να χρησιμοποιεί την εφαρμογή. Οι σειρές του πίνακα αντιστοιχούν στις ημέρες της εβδομάδας, ενώ οι στήλες του πίνακα αντιστοιχούν σε διαστήματα 1 ώρας στην κλίμακα του χρόνου. Ανάλογα με τις τοπικές ρυθμίσεις του λειτουργικού συστήματος, η κλίμακα χρόνου μπορεί να εμφανίζεται σε 24-ωρη ή 12-ωρη μορφή. Τα χρώματα στα κελιά του πίνακα υποδεικνύουν τους περιορισμούς που είναι σε ισχύ: το κόκκινο σημαίνει ότι η χρήση της εφαρμογής είναι μπλοκαρισμένη και το γκρι σημαίνει ότι η χρήση της εφαρμογής επιτρέπεται. Κάνοντας κλικ σε ένα κελί του πίνακα, αλλάζει το χρώμα του. Όταν τοποθετείτε τον δείκτη του ποντικιού επάνω από ένα κελί, εμφανίζεται το χρονικό διάστημα που αντιστοιχεί στο εν λόγω κελί κάτω από τον πίνακα.

Παράθυρο Λίστα προσωπικών δεδομένων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Λίστα προσωπικών δεδομένων</u> ව

Αυτή η λίστα περιέχει προσωπικά δεδομένα του χρήστη για τα οποία η αποστολή πρέπει να ελέγχεται.

<u>Όνομα πεδίου</u> 🕐

Αυτή η στήλη δείχνει τον τύπο προσωπικών δεδομένων (για παράδειγμα, Αριθμός τραπεζικής κάρτας ή Τηλέφωνο σπιτιού).

<u>Τιμή</u> ?

Αυτή η στήλη περιέχει προσωπικά δεδομένα (για παράδειγμα, ένας αριθμός τραπεζικής κάρτας ή αριθμός τηλεφώνου) που θέλετε να παρακολουθούνται στα μηνύματα.

<u>Επεξεργασία</u> ?

Κάνοντας κλικ σε αυτό το κουμπί ανοίγει ένα παράθυρο στο οποίο μπορείτε να επεξεργαστείτε μια εγγραφή με προσωπικά δεδομένα.

Εάν κάνετε κλικ σε αυτό το κουμπί, μπορείτε να καταργήσετε την εγγραφή προσωπικών δεδομένων από τη λίστα.

<u>Προσθήκη</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο, στο οποίο μπορείτε να προσθέσετε μια νέα εγγραφή στη λίστα προσωπικών δεδομένων.

Αναφορά αποκλ. δικτ. τόπων και λήψ. αρχείων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Σήμερα</u> ?

Κάνοντας κλικ σε αυτό το κουμπί ανοίγει η αναφορά σχετικά με τη δραστηριότητα του χρήστη για την τρέχουσα ημέρα.



Κάνοντας κλικ σε αυτά τα κουμπιά ανοίγουν οι αναφορές για τις προηγούμενες και επόμενες περιόδους.

Ημέρα / Εβδομάδα / Μήνας 🖓

Χρονική περίοδος για την οποία δημιουργείται μια αναφορά. Μπορείτε να δημιουργήσετε αναφορά για τις παρακάτω περιόδους: ημέρα, εβδομάδα και μήνας.



Κάνοντας κλικ σε αυτό το κουμπί ανοίγει το παράθυρο ρυθμίσεων Γονικού ελέγχου, στο οποίο εμφανίζεται η ενότητα **Διαδίκτυο**. Σε αυτή την ενότητα μπορείτε να επιβάλετε περιορισμούς για τον χρόνο χρήσης του Διαδικτύου, την πρόσβαση σε δικτυακούς τόπους και τις λήψεις αρχείων για τον επιλεγμένο χρήστη. Αυτή η λίστα περιέχει τους δικτυακούς τόπους που έχουν αποκλειστεί από τον Γονικό έλεγχο και τα αρχεία η λήψη των οποίων έχει αποκλειστεί.

Η λίστα περιέχει τα παρακάτω δεδομένα:

- Όνομα αποκλεισμένου δικτυακού τόπου ή αρχείου
- Αιτία για την οποία η προσπάθεια εφαρμογής αποκλείστηκε για τον χρήστη (για παράδειγμα, Δικτυακός τόπος από αποκλεισμένη κατηγορία)
- Ημερομηνία ανοίγματος του δικτυακού τόπου ή λήψης του αρχείου

Αναφορά χρήσης εφαρμογών

Ανάπτυξη όλων | Σύμπτυξη όλων

Το επάνω μέρος του παραθύρου εμφανίζει το όνομα του λογαριασμού χρήστη, οι ενέργειες του οποίου αναφέρονται στο συγκεκριμένο παράθυρο.

Έλεγχος ενεργοποιημένος / απενεργοποιημένος 🛛 🚺 / 🔵

Αυτός ο διακόπτης καθιστά εφικτή την ενεργοποίηση / απενεργοποίηση των ενεργειών του χρήστη μέσω του Γονικού ελέγχου.

Ανάλογα με το εάν ο Γονικός έλεγχος παρακολουθεί τις ενέργειες του χρήστη, το κουμπί αυτό μπορεί να εμφανίζεται ως εξής:



) – Ο Γονικός έλεγχος παρακολουθεί τις ενέργειες του χρήστη.

– Ο Γονικός έλεγχος δεν παρακολουθεί τις ενέργειες του χρήστη.

Η παρακολούθηση των ενεργειών του χρήστη πραγματοποιείται σύμφωνα με τις ρυθμίσεις Γονικού ελέγχου που έχουν οριστεί για τον συγκεκριμένο χρήστη.

Στο παράθυρο **Αναφορά χρήσης εφαρμογών**, μπορείτε να δείτε πληροφορίες σχετικά με την εκκίνηση εφαρμογών κατά τη διάρκεια ενός καθορισμένου χρονικού διαστήματος για έναν επιλεγμένο λογαριασμό.

<u>Σήμερα</u> ?

Κάνοντας κλικ σε αυτό το κουμπί ανοίγει η αναφορά σχετικά με τη δραστηριότητα του χρήστη για την τρέχουσα ημέρα.



Κάνοντας κλικ σε αυτά τα κουμπιά ανοίγουν οι αναφορές για τις προηγούμενες και επόμενες περιόδους.

Ημέρα / Εβδομάδα / Μήνας 🖓

Χρονική περίοδος για την οποία δημιουργείται μια αναφορά. Μπορείτε να δημιουργήσετε αναφορά για τις παρακάτω περιόδους: ημέρα, εβδομάδα και μήνας.

<u>Κουμπί</u> ?

Κάνοντας κλικ σε αυτό το κουμπί ανοίγει το παράθυρο ρυθμίσεων Γονικού ελέγχου, στο οποίο εμφανίζεται η ενότητα **Εφαρμογές**. Σε αυτή την ενότητα μπορείτε να επιβάλετε περιορισμούς για την εκκίνηση και τη χρήση των εφαρμογών.

Εφαρμογές που χρησιμοποιούνται συχνά 🖓

Περιέχει μια λίστα με τις εφαρμογές που έχουν εκκινηθεί πιο συχνά από το χρήστη εντός της καθορισμένης προθεσμίας. Η λίστα περιγράφει επίσης τη διάρκεια χρήσης κάθε εφαρμογής.

<u>Αποκλεισμένες εφαρμογές 🖓</u>

Περιέχει μια λίστα με τις εφαρμογές, η εκκίνηση των οποίων έχει αποκλειστεί από το Γονικό έλεγχο. Οι εφαρμογές εμφανίζονται με χρονολογική σειρά, με αυτές που έχουν ξεκινήσει πρόσφατα να εμφανίζονται στην κορυφή.

Κάνοντας κλικ στη σύνδεση **Περισσότερα <N>** μπορείτε να δείτε άλλες εφαρμογές, η εκκίνηση των οποίων έχει αποκλειστεί.

<u>Όλες οι χρησιμοποιούμενες εφαρμογές 🖻</u>

Περιέχει μια λίστα με εφαρμογές, τις οποίες έχει εκτελέσει ο χρήστης κατά την καθορισμένη περίοδο. Η λίστα περιγράφει επίσης τη διάρκεια χρήσης κάθε εφαρμογής.

Οι εφαρμογές ομαδοποιούνται σε κατηγορίες (για παράδειγμα, "Παιχνίδια" ή "Προγράμματα-πελάτη ΙΜ").

Κάνοντας κλικ στο κουμπί 🖉 μπορείτε να δείτε τη λίστα των εφαρμογών στην κατηγορία.

Κάνοντας κλικ στο κουμπί _> ελαχιστοποιείται η λίστα εφαρμογών στην κατηγορία σε μέγεθος μίας γραμμής.

Αποκλεισμός παιχνιδιών ανά κατηγορία

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

Σε αυτό το παράθυρο, μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε τον αποκλεισμό παιχνιδιών ανάλογα με το περιεχόμενό τους. Η ταξινόμηση του τύπου περιεχομένου των παιχνιδιών (το σύνολο των πλαισίων ελέγχου) αντιστοιχεί στις αξιολογήσεις PEGI ή ESRB. Ο τύπος ταξινόμησης παιχνιδιών επιλέγεται αυτόματα ανάλογα με την τοποθεσία σας. Εάν είναι απαραίτητο, μπορείτε να επιλέξετε τον τύπο ταξινόμησης των παιχνιδιών χειροκίνητα στις ρυθμίσεις του στοιχείου Γονικός Έλεγχος.

Εάν το πλαίσιο ελέγχου δίπλα σε μια κατηγορία είναι ενεργοποιημένο, ο Γονικός έλεγχος αποκλείει τα παιχνίδια που περιλαμβάνονται σε αυτή την κατηγορία.

Εάν το πλαίσιο ελέγχου δίπλα σε μια κατηγορία είναι απενεργοποιημένο, ο Γονικός έλεγχος επιτρέπει την έναρξη των παιχνιδιών αυτής της κατηγορίας.

Η έναρξη ενός παιχνιδιού επιτρέπεται εάν επιτρέπονται όλες οι κατηγορίες που αντιστοιχούν στο περιεχόμενο του παιχνιδιού.

Πληροφορίες για κατηγορίες τοποθεσιών web

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

Μπορείτε να <u>δείτε τις περιγραφές των κατηγοριών δικτυακών τόπων</u> ακολουθώντας τη σύνδεση.

Παράθυρο Ισχύς κωδικού πρόσβασης

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Διαχείριση Γονικού ελέγχου</u> 🖓

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την εμφάνιση της ειδοποίησης κωδικού πρόσβασης όταν ένας χρήστης επιχειρεί να ανοίξει το παράθυρο του Γονικού ελέγχου.

<u>Διαχείριση δημιουργίας αντιγράφων ασφαλείας 🖻</u>

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την επιλογή που ζητά από τον χρήστη τον κωδικό πρόσβασης για το άνοιγμα του παραθύρου **Δημιουργία αντιγράφων ασφαλείας**.

<u>Διαμόρφωση ρυθμίσεων εφαρμογής 💿</u>

Το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την εμφάνιση της ειδοποίησης κωδικού πρόσβασης όταν ένας χρήστης επιχειρεί να αποθηκεύσει αλλαγές στις ρυθμίσεις της εφαρμογής.

Το πλαίσιο ελέγχου αυτό είναι επιλεγμένο και ανενεργό εάν έχει επιλεγεί το πλαίσιο ελέγχου **Διαχείριση Γονικού ελέγχου**.

Έξοδος από την εφαρμογή ?

Το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την εμφάνιση της ειδοποίησης κωδικού πρόσβασης όταν ο χρήστης επιχειρεί να κλείσει την εφαρμογή.

Το πλαίσιο ελέγχου αυτό είναι επιλεγμένο και ανενεργό εάν έχει επιλεγεί το πλαίσιο ελέγχου **Διαχείριση Γονικού ελέγχου**.

<u>Κατάργηση της εφαρμογής</u> 🖓

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί την εμφάνιση της ειδοποίησης κωδικού πρόσβασης όταν ένας χρήστης επιχειρεί να καταργήσει την εφαρμογή.

Το πλαίσιο ελέγχου αυτό είναι επιλεγμένο και ανενεργό εάν έχει επιλεγεί το πλαίσιο ελέγχου **Διαχείριση Γονικού ελέγχου**.

<u>Δημιουργία κωδικού 🕐</u>

Κάνοντας κλικ σε αυτό το κουμπί, ενεργοποιείται η προστασία με χρήση κωδικού πρόσβασης για τον περιορισμό της πρόσβασης σε καθορισμένες λειτουργίες της εφαρμογής.

Γενικά στατιστικά στοιχεία

Ανάπτυξη όλων | Σύμπτυξη όλων

Το επάνω μέρος του παραθύρου εμφανίζει το όνομα του λογαριασμού χρήστη, οι ενέργειες του οποίου αναφέρονται στο συγκεκριμένο παράθυρο.

Έλεγχος ενεργοποιημένος / απενεργοποιημένος 🛛 🔵 / 🔵

Αυτός ο διακόπτης καθιστά εφικτή την ενεργοποίηση / απενεργοποίηση των ενεργειών του χρήστη μέσω του Γονικού ελέγχου.

Ανάλογα με το εάν ο Γονικός έλεγχος παρακολουθεί τις ενέργειες του χρήστη, το κουμπί αυτό μπορεί να εμφανίζεται ως εξής:



) – Ο Γονικός έλεγχος παρακολουθεί τις ενέργειες του χρήστη.

– Ο Γονικός έλεγχος δεν παρακολουθεί τις ενέργειες του χρήστη.

Η παρακολούθηση των ενεργειών του χρήστη πραγματοποιείται σύμφωνα με τις ρυθμίσεις Γονικού ελέγχου που έχουν οριστεί για τον συγκεκριμένο χρήστη.

<u>Προφίλ: <ρυθμίσεις προφίλ></u> ?

Κάνοντας κλικ στη σύνδεση, μπορείτε να προσαρμόσετε τις ρυθμίσεις Γονικού ελέγχου που εφαρμόζονται στον τρέχοντα λογαριασμό.

Στην ενότητα **Υπολογιστής**, μπορείτε να προβάλλετε το χρόνο χρήσης του υπολογιστή για τον επιλεγμένο χρήστη, να προβάλλετε την αναφορά χρήσης του υπολογιστή και να διαμορφώσετε τις ρυθμίσεις Γονικού ελέγχου. Τα στατιστικά στοιχεία χρήσης του υπολογιστή εμφανίζονται για το διάστημα που ορίζεται στην αναφορά σχετικά με τον χρόνο χρήσης του υπολογιστή. Από προεπιλογή, εμφανίζονται τα στατιστικά στοιχεία για τη χρήση των τελευταίων είκοσι τεσσάρων ωρών.

<u>Λεπτομέρειες ?</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Αναφορά χρήσης υπολογιστή**. Σε αυτό το παράθυρο, μπορείτε να δείτε πληροφορίες σχετικά με το χρόνο χρήσης του υπολογιστή από τον επιλεγμένο χρήστη.

<u>Ρυθμίσεις</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο. Σε αυτό το παράθυρο, μπορείτε να προσδιορίσετε τη χρονική περίοδο κατά την οποία ο επιλεγμένος χρήστης μπορεί να χρησιμοποιήσει τον υπολογιστή.

Στην ενότητα **Εφαρμογές**, μπορείτε να δείτε λεπτομέρειες για τις εφαρμογές που έχει χρησιμοποιήσει πρόσφατα ο επιλεγμένος χρήστης. Τα στατιστικά στοιχεία σχετικά με τη χρήση των εφαρμογών εμφανίζονται για το χρονικό διάστημα που καθορίζεται στην αναφορά χρήσης των εφαρμογών. Από προεπιλογή, εμφανίζονται τα στατιστικά στοιχεία για τη χρήση των τελευταίων είκοσι τεσσάρων ωρών.

<u>Λεπτομέρειες ?</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Αναφορά χρήσης εφαρμογών**. Αυτό το παράθυρο εμφανίζει λεπτομέρειες σχετικά με εφαρμογές που έχουν εκκινηθεί από τον επιλεγμένο χρήστη, καθώς και τον χρόνο χρήσης του.

<u>Ρυθμίσεις ?</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο. Σε αυτό το παράθυρο, μπορείτε να προσδιορίσετε τις εφαρμογές που μπορεί να χρησιμοποιεί ο επιλεγμένος χρήστης.

Η ενότητα **Διαδίκτυο** περιέχει στατιστικά στοιχεία σχετικά με τις επισκέψεις σε δικτυακούς τόπους, καθώς και μια αναφορά σχετικά με το χρόνο που ο χρήστης ξόδεψε στους εν λόγω δικτυακούς τόπους. Μπορείτε, επίσης, να προβάλετε τον συνολικό αριθμό των αποκλεισμένων προσπαθειών επίσκεψης στους αποκλεισμένους δικτυακούς τόπους.

Τα στατιστικά στοιχεία σχετικά με τους πόρους στον ιστό που επισκέφθηκε ο χρήστης εμφανίζονται για το διάστημα που ορίζεται στην αναφορά σχετικά με το χρόνο χρήσης του Διαδικτύου. Από προεπιλογή, εμφανίζονται τα στατιστικά στοιχεία για τη χρήση των τελευταίων είκοσι τεσσάρων ωρών.

<u>Λεπτομέρειες ?</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Αναφορά χρήσης** διαδικτύου. Σε αυτό το παράθυρο, μπορείτε να δείτε πληροφορίες σχετικά με τους διαδικτυακούς πόρους που επισκέφθηκε ο επιλεγμένος χρήστης.

<u>Ρυθμίσεις </u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο. Σε αυτό το παράθυρο, μπορείτε να προσδιορίσετε τη χρονική περίοδο κατά την οποία ο επιλεγμένος χρήστης μπορεί να χρησιμοποιήσει τον υπολογιστή.

Η ενότητα **Έλεγχος περιεχομένου** εμφανίζει πληροφορίες για τον αριθμό των αποκλεισμένων προσπαθειών για τη μετάδοση προσωπικών δεδομένων.

Αυτά τα στατιστικά εμφανίζονται για την περίοδο που ορίζεται στην αναφορά ελέγχου περιεχομένου. Από προεπιλογή, εμφανίζονται τα στατιστικά στοιχεία για μία εβδομάδα.

<u>Λεπτομέρειες </u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο. Σε αυτό το παράθυρο, μπορείτε να λάβετε πληροφορίες σχετικά με το ποια προσωπικά δεδομένα επιχείρησε να μεταδώσει ο χρήστης κατά την επικοινωνία στα κοινωνικά δίκτυα.

<u>Ρυθμίσεις ?</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο. Σε αυτό το παράθυρο, μπορείτε να προσδιορίσετε τα προσωπικά δεδομένα των οποίων τη χρήση επιθυμείτε να παρακολουθείτε στην επικοινωνία του επιλεγμένου χρήστη.

Αναφορά χρήσης διαδικτύου

Ανάπτυξη όλων | Σύμπτυξη όλων

Το επάνω μέρος του παραθύρου εμφανίζει το όνομα του λογαριασμού χρήστη, οι ενέργειες του οποίου αναφέρονται στο συγκεκριμένο παράθυρο.

Έλεγχος ενεργοποιημένος / απενεργοποιημένος 🛛 🌔 / 🤇

Αυτός ο διακόπτης καθιστά εφικτή την ενεργοποίηση / απενεργοποίηση των ενεργειών του χρήστη μέσω του Γονικού ελέγχου.

Ανάλογα με το εάν ο Γονικός έλεγχος παρακολουθεί τις ενέργειες του χρήστη, το κουμπί αυτό μπορεί να εμφανίζεται ως εξής:



– Ο Γονικός έλεγχος παρακολουθεί τις ενέργειες του χρήστη.

– Ο Γονικός έλεγχος δεν παρακολουθεί τις ενέργειες του χρήστη.

Η παρακολούθηση των ενεργειών του χρήστη πραγματοποιείται σύμφωνα με τις ρυθμίσεις Γονικού ελέγχου που έχουν οριστεί για τον συγκεκριμένο χρήστη.

Στο παράθυρο **Αναφορά χρήσης διαδικτύου**, μπορείτε να εμφανίσετε πληροφορίες για τους δικτυακούς τόπους που επισκέφθηκε ο επιλεγμένος χρήστης κατά το καθορισμένο διάστημα.

<u>Σήμερα</u> ?

Κάνοντας κλικ σε αυτό το κουμπί ανοίγει η αναφορά σχετικά με τη δραστηριότητα του χρήστη για την τρέχουσα ημέρα.

<u>Κουμπιά</u> ? < >

Κάνοντας κλικ σε αυτά τα κουμπιά ανοίγουν οι αναφορές για τις προηγούμενες και επόμενες περιόδους.

<u>Ημέρα / Εβδομάδα / Μήνας </u>

Χρονική περίοδος για την οποία δημιουργείται μια αναφορά. Μπορείτε να δημιουργήσετε αναφορά για τις παρακάτω περιόδους: ημέρα, εβδομάδα και μήνας.

<u>Κουμπί</u> ? 🧐

Κάνοντας κλικ σε αυτό το κουμπί ανοίγει το παράθυρο ρυθμίσεων Γονικού ελέγχου, στο οποίο εμφανίζεται η ενότητα **Διαδίκτυο**. Σε αυτή την ενότητα μπορείτε να επιβάλετε περιορισμούς για τον χρόνο χρήσης του Διαδικτύου, την πρόσβαση σε δικτυακούς τόπους και τις λήψεις αρχείων για τον επιλεγμένο χρήστη.

<u>Κυριότερες αγαπημένες τοποθεσίες web</u> 🖓

Αυτή η αναφορά εμφανίζει μια λίστα με τους δικτυακούς τόπους τους οποίους ο χρήστης επισκέφθηκε συχνά κατά τη διάρκεια της περιόδου αναφοράς και τον αριθμό των επισκέψεων.

<u>Δαπανήθηκαν</u> 🕐

Συνολικός χρόνος που δαπανήθηκε στο Διαδίκτυο από τον επιλεγμένο χρήστη κατά τη συγκεκριμένη περίοδο.

<u>Αποκλεισμένοι πόροι web</u> 🖓

Λίστα με δικτυακούς τόπους που έχουν αποκλειστεί από τον Γονικό έλεγχο και λίστα αρχείων η λήψη των οποίων έχει αποκλειστεί.

<u>Εμφάνιση όλων</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο που περιέχει πληροφορίες σχετικά με τον αριθμό των αποκλεισμένων λήψεων αρχείων και επισκέψεων σε δικτυακούς τόπους.

<u>Κατηγορίες τοποθεσιών web</u> ?

Περιέχει μια λίστα με τις κατηγορίες δικτυακών τόπων. Για κάθε κατηγορία δικτυακών τόπων, εμφανίζεται ο αριθμός των επισκέψεων που έχουν αποκλειστεί ή επιτραπεί από τον Γονικό έλεγχο:

- Ο αριθμός προσπαθειών πρόσβασης σε δικτυακούς τόπους που αποκλείστηκαν από τον Γονικό έλεγχο εμφανίζεται με κόκκινο.
- Ο αριθμός προσπαθειών πρόσβασης σε δικτυακούς τόπους που επιτράπηκαν από το Γονικό έλεγχο εμφανίζεται με γκρι.

Αναφορά χρήσης υπολογιστή

Ανάπτυξη όλων | Σύμπτυξη όλων

Το επάνω μέρος του παραθύρου εμφανίζει το όνομα του λογαριασμού χρήστη, οι ενέργειες του οποίου αναφέρονται στο συγκεκριμένο παράθυρο.

Έλεγχος ενεργοποιημένος / απενεργοποιημένος 🛛 🌔 / 🔵

Αυτός ο διακόπτης καθιστά εφικτή την ενεργοποίηση / απενεργοποίηση των ενεργειών του χρήστη μέσω του Γονικού ελέγχου.

Ανάλογα με το εάν ο Γονικός έλεγχος παρακολουθεί τις ενέργειες του χρήστη, το κουμπί αυτό μπορεί να εμφανίζεται ως εξής:

🔵 – Ο Γονικός έλεγχος παρακολουθεί τις ενέργειες του χρήστη.

– Ο Γονικός έλεγχος δεν παρακολουθεί τις ενέργειες του χρήστη.

Η παρακολούθηση των ενεργειών του χρήστη πραγματοποιείται σύμφωνα με τις ρυθμίσεις Γονικού ελέγχου που έχουν οριστεί για τον συγκεκριμένο χρήστη.

Στο παράθυρο **Αναφορά χρήσης υπολογιστή** μπορείτε να δείτε πληροφορίες σχετικά με το χρόνο χρήσης του υπολογιστή κατά τη διάρκεια ενός καθορισμένου χρονικού διαστήματος για έναν επιλεγμένο λογαριασμό.

<u>Σήμερα</u> ?

Κάνοντας κλικ σε αυτό το κουμπί ανοίγει η αναφορά σχετικά με τη δραστηριότητα του χρήστη για την τρέχουσα ημέρα.

<u>Κουμπιά</u> ?

Κάνοντας κλικ σε αυτά τα κουμπιά ανοίγουν οι αναφορές για τις προηγούμενες και επόμενες περιόδους.

<u>Ημέρα / Εβδομάδα / Μήνας</u> 🖓

Χρονική περίοδος για την οποία δημιουργείται μια αναφορά. Μπορείτε να δημιουργήσετε αναφορά για τις παρακάτω περιόδους: ημέρα, εβδομάδα και μήνας.



Κάνοντας κλικ σε αυτό το κουμπί ανοίγει το παράθυρο ρυθμίσεων Γονικού ελέγχου, στο οποίο εμφανίζεται η ενότητα **Υπολογιστής**. Σε αυτή την ενότητα μπορείτε να ορίσετε χρονικά όρια για τη χρήση του υπολογιστή.

Περιλαμβάνει πληροφορίες σχετικά με τις περιόδους και τη διάρκεια χρήσης του υπολογιστή κατά τη διάρκεια του καθορισμένου διαστήματος.

Οι χρονικές περίοδοι κατά τις οποίες ο υπολογιστής χρησιμοποιήθηκε από τον επιλεγμένο λογαριασμό απεικονίζονται με ροζ χρώμα.

Η τρέχουσα χρονική περίοδος (ημέρα, εβδομάδα ή μήνας) επισημαίνεται με πράσινο.

Η τρέχουσα ώρα της ημέρας (εάν έχει επιλεγεί διάστημα *Ημέρας* ή *Εβδομάδας*) εμφανίζεται με κόκκινη γραμμή.

Παράθυρο Διαχείριση εφαρμογών

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Εκκίνηση / Περιορισμοί</u> 🖓

Για να αλλάξετε τον τρόπο με τον οποίο εμφανίζονται οι εφαρμογές στη λίστα, κάντε κλικ σε αυτούς τους συνδέσμους:

- Κάνοντας κλικ στη σύνδεση Έναρξη, οι εφαρμογές στη λίστα ταξινομούνται σε δύο ομάδες: Αποκλεισμός εκκίνησης και Να επιτρέπεται η εκκίνηση.
- Κάνοντας κλικ στο κουμπί Περιορισμοί, οι εφαρμογές στη λίστα ταξινομούνται κατά ομάδες αξιοπιστίας. Για παράδειγμα, οι αξιόπιστες εφαρμογές παρατίθενται στην ομάδα Αξιόπιστες.

<u>Εκκαθάριση</u> 🕐

Κάνοντας κλικ σε αυτή τη σύνδεση, το Kaspersky Total Security αφαιρεί από τη λίστα τις εφαρμογές που δεν υπάρχουν πλέον.

<u>Εμφάνιση</u> ?

Στην αναπτυσσόμενη λίστα, μπορείτε να επιλέξετε έναν τρόπο προβολής για τις εφαρμογές και διεργασίες:

- Επέκταση όλων. Επιλέγοντας αυτό το στοιχείο, εμφανίζονται στη λίστα όλες οι εφαρμογές που είναι εγκατεστημένες στον υπολογιστή.
- Κλείσιμο όλων. Επιλέγοντας αυτό το στοιχείο, εμφανίζονται οι ομάδες αξιοπιστίας στη λίστα.

Στην αναπτυσσόμενη λίστα, μπορείτε να επιλέξετε έναν τρόπο προβολής για τις εφαρμογές και διεργασίες:

- Προβολή ως λίστα. Εάν επιλέξετε αυτό το στοιχείο επιλογής, οι εφαρμογές και οι διεργασίες θα εμφανίζονται ως λίστα.
- Προβολή ως δομή. Εάν επιλέξετε αυτό το στοιχείο επιλογής, οι εφαρμογές και οι διεργασίες θα εμφανίζονται σε ιεραρχική δομή με βάση τη σειρά κλήσης των διεργασιών.

Αυτή η αναπτυσσόμενη λίστα σας επιτρέπει επίσης να απενεργοποιήσετε την εμφάνιση των εφαρμογών του συστήματος, των εφαρμογών της Kaspersky και των εφαρμογών που δεν σχετίζονται με το δίκτυο:

- Απόκρυψη εφαρμογών συστήματος. Εάν επιλέξετε αυτό το στοιχείο, η συνολική λίστα εφαρμογών και διεργασιών δεν εμφανίζει τις εφαρμογές που απαιτούνται για τη σωστή λειτουργία του λειτουργικού συστήματος. Οι εφαρμογές συστήματος αποκρύπτονται από προεπιλογή.
- Απόκρυψη Kaspersky Total Security. Εάν επιλέξετε αυτό το στοιχείο, η συνολική λίστα εφαρμογών και διεργασιών δεν εμφανίζει τις εφαρμογές της Kaspersky. Οι εφαρμογές της Kaspersky αποκρύπτονται από προεπιλογή.
- Εμφάνιση μόνο εφαρμογών δικτύου. Εάν επιλέξετε αυτό το στοιχείο, η συνολική λίστα εφαρμογών και διεργασιών εμφανίζει μόνο τις εφαρμογές δικτύου. Εφαρμογές δικτύου είναι οι εφαρμογές που προορίζονται για την οργάνωση της συνεργασίας μιας ομάδας χρηστών σε διαφορετικούς υπολογιστές.

<u>Λίστα εφαρμογών </u>

Αυτή η λίστα περιέχει εφαρμογές που είναι εγκατεστημένες στον υπολογιστή σας. Για κάθε εφαρμογή στη λίστα, μπορείτε να προβάλλετε πληροφορίες σχετικά με την κατάσταση, την ψηφιακή υπογραφή, την ομάδα αξιοπιστίας, τη δημοτικότητα μεταξύ των χρηστών του KSN και τον χρόνο της πιο πρόσφατης εκκίνησής της.

Κάνοντας διπλό κλικ στη σειρά μιας εφαρμογής ή διεργασίας, ανοίγει το παράθυρο **Κανόνες εφαρμογής**. Σε αυτό το παράθυρο, μπορείτε να διαμορφώσετε κανόνες για τον έλεγχο των ενεργειών της εφαρμογής.

Κάνοντας δεξί κλικ στη γραμμή της εφαρμογής ανοίγει ένα μενού περιβάλλοντος. Από το μενού περιβάλλοντος, μπορείτε να εκτελέσετε τις παρακάτω ενέργειες:

 Να ανοίξετε το παράθυρο Κανόνες εφαρμογής, στο οποίο μπορείτε να διαμορφώσετε τα δικαιώματα για τη δραστηριότητα της εφαρμογής.

- Να επιτρέψετε ή να αποκλείσετε την εκκίνηση εφαρμογών.
- Να μετακινήσετε την εφαρμογή σε άλλη ομάδα αξιοπιστίας.
- Να εφαρμόσετε τις προεπιλεγμένες ρυθμίσεις Ελέγχου προνομίων εφαρμογών σε μια εφαρμογή (επαναφορά ρυθμίσεων εφαρμογής).
- Να αφαιρέσετε την εφαρμογή από τη λίστα.
- Να ανοίξετε το φάκελο που περιέχει το εκτελέσιμο αρχείο της εφαρμογής.

Οι εφαρμογές της λίστας περιλαμβάνονται σε ομάδες και υποομάδες. Κάνοντας δεξί κλικ στη γραμμή της ομάδας, ανοίγει ένα μενού περιβάλλοντος. Από το μενού περιβάλλοντος, μπορείτε να εκτελέσετε τις παρακάτω ενέργειες:

- Να ανοίξετε το παράθυρο Κανόνες ομάδας, όπου μπορείτε να ορίσετε προεπιλεγμένα δικαιώματα για ενέργειες των εφαρμογών της συγκεκριμένης ομάδας.
- Να δημιουργήσετε μια υποομάδα στην ομάδα. Από προεπιλογή, οι κανόνες που καθορίζονται για την ομάδα στην οποία ανήκει η υποομάδα εφαρμόζονται και στην υποομάδα.
- Να προσθέσετε μια εφαρμογή στην ομάδα. Από προεπιλογή, οι κανόνες που καθορίζονται για την ομάδα στην οποία ανήκει η εφαρμογή εφαρμόζονται και στην εφαρμογή.
- Να εφαρμόσετε τις προεπιλεγμένες ρυθμίσεις Ελέγχου προνομίων εφαρμογών στην ομάδα και σε όλες τις υποομάδες και τις εφαρμογές της ομάδας (επαναφορά ρυθμίσεων ομάδας).
- Να εφαρμόσετε τις προεπιλεγμένες ρυθμίσεις Ελέγχου προνομίων εφαρμογών σε όλες τις υποομάδες και τις εφαρμογές της ομάδας, διατηρώντας παράλληλα ανέπαφες τις ρυθμίσεις της ομάδας (επαναφορά ρυθμίσεων υποομάδας και εφαρμογής).
- Να διαγράψετε υποομάδες και εφαρμογές από την ομάδα.

<u>Εφαρμογή</u> 🕐

Αυτή η στήλη εμφανίζει το όνομα της εφαρμογής.

Αυτή η στήλη δείχνει την ομάδα αξιοπιστίας στην οποία ανήκει η εφαρμογή. Η ομάδα αξιοπιστίας ορίζει τους κανόνες χρήσης της εφαρμογής στον υπολογιστή: απαγόρευση ή παραχώρηση άδειας εκκίνησης, πρόσβαση της εφαρμογής σε αρχεία και στο μητρώο συστήματος και περιορισμοί στη δραστηριότητα δικτύου της εφαρμογής.

<u>Δημοτικότητα </u>

Αυτή η στήλη εμφανίζει τη δημοτικότητα της εφαρμογής μεταξύ συμμετεχόντων του Kaspersky Security Network (KSN). Το επίπεδο δημοτικότητας αντικατοπτρίζει τον αριθμό των συμμετεχόντων του KSN που χρησιμοποιούν την εφαρμογή.

<u>Δίκτυο</u> ?

Αυτή η στήλη σας επιτρέπει να επιλέγετε την ενέργεια που θα εκτελεστεί από την εφαρμογή, όταν η εφαρμογή επιχειρεί να αποκτήσει πρόσβαση στο δίκτυο.

Ο παρακάτω πίνακας περιέχει τις λειτουργίες που εκτελούνται από το Kaspersky Total Security όταν μια εφαρμογή ή ομάδα εφαρμογών επιχειρεί να αποκτήσει πρόσβαση στο δίκτυο.

Περιγραφή των ενεργειών του Kaspersky Total Security

Ενέργεια	Περιγραφή
Μεταβίβαση	Η απόκριση από τη γονική ομάδα μεταβιβάζεται στην εφαρμογή ή την ομάδα.
Να επιτρέπεται	Το Kaspersky Total Security επιτρέπει την πρόσβαση στο δίκτυο στις εφαρμογές που περιλαμβάνονται στην επιλεγμένη ομάδα.
Αποκλεισμός	Το Kaspersky Total Security δεν επιτρέπει την πρόσβαση στο δίκτυο στις εφαρμογές που περιλαμβάνονται στην επιλεγμένη ομάδα.
Προτροπή χρήστη	Εάν το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών είναι επιλεγμένο στην περιοχή Ρυθμίσεις → Γενικά , το Kaspersky Total Security επιλέγει αυτόματα μια ενέργεια βάσει των κανόνων που έχουν δημιουργήσει οι ειδικοί της Kaspersky. Μπορείτε να ακολουθήσετε την υποσημείωση για να διαβάσετε ακριβώς ποια ενέργεια θα επιλεγεί.
	Εάν δεν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, η εφαρμογή ρωτά τον χρήστη εάν θα επιτρέψει ή όχι σε αυτήν την εφαρμογή να έχει πρόσβαση στο δίκτυο.
------------------------	--
Καταγραφή συμβάντων	Εκτός από την καθορισμένη απόκριση, το Kaspersky Total Security καταγράφει πληροφορίες σχετικά με τις προσπάθειες της εφαρμογής για πρόσβαση στο δίκτυο και προσθέτει τις πληροφορίες σε μια αναφορά.

<u>Έναρξη</u> ?

Σε αυτή τη στήλη, μπορείτε να χρησιμοποιήσετε το διακόπτη για να επιτρέψετε ή να αποκλείσετε την εκκίνηση της επιλεγμένης εφαρμογής. Από προεπιλογή, η εκκίνηση μιας εφαρμογής επιτρέπεται ή αποκλείεται ανάλογα με τους περιορισμούς για την ομάδα στην οποία ανήκει η εφαρμογή.

Εκκαθάριση ιδιωτικού απορρήτου / Επαναφορά αλλαγών

Αυτό το παράθυρο εμφανίζει την πρόοδο εκκαθάρισης των ιχνών της δραστηριότητάς σας στο λειτουργικό σύστημα. Η εξάλειψη προβλημάτων ενδέχεται να διαρκέσει αρκετή ώρα. Για την κατάργηση κάποιων ιχνών δραστηριότητας, θα πρέπει να επανεκκινήσετε τον υπολογιστή.

Εάν επιλέξατε **Επαναφορά αλλαγών** στο πρώτο βήμα, ο Οδηγός εκκαθάρισης ιδιωτικού απορρήτου επαναφέρει τις ενέργειες που επιλέχθηκαν στο προηγούμενο βήμα.

Παράθυρο Ασφαλείς τραπεζικές συναλλαγές

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Ενεργοποίηση </u>

Ενεργοποίηση του στοιχείου Ασφαλείς τραπεζικές συναλλαγές.

Το κουμπί εμφανίζεται όταν το στοιχείο Ασφαλείς τραπεζικές συναλλαγές είναι απενεργοποιημένο.

<u>Ενεργοποίηση αυτοάμυνας</u> 🖓

Ενεργοποίηση ενός μηχανισμού του Kaspersky Total Security που προστατεύει την εφαρμογή από την αλλαγή ή τη διαγραφή των αρχείων του από τον σκληρό δίσκο, τις διεργασίες της μνήμης και τις εγγραφές του μητρώου συστήματος.

Το κουμπί εμφανίζεται εάν έχει αποεπιλεγεί το πλαίσιο ελέγχου **Ενεργοποίηση** αυτοάμυνας στην υποενότητα **Αυτοάμυνα** της ενότητας **Πρόσθετα** του παραθύρου ρυθμίσεων της εφαρμογής.

<u>Προσθήκη δικτυακού τόπου / Προσθήκη δικτυακού τόπου στις Ασφαλείς τραπεζικές</u> συναλλαγές 🖓

Κάνοντας κλικ στο κουμπί εμφανίζονται τα πλαίσια κειμένου, στα οποία μπορείτε να παρέχετε τη διεύθυνση της τοποθεσίας web της τράπεζας ή του συστήματος πληρωμής και την περιγραφή τους. Όταν ο χρήστης επιχειρεί να αποκτήσει πρόσβαση στον καθορισμένο δικτυακό τόπο ή σύστημα πληρωμής, το Kaspersky Total Security εκτελεί την ενέργεια που έχει επιλεγεί στην ενότητα **Όταν γίνεται επίσκεψη σε αυτήν την τοποθεσία web**.

Πληκτρολόγιο οθόνης 🖓

Κάνοντας κλικ σε αυτή τη σύνδεση, εμφανίζεται το πληκτρολόγιο οθόνης. Το πληκτρολόγιο οθόνης προστατεύει τα δεδομένα που εισάγονται με το πληκτρολόγιο από υποκλοπή. Μπορείτε να χρησιμοποιήσετε το πληκτρολόγιο οθόνης για να εισάγετε προσωπικά δεδομένα, για παράδειγμα, κατά τη σύνδεση σε δικτυακούς τόπους ή κατά τη μεταφορά χρημάτων μέσω του Διαδικτύου.

Για να ενεργοποιηθεί το πληκτρολόγιο οθόνης, επανεκκινήστε τον υπολογιστή σας μετά την εγκατάσταση του Kaspersky Total Security.

<u>Λίστα τραπεζών και συστημάτων πληρωμής 🖸</u>

Περιέχει μια λίστα δικτυακών τόπων τραπεζών και συστημάτων πληρωμής για τις οποίες έχετε διαμορφώσει ειδικές ρυθμίσεις στη λειτουργία Ασφαλείς τραπεζικές συναλλαγές. Κάντε κλικ σε ένα στοιχείο της λίστας και προσδιορίστε την ενέργεια που πρέπει να εκτελεί το Kaspersky Total Security:

- 🔜 Εκτέλεση Προστατευμένου προγράμματος περιήγησης.
- 🔜 Εντολή για ενέργεια.

 Να μην εκτελείται το Προστατευμένο πρόγραμμα περιήγησης, αλλά να ανοίγει ο δικτυακός τόπος στο τυπικό πρόγραμμα περιήγησης.

Το κουμπί 🧔 επιτρέπει τη ρύθμιση παραμέτρων για τις Ασφαλείς τραπεζικές συναλλαγές για μια τοποθεσία web ή ένα σύστημα πληρωμής.

Αν η λίστα είναι κενή, το Kaspersky Total Security χρησιμοποιεί τη βάση δεδομένων δικτυακών τόπων τραπεζών και συστημάτων πληρωμής που προτείνονται από τους ειδικούς της Kaspersky. Σε αυτή την περίπτωση, εμφανίζεται το κουμπί **Προσθήκη τοποθεσίας web στις Ασφαλείς τραπεζικές συναλλαγές** και όχι η λίστα.

<u>Εμφάνιση όλων | Απόκρυψη</u> 🖓

Κάνοντας κλικ σε αυτή τη σύνδεση, εμφανίζεται / αποκρύπτεται ένα μέρος της λίστας των δικτυακών τόπων τραπεζών και συστημάτων πληρωμών για τα οποία έχει επιλεγεί η ενέργεια **Να μην εκτελείται το Προστατευμένο πρόγραμμα περιήγησης**.

<u>Τοποθεσία web (URL)</u> ?

Η διεύθυνση web του δικτυακού τόπου μιας τράπεζας ή ενός συστήματος πληρωμών. Μπορείτε να ορίσετε μια διεύθυνση web ή μια μάσκα διεύθυνσης.

Στην ενότητα **Όταν γίνεται επίσκεψη σε αυτήν την τοποθεσία web**, μπορείτε να επιλέξετε την ενέργεια που θα εκτελεί το Kaspersky Total Security κατά την πρόσβαση στον καθορισμένο δικτυακό τόπο από τον χρήστη.

Εκτέλεση Προστατευμένου προγράμματος περιήγησης 🖓

Εάν το Kaspersky Total Security εντοπίσει μια προσπάθεια πρόσβασης στον συγκεκριμένο δικτυακό τόπο, ανοίγει τον δικτυακό τόπο χρησιμοποιώντας το Προστατευμένο πρόγραμμα περιήγησης. Το τυπικό πρόγραμμα περιήγησης που χρησιμοποιείται για την πρόσβαση στον δικτυακό τόπο εμφανίζει ένα μήνυμα που σας ενημερώνει για την εκκίνηση του Προστατευμένου προγράμματος περιήγησης.

<u>Προτροπή χρήστη</u> 🕐

Εάν το Kaspersky Total Security εντοπίσει μια προσπάθεια πρόσβασης στον συγκεκριμένο δικτυακό τόπο, σας ειδοποιεί να εκκινήσετε ένα Προστατευμένο πρόγραμμα περιήγησης ή να ανοίξετε τον δικτυακό τόπο με το τυπικό πρόγραμμα περιήγησης. Όταν επιχειρείτε να αποκτήσετε πρόσβαση στον συγκεκριμένο δικτυακό τόπο, το Kaspersky Total Security δεν χρησιμοποιεί το Προστατευμένο πρόγραμμα περιήγησης. Ο δικτυακός τόπος ανοίγει στο τυπικό πρόγραμμα περιήγησης.

<u>Προσθήκη περιγραφής </u>

Κάνοντας κλικ σε αυτή τη σύνδεση, εμφανίζεται ένα πεδίο εισαγωγής στο οποίο μπορείτε να συμπληρώσετε μια περιγραφή του δικτυακού τόπου (για παράδειγμα, το όνομα της τράπεζας). Η περιγραφή εμφανίζεται στη λίστα των τοποθεσιών web τραπεζών και συστημάτων πληρωμής.

<u>Περιγραφή</u> 🕐

Ένα πεδίο εισαγωγής στο οποίο μπορείτε να αλλάξετε την περιγραφή ενός δικτυακού τόπου (για παράδειγμα, το όνομα της τράπεζας). Η περιγραφή εμφανίζεται στη λίστα των τοποθεσιών web τραπεζών και συστημάτων πληρωμής.

<u>Προσθήκη / Αποθήκευση </u>

Κάνοντας κλικ σε αυτό το κουμπί, αποθηκεύονται στη λίστα οι πληροφορίες που έχουν εισαχθεί σχετικά με έναν δικτυακό τόπο τράπεζας ή συστήματος πληρωμής.

<u>Άκυρο</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, απορρίπτονται όλες οι αλλαγές που έχουν πραγματοποιηθεί.

<u>Διαγραφή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, καταργείται ο επιλεγμένος δικτυακός τόπος μιας τράπεζας από τη λίστα.

Μπορείτε να αναιρέσετε την κατάργηση κάνοντας κλικ στο κουμπί Επαναφορά.

Κάνοντας κλικ σε αυτό το κουμπί, εκτελείται επαναφορά μιας καταχώρησης δικτυακού τόπου τράπεζας ή συστήματος πληρωμής που είχε διαγραφεί προηγουμένως.

<u>Αποστολή σχολίων ?</u>

Κάνοντας κλικ σε αυτήν τη σύνδεση, ανοίγει ένα παράθυρο στο οποίο μπορείτε να στέλνετε σχόλια για τη λειτουργία του στοιχείου Ασφαλείς τραπεζικές συναλλαγές.

Παράθυρο Ενημέρωση βάσης δεδομένων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Ενημέρωση</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, εκτελείται ενημέρωση των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής.

<u>Τελευταία ενημέρωση: <ώρα τελευταίας ενημέρωσης> ?</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Λεπτομερείς αναφορές**, στο οποίο μπορείτε να δείτε πληροφορίες σχετικά με τις ολοκληρωμένες ενημερώσεις των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής.

<u>Λειτουργία εκτέλεσης: <όνομα λειτουργίας εκτέλεσης> ?</u>

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο **Ρυθμίσεις ενημέρωσης**. Σε αυτό το παράθυρο, μπορείτε να ρυθμίσετε τις παραμέτρους της λειτουργίας εκτέλεσης για ενημερώσεις.



Κάνοντας κλικ σε αυτό το κουμπί, τυχόν ενημερώσεις ακυρώνονται και οι βάσεις δεδομένων και οι λειτουργικές μονάδες της εφαρμογής μένουν ως έχουν.

Το κουμπί εμφανίζεται κατά τη διάρκεια ενημέρωσης των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής.

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Λεπτομερείς αναφορές**, στο οποίο μπορείτε να δείτε πληροφορίες σχετικά με τις ολοκληρωμένες ενημερώσεις των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής.

Η σύνδεση εμφανίζεται κατά τη διάρκεια μιας ενημέρωσης των βάσεων δεδομένων και των λειτουργικών μονάδων της εφαρμογής.

Επισκόπηση παγκόσμιας δραστηριότητας ιών 💿

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το securelist.com σε ένα παράθυρο προγράμματος περιήγησης, με μια επισκόπηση της τρέχουσας δραστηριότητας ιών.

Γενικά

Ρυθμίσεις	Περιγραφή
Αυτόματη εκτέλεση των συνιστώμενων ενεργειών	Εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου, τα στοιχεία της κύριας εφαρμογής λειτουργούν σε διαδραστική λειτουργία. Αυτό σημαίνει ότι το Kaspersky Total Security σάς ζητά να αποφασίσετε ποια ενέργεια θα εκτελέσετε τα εντοπισμένα αντικείμενα και απειλές, εάν είναι ενεργοποιημένη η επιλογή Προτροπή χρήστη στις ρυθμίσεις Προστασία αρχείων από ιούς, Προστασία από ιούς στο Web, Προστασία email από ιούς, Παρακολούθηση συστημάτων και Έλεγχος εφαρμογών. Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security επιλέγει αυτόματα την ενέργεια βάσει κανόνων που ορίζονται από ειδικούς της Kaspersky
Διαγραφή κακόβουλων εργαλείων, προγραμμάτων adware, λογισμικού αυτόματων κλήσεων και ύποπτων πακέτων	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security εκτελεί διαγραφή κακόβουλων εργαλείων, προγραμμάτων adware, λογισμικού αυτόματων κλήσεων και ύποπτων πακέτων σε λειτουργία αυτόματης προστασίας. Η λειτουργία είναι διαθέσιμη εάν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών .
Απενεργοποίηση προγραμματισμένων	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, η λειτουργία εξοικονόμησης ενέργειας είναι ενεργοποιημένη. Το Kaspersky

εργασιών όταν ο υπολογιστής λειτουργεί με μπαταρία	Total Security αναβάλλει προγραμματισμένες εργασίες. Μπορείτε να ξεκινήσετε τη σάρωση και να ενημερώσετε εργασίες με μη αυτόματο τρόπο, εάν είναι απαραίτητο.
Χρήση της λειτουργίας παιχνιδιών	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security δεν εκτελεί σάρωση ή εργασίες ενημέρωσης και δεν εμφανίζει ειδοποιήσεις όταν παίζετε παιχνίδια ή εκτελείτε εφαρμογές σε λειτουργία πλήρους οθόνης.
Αναβολή εργασιών σάρωσης του υπολογιστή όταν ο επεξεργαστής (CPU) και τα συστήματα δίσκου βρίσκονται υπό υψηλό φορτίο	Όταν το Kaspersky Total Security εκτελεί εργασίες χρονοδιαγράμματος, μπορεί να προκληθεί αυξημένος φόρτος εργασίας στα υποσυστήματα της CPU και του δίσκου, κάτι που επηρεάζει την απόδοση άλλων εφαρμογών. Όταν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security αναστέλλει προγραμματισμένες εργασίες όταν εντοπίζει αυξημένο φορτίο και ελευθερώνει πόρους λειτουργικού συστήματος για εφαρμογές χρηστών.
Έναρξη του Kaspersky Total Security κατά την εκκίνηση του υπολογιστή (συνιστάται)	Όταν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security ξεκινά μετά τη φόρτωση του λειτουργικού συστήματος, προστατεύοντας τον υπολογιστή καθ' όλη τη διάρκεια της περιόδου λειτουργίας. Όταν δεν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security δεν ξεκινά μετά τη φόρτωση του λειτουργικού συστήματος, έως ότου ο χρήστης το ξεκινήσει χειροκίνητα. Η προστασία του υπολογιστή είναι απενεργοποιημένη και τα δεδομένα χρήστη ενδέχεται να εκτεθούν σε απειλές.
Ενεργοποίηση της τεχνολογίας προηγμένης απολύμανσης	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, εμφανίζεται μια αναδυόμενη ειδοποίηση στην οθόνη όταν εντοπίζεται κακόβουλη δραστηριότητα στο λειτουργικό σύστημα. Στην ειδοποίησή του, το Kaspersky Total Security προτείνει στον χρήστη να εκτελέσει Προηγμένη απολύμανση του υπολογιστή. Αφού ο χρήστης εγκρίνει αυτήν τη διαδικασία, το Kaspersky Total Security εξουδετερώνει την απειλή. Μετά την ολοκλήρωση της διαδικασίας προηγμένης απολύμανσης, το Kaspersky Total Security επανεκκινεί τον υπολογιστή. Η τεχνολογία προηγμένης απολύμανσης χρησιμοποιεί σημαντικούς υπολογιστικούς πόρους, οι οποίοι ενδέχεται να επιβραδύνουν άλλες εφαρμογές.

αυτοάμυνας	Total Security αποτρέπει την τροποποίηση ή τη διαγραφή αρχείων εφαρμογών στον σκληρό δίσκο, τις διαδικασίες μνήμης και τις καταχωρήσεις στο μητρώο του συστήματος.
Να επιτρέπεται η διαχείριση των ρυθμίσεων του Kaspersky Total Security μέσω εφαρμογών απομακρυσμένου ελέγχου	Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, οι αξιόπιστες εφαρμογές απομακρυσμένης διαχείρισης (όπως το TeamViewer, το LogMeIn Pro και το Remotely Anywhere) μπορούν να αλλάξουν τις ρυθμίσεις του Kaspersky Total Security. Δεν θα επιτρέπεται η αλλαγή των ρυθμίσεων του Kaspersky Total Security από μη αξιόπιστες εφαρμογές απομακρυσμένου ελέγχου, ακόμα και αν είναι επιλεγμένο το πλαίσιο ελέγχου.
Ενεργοποίηση εξωτερικού ελέγχου υπηρεσίας	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security επιτρέπει τη διαχείριση υπηρεσιών εφαρμογών από απομακρυσμένο υπολογιστή. Όταν γίνεται προσπάθεια απομακρυσμένης διαχείρισης των υπηρεσιών εφαρμογών, εμφανίζεται μια ειδοποίηση στη γραμμή εργασιών των Microsoft Windows, πάνω από το εικονίδιο της εφαρμογής (εκτός εάν η υπηρεσία ειδοποιήσεων έχει απενεργοποιηθεί από τον χρήστη).
Ενεργοποίηση εγγραφής αρχείου αποτύπωσης	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security εγγράφει αρχεία αποτύπωσης όταν διακόπτεται. Εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security δεν εκτελεί εγγραφή ένδειξης σφαλμάτων. Η εφαρμογή διαγράφει επίσης υπάρχοντα αρχεία αποτύπωσης από τον σκληρό δίσκο του υπολογιστή.
Ενεργοποίηση προστασίας αρχείων ένδειξης σφαλμάτων και αρχείων ιχνών	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, παρέχεται πρόσβαση σε αρχεία αποτύπωσης στον διαχειριστή συστήματος και στον τοπικό διαχειριστή, καθώς και στον χρήστη που έκανε την ενεργοποίηση εγγραφής αρχείου αποτύπωσης. Μόνο οι διαχειριστές συστήματος και οι τοπικοί διαχειριστές μπορούν να έχουν πρόσβαση σε αρχεία ιχνών. Εάν το πλαίσιο ελέγχου έχει διαγραφεί, οποιοσδήποτε χρήστης μπορεί να έχει πρόσβαση σε αρχεία αποτύπωσης και αρχεία ιχνών.

Απειλές και Εξαιρέσεις

I COMECCES	Ρ	υ	θμ	ίσ	εις
------------	---	---	----	----	-----

Περιγραφή

Τύποι απειλών που εντοπίζονται	Το Kaspersky Total Security εντοπίζει διάφορους τύπους αντικειμένων, όπως ιούς και worms, δούρειους ίππους και προγράμματα adware. Για λεπτομέρειες, ανατρέξτε στην <u>Εγκυκλοπαίδεια Kaspersky</u> 🖬.
	Μπορείτε να απενεργοποιήσετε τον εντοπισμό των ακόλουθων τύπων αντικειμένων:
	 Άλλο λογισμικό που μπορεί να χρησιμοποιηθεί από εγκληματίες για την καταστροφή του υπολογιστή σας ή των προσωπικών δεδομένων σας. Αυτό το λογισμικό περιλαμβάνει εφαρμογές απομακρυσμένης διαχείρισης που οι διαχειριστές συστήματος μπορούν να χρησιμοποιήσουν για πρόσβαση στη διεπαφή ενός απομακρυσμένου υπολογιστή για σκοπούς παρακολούθησης ή διαχείρισης.
	 Πολλαπλά αρχεία. Αρχεία που συσκευάζονται πολλές φορές, από διάφορα προγράμματα συσκευασίας. Η πολλαπλή συσκευασία καθιστά πιο δύσκολη τη σάρωση αντικειμένων.
Διαχείριση εξαιρέσεων	Κάνοντας κλικ στη σύνδεση ανοίγει το παράθυρο Εξαιρέσεις που περιλαμβάνει μια λίστα εξαιρέσεων σάρωσης. Η <i>εξαίρεση σάρωσης</i> είναι ένα σύνολο συνθηκών που, όταν πληρούνται, το Kaspersky Total Security δεν σαρώνει ένα συγκεκριμένο αντικείμενο για ιούς και άλλες απειλές.
	Μπορείτε να προσθέσετε, να επεξεργαστείτε ή να διαγράψετε εξαιρέσεις από τη λίστα.
	Στο παράθυρο για την προσθήκη ή την επεξεργασία μιας εξαίρεσης, μπορείτε να ορίσετε συγκεκριμένες συνθήκες που, όταν πληρούνται, θα αποτρέψουν τη σάρωση αντικειμένων (το Kaspersky Total Security δεν θα τα σαρώσει):
	 Αρχείο ή φάκελος που πρέπει να εξαιρεθεί από τις σαρώσεις (μπορείτε επίσης να εξαιρέσετε εκτελέσιμα αρχεία εφαρμογών και διαδικασιών). Μπορείτε να χρησιμοποιήσετε μάσκες σύμφωνα με τους ακόλουθους κανόνες:
	 Ο χαρακτήρας * (αστερίσκος), ο οποίος αντικαθιστά οποιοδήποτε σύνολο χαρακτήρων, εκτός από τους χαρακτήρες \ και / (οριοθέτες των ονομάτων των αρχείων και των φακέλων σε διαδρομές προς αρχεία και φακέλους). Για παράδειγμα, η μάσκα C:**.txt θα περιλαμβάνει όλες τις διαδρομές προς αρχεία με την επέκταση TXT που

βρίσκονται σε φακέλους στη μονάδα δίσκου C: αλλά όχι σε υποφακέλους.

- Δύο διαδοχικοί χαρακτήρες * αντικαθιστούν οποιοδήποτε σύνολο χαρακτήρων (συμπεριλαμβανομένου ενός κενού συνόλου) στο όνομα του αρχείου ή του φακέλου, συμπεριλαμβανομένων των χαρακτήρων \ και / (οριοθέτες των ονομάτων των αρχείων και των φακέλων σε διαδρομές προς αρχεία και φακέλους). Για παράδειγμα, η μάσκα C:\Folder***.txt θα περιλαμβάνει όλες τις διαδρομές προς αρχεία με την επέκταση ΤΧΤ που βρίσκεται στον φάκελο με το όνομα Folder και τους υποφακέλους του. Η μάσκα πρέπει να περιλαμβάνει τουλάχιστον ένα επίπεδο ένθεσης. Η μάσκα C:***.txt δεν είναι έγκυρη μάσκα.
- Ο χαρακτήρας ? (αγγλικό ερωτηματικό), ο οποίος αντικαθιστά οποιονδήποτε μεμονωμένο χαρακτήρα, εκτός από τους χαρακτήρες \ και / (οριοθέτες των ονομάτων των αρχείων και των φακέλων σε διαδρομές προς αρχεία και φακέλους). Για παράδειγμα, η μάσκα C:\Folder\???.txt θα περιλαμβάνει διαδρομές προς όλα τα αρχεία που βρίσκονται στον φάκελο με το όνομα Folder τα οποία έχουν την επέκταση TXT και ένα όνομα που αποτελείται από τρεις χαρακτήρες.
- Τύπος αντικειμένων που πρέπει να εξαιρεθούν από τις σαρώσεις. Εισαγάγετε το όνομα του τύπου αντικειμένου σύμφωνα με την ταξινόμηση της Εγκυκλοπαίδειας Kaspersky (για παράδειγμα, Email-Worm, Rootkit ή RemoteAdmin).
 Μπορείτε να χρησιμοποιήσετε μάσκες με τον χαρακτήρα ? (αντικαθιστά οποιονδήποτε μεμονωμένο χαρακτήρα) και τον χαρακτήρα * (αντικαθιστά οποιονδήποτε αριθμό χαρακτήρων).
 Για παράδειγμα, εάν έχει καθοριστεί η μάσκα Client*, το Kaspersky Total Security εξαιρεί τα αντικείμενα Client-IRC, Client-P2P και Client-SMTP από τις σαρώσεις.
- Άθροισμα ελέγχου αντικειμένου. Η σύγκριση του αθροίσματος ελέγχου ενός αντικειμένου με το άθροισμα ελέγχου που υποδεικνύεται σε αυτήν τη ρύθμιση επιτρέπει στη σάρωση να αποκλείσει ένα αντικείμενο που δεν έχει τροποποιηθεί από την τελευταία σάρωση.
- Στοιχεία προστασίας για τα οποία εφαρμόζεται η εξαίρεση.

	Αντί να διαγράψετε μια εξαίρεση από τη λίστα, μπορείτε να αλλάξετε την κατάσταση ενός αποκλεισμού σε Ανενεργό (στο παράθυρο για προσθήκη ή επεξεργασία μιας εξαίρεσης). Όταν είναι ανενεργή, η εξαίρεση δεν θα εφαρμοστεί.
Ορισμός αξιόπιστων εφαρμογών	Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο με τη λίστα αξιόπιστων εφαρμογών. Το Kaspersky Total Security δεν παρακολουθεί τη δραστηριότητα αρχείων και τη δραστηριότητα δικτύου αξιόπιστων εφαρμογών (συμπεριλαμβανομένων των κακόβουλων εφαρμογών) και δεν παρακολουθεί τα ερωτήματα αυτών των εφαρμογών στο μητρώο συστήματος. Μπορείτε να προσθέσετε, να επεξεργαστείτε ή να διαγράψετε αξιόπιστες εφαρμογές από τη λίστα.
	Ακόμα κι αν μια εφαρμογή περιλαμβάνεται στη λίστα των αξιόπιστων εφαρμογών, το Kaspersky Total Security συνεχίζει τη σάρωση του εκτελέσιμου αρχείου και της διεργασίας αυτής της εφαρμογής για ιούς και άλλες απειλές. Εάν δεν θέλετε να σαρώσετε το εκτελέσιμο αρχείο και τη διεργασία μιας αξιόπιστης εφαρμογής, προσθέστε την εφαρμογή στη λίστα εξαιρέσεων.
	Κατά την προσθήκη ή την επεξεργασία μιας αξιόπιστης εφαρμογής, στο παράθυρο Εξαιρέσεις για εφαρμογή μπορείτε να καθορίσετε κανόνες που θα χρησιμοποιηθούν από το Kaspersky Total Security για την παρακολούθηση της δραστηριότητας της αξιόπιστης εφαρμογής. Στο παράθυρο Εξαιρέσεις για εφαρμογή , υπάρχουν οι ακόλουθοι
	 Να μη γίνει σάρωση ανοιγμένων αρχείων.
	 Να μην παρακολουθείται η δραστηριότητα της εφαρμογής. Ο Έλεγχος εφαρμογών δεν παρακολουθεί καμία δραστηριότητα εφαρμογής.
	 Να μην γίνει μεταβίβαση περιορισμών της γονικής διεργασίας (της εφαρμογής) Εάν οι περιορισμοί μιας γονικής διεργασίας δεν μεταβιβάζονται, η δραστηριότητα της εφαρμογής παρακολουθείται σύμφωνα με τους κανόνες που ορίσατε ή σύμφωνα με τους κανόνες της ομάδας αξιόπιστων εφαρμογών

στην οποία ανήκει η εφαρμογή.

- Να μην παρακολουθείται η δραστηριότητα των θυγατρικών εφαρμογών.
- Μην αποκλείετε την αλληλεπίδραση με τη διεπαφή Kaspersky Total Security. Η εφαρμογή επιτρέπεται να διαχειρίζεται το Kaspersky Total Security χρησιμοποιώντας τη γραφική διεπαφή Kaspersky Total Security. Μπορεί να χρειαστεί να επιτρέψετε σε μια εφαρμογή να διαχειριστεί το περιβάλλον εργασίας του Kaspersky Total Security όταν χρησιμοποιείτε μια εφαρμογή σύνδεσης απομακρυσμένης επιφάνειας εργασίας ή μια εφαρμογή που υποστηρίζει τη λειτουργία συσκευής εισόδου δεδομένων. Αυτές οι συσκευές μπορεί να είναι, για παράδειγμα, ένα touch pad ή tablet.
- Να μην γίνει σάρωση όλης της κυκλοφορίας (ή της κρυπτογραφημένης κυκλοφορίας). Ανάλογα με την ενεργοποιημένη επιλογή (Να μην γίνει σάρωση όλης της κυκλοφορίας ή Να μην γίνει σάρωση κρυπτογραφημένης κυκλοφορίας), το Kaspersky Total Security αποκλείει τη σάρωση όλης της κυκλοφορίας δικτύου της εφαρμογής ή της κυκλοφορίας που μεταδίδεται μέσω SSL. Η τιμή αυτής της ρύθμισης δεν επηρεάζει τη λειτουργία του Τείχους προστασίας: Το Τείχος προστασίας σαρώνει την κυκλοφορία εφαρμογής σύμφωνα με τις ρυθμίσεις του Τείχους προστασίας. Οι εξαιρέσεις επηρεάζουν την Προστασία email από ιούς, την Προστασία από ιούς στο Web και το Πρόγραμμα Anti-Spam. Μπορείτε να καθορίσετε τις διευθύνσεις ΙΡ ή τις θύρες δικτύου στις οποίες πρέπει να ισχύει ο περιορισμός ελέγχου κυκλοφορίας.

Εάν αλλάξετε την κατάσταση μιας εφαρμογής σε **Ανενεργό** στο παράθυρο **Εξαιρέσεις για εφαρμογή**, το Kaspersky Total Security δεν αντιμετωπίζει την εφαρμογή ως αξιόπιστη εφαρμογή. Με αυτόν τον τρόπο, μπορείτε να εξαιρέσετε προσωρινά μια εφαρμογή από τη λίστα αξιόπιστων εφαρμογών χωρίς να τη διαγράψετε από τη λίστα.

Χρήση αξιόπιστου καταστήματος πιστοποιητικών συστήματος Εάν επιλεγεί ένα από τα αξιόπιστα καταστήματα πιστοποιητικών συστήματος, το Kaspersky Total Security εξαιρεί τις εφαρμογές που έχουν υπογραφεί με αξιόπιστη ψηφιακή υπογραφή από τις σαρώσεις. Το Kaspersky Total Security εκχωρεί αυτόματα τέτοιες εφαρμογές στην ομάδα *Αξιόπιστες*. Εάν είναι επιλεγμένη η επιλογή **Να μην χρησιμοποιείται**, το Kaspersky Total Security σαρώνει τις εφαρμογές ανεξάρτητα από το αν έχουν ψηφιακή υπογραφή ή όχι. Το Kaspersky Total Security τοποθετεί μια εφαρμογή σε μια ομάδα αξιόπιστων εφαρμογών ανάλογα με το επίπεδο του κινδύνου στον οποίο ενδέχεται να εκθέσει αυτή η εφαρμογή τον υπολογιστή.

Ρυθμίσεις δικτύου

Ρυθμίσεις	Περιγραφή
Περιορισμός κυκλοφορίας για συνδέσεις ογκοχρέωσης	Εάν αυτό το πλαίσιο ελέγχου είναι επιλεγμένο, η εφαρμογή περιορίζει τη δική της κυκλοφορία δικτύου όταν η σύνδεση στο Διαδίκτυο είναι περιορισμένη. Το Kaspersky Total Security αναγνωρίζει μια σύνδεση στο Διαδίκτυο κινητών τηλεφώνων υψηλής ταχύτητας ως περιορισμένη σύνδεση και αναγνωρίζει μια σύνδεση Wi-Fi ως απεριόριστη σύνδεση. Η Δικτύωση με προσιτό κόστος λειτουργεί σε υπολογιστές με Windows 8 ή νεότερη έκδοση.
Ποοσθήκη δέσμης	Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total
προσσηκη σεομης ενεργειών στην κυκλοφορία web για αλληλεπίδραση με ιστοσελίδες	Security προσθέτει μια δέσμη ενεργειών στην κυκλοφορία web για αλληλεπίδραση με τον δικτυακό τόπο. Αυτή η δέσμη ενεργειών διασφαλίζει τη λειτουργία τέτοιων στοιχείων, όπως Ασφαλείς τραπεζικές συναλλαγές, Ιδιωτική περιήγηση, Πρόγραμμα Anti-Banner και Σύμβουλος URL.
Υποστήριξη DNS μέσω HTTPS (DoH)	Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, η εφαρμογή επεξεργάζεται σωστά τα <u>δεδομένα DNS που μεταδίδονται μέσω</u> <u>HTTPS</u> .
	Δεν συνιστούμε την κατάργηση της επιλογής αυτού του πλαισίου ελέγχου.
Διαχείριση διακομιστών DoH	Η σύνδεση ανοίγει ένα παράθυρο στο οποίο μπορείτε να προσθέσετε χειροκίνητα έναν διακομιστή DoH μέσω του οποίου τα δεδομένα DNS θα μεταφερθούν σε ένα πρόγραμμα περιήγησης. <u>Εδώ</u> μπορείτε να διαβάσετε σχετικά με την υποστήριξη DNS μέσω HTTPS (DoH) και τον τρόπο προσθήκης διακομιστή DoH.
Θύρες που παρακολουθούνται	Παρακολούθηση όλων των θυρών δικτύου . Σε αυτήν τη λειτουργία παρακολούθησης θυρών, η Προστασία email από ιούς, το Πρόγραμμα Anti-Spam και η Προστασία από ιούς στο

Web παρακολουθούν όλες τις ανοικτές θύρες του υπολογιστή σας.

Παρακολούθηση μόνο επιλεγμένων θυρών δικτύου. Σε αυτήν τη λειτουργία παρακολούθησης θυρών, η Προστασία email από ιούς, το Πρόγραμμα Anti-Spam και η Προστασία από ιούς στο Web παρακολουθούν τις επιλεγμένες θύρες του υπολογιστή σας. Μπορείτε να καθορίσετε τις παρακολουθούμενες θύρες δικτύου στο παράθυρο **Θύρες δικτύου**, το οποίο μπορείτε να ανοίξετε κάνοντας κλικ στη σύνδεση **Επιλογή**. Μπορείτε επίσης να καθορίσετε τις συγκεκριμένες εφαρμογές στις οποίες θα πρέπει να είναι ενεργοποιημένη η παρακολούθηση όλων των θυρών δικτύου που χρησιμοποιούνται από αυτές τις εφαρμογές:

 Παρακολούθηση όλων των θυρών για τις εφαρμογές από τη λίστα που προτείνει η Kaspersky. Η λίστα αυτών των εφαρμογών καθορίζεται από προεπιλογή και περιλαμβάνεται στο πακέτο λογισμικού για το Kaspersky Total Security.

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security παρακολουθεί όλες τις θύρες για τις ακόλουθες εφαρμογές:

- Adobe Reader.
- Υποστήριξη εφαρμογών της Apple.
- Google Chrome.
- Microsoft Edge.
- Mozilla Firefox.
- Internet Explorer.
- Java.
- mIRC.
- Opera.
- Pidgin.
- Safari.

	Mail ru Agent
	• Maillia Agent.
	Yandex Browser.
	 Παρακολούθηση θυρών για ορισμένες εφαρμογές. Μπορείτε να καθορίσετε τις εφαρμογές στο παράθυρο Εφαρμογές, το οποίο μπορείτε να ανοίξετε κάνοντας κλικ στη σύνδεση Επιλογή.
Θύρες δικτύου	Μια λίστα θυρών που χρησιμοποιούνται συνήθως για τη μεταφορά email και της κυκλοφορίας στον Ιστό περιλαμβάνεται στο πακέτο διανομής του Kaspersky Total Security. Από προεπιλογή, το Kaspersky Total Security παρακολουθεί την κυκλοφορία που περνά μέσα από όλες τις θύρες αυτής της λίστας. Μπορείτε να προσθέσετε θύρες στη λίστα ή να τις διαγράψετε από τη λίστα. Εάν έχει οριστεί η τιμή <i>Ενεργό</i> στη γραμμή θύρας της στήλης Κατάσταση , το Kaspersky Total Security παρακολουθεί την κίνηση που διέρχεται από αυτή τη θύρα. Αν έχει οριστεί η τιμή <i>Ανενεργό</i> στη γραμμή θύρας της στήλης Κατάσταση , το Kaspersky Total Security εξαιρεί αυτή τη θύρα από σαρώσεις, αλλά δεν την καταργεί από τη λίστα θυρών. Μπορείτε να
	αλλάξετε την καταστάση και άλλες ρυθμισείς θυράς στο παράθυρο κάνοντας κλικ στο κουμπί Επεξεργασία .
Σάρωση κρυπτογραφημένων	Μπορείτε να επιλέξετε μία από τις ακόλουθες λειτουργίες για σάρωση κρυπτογραφημένων συνδέσεων μέσω SSL:
συνδέσεων	 Να μη γίνεται σάρωση των κρυπτογραφημένων συνδέσεων.
	 Σάρωση κρυπτογραφημένων συνδέσεων κατόπιν αίτησης από τα στοιχεία προστασίας.
	 Να γίνεται πάντα σάρωση των κρυπτογραφημένων συνδέσεων.

	 Εάν έχει ενεργοποιηθεί η επιλογή Σάρωση κρυπτογραφημένων συνδέσεων κατόπιν αίτησης από τα στοιχεία προστασίας, το Kaspersky Total Security χρησιμοποιεί το εγκατεστημένο πιστοποιητικό Kaspersky για να επαληθεύσει την ασφάλεια των συνδέσεων SSL, εάν αυτό απαιτείται από τα στοιχεία προστασίας Προστασία από ιούς στο Web και Σύμβουλος URL. Εάν αυτά τα στοιχεία είναι απενεργοποιημένα, το Kaspersky Total Security δεν επαληθεύει την ασφάλεια των συνδέσεων SSL. Μετά την επαλήθευση μιας σύνδεσης SSL από το Kaspersky Total Security, τα πιστοποιητικά των δικτυακών τόπων ενδεχομένως να μην εμφανίζουν το όνομα του οργανισμού υπό τον οποίο έχει καταχωρηθεί ο δικτυακός τόπος.
	SSL με μια τοποθεσία web, μπορείτε να προσθέσετε την τοποθεσία web στη λίστα εξαιρέσεων κάνοντας κλικ στη σύνδεση Διαχείριση εξαιρέσεων .
Όταν προκύπτουν σφάλματα σάρωσης κρυπτογραφημένης	Στο αναπτυσσόμενο μενού μπορείτε να επιλέξετε την ενέργεια που θα εκτελεί η εφαρμογή εάν παρουσιαστεί σφάλμα σάρωσης ασφαλών συνδέσεων σε έναν δικτυακό τόπο.
συνδεσης	 Παράβλεψη. Η εφαρμογή τερματίζει τη σύνδεση με τον δικτυακό τόπο στον οποίο παρουσιάστηκε σφάλμα σάρωσης.
	 Ερώτηση. Η εφαρμογή εμφανίζει μια ειδοποίηση που σας ζητά να προσθέσετε μια διεύθυνση δικτυακού τόπου στη λίστα των δικτυακών τόπων στους οποίους παρουσιάστηκαν σφάλματα σάρωσης. Η διεύθυνση του δικτυακού τόπου θα ελεγχθεί σε σχέση με τη βάση δεδομένων κακόβουλων αντικειμένων.
	 Προσθήκη τομέα στις εξαιρέσεις. Η εφαρμογή προσθέτει τη διεύθυνση του δικτυακού τόπου στη λίστα των δικτυακών τόπων στους οποίους παρουσιάστηκαν σφάλματα σάρωσης. Η διεύθυνση του δικτυακού τόπου θα ελεγχθεί σε σχέση με τη βάση δεδομένων κακόβουλων αντικειμένων.
Τομείς με σφάλματα σάρωσης	Λίστα τομέων που δεν ήταν δυνατό να σαρωθούν λόγω σφαλμάτων κατά τη σύνδεσή σε αυτές. Οι διευθύνσεις των

	τομέων ελέγχθηκαν σε σχέση με τη βάση δεδομένων κακόβουλων αντικειμένων.
Διαχείριση εξαιρέσεων	Κάντε κλικ σε αυτήν τη σύνδεση για να ανοίξετε το παράθυρο Εξαιρέσεις , το οποίο περιέχει μια λίστα τοποθεσιών web που προσθέσατε ως εξαίρεση για τα στοιχεία Προστασία από ιούς στο Web και Σύμβουλος URL.
Αξιόπιστες εφαρμογές	Λίστα εφαρμογών των οποίων η δραστηριότητα δεν παρακολουθείται από το Kaspersky Total Security κατά τη λειτουργία του. Μπορείτε να επιλέξετε τους τύπους δραστηριότητας εφαρμογής που δεν θα παρακολουθεί το Kaspersky Total Security (για παράδειγμα, να μην πραγματοποιείται έλεγχος κυκλοφορίας δικτύου). Το Kaspersky Total Security υποστηρίζει μεταβλητές περιβάλλοντος και τις μάσκες * και ?.
Αποκλεισμός συνδέσεων μέσω πρωτοκόλλου SSL 2.0 (συνιστάται)	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security αποκλείει συνδέσεις δικτύου που έχουν δημιουργηθεί μέσω του πρωτοκόλλου SSL 2.0. Εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security δεν αποκλείει συνδέσεις δικτύου που έχουν δημιουργηθεί μέσω του πρωτοκόλλου SSL 2.0 και δεν παρακολουθεί την κυκλοφορία δικτύου που μεταδίδεται μέσω αυτών των συνδέσεων.
Αποκρυπτογράφηση κρυπτογραφημένων συνδέσεων με τοποθεσίες web που χρησιμοποιούν πιστοποιητικά ΕV	Τα πιστοποιητικά EV (Extended Validation Certificates) επιβεβαιώνουν την αυθεντικότητα των δικτυακών τόπων και βελτιώνουν την ασφάλεια της σύνδεσης. Τα προγράμματα περιήγησης χρησιμοποιούν ένα εικονίδιο κλειδαριάς στη γραμμή διευθύνσεών τους για να υποδείξουν ότι ένας δικτυακός τόπος διαθέτει πιστοποιητικό EV. Τα προγράμματα περιήγησης μπορούν επίσης να χρωματίζουν είτε πλήρως είτε εν μέρει τη γραμμή διευθύνσεων με πράσινο χρώμα. Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security αποκρυπτογραφεί και παρακολουθεί κρυπτογραφημένες συνδέσεις με τοποθεσίες web που χρησιμοποιούν πιστοποιητικό EV.

	Εάν το πλαίσιο ελέγχου δεν είναι επιλεγμένο, το Kaspersky Total Security δεν έχει πρόσβαση στα περιεχόμενα της κυκλοφορίας HTTPS. Για αυτόν τον λόγο, η εφαρμογή παρακολουθεί την κυκλοφορία HTTPS μόνο με βάση τη διεύθυνση της τοποθεσίας web, για παράδειγμα, https://facebook.com. Εάν ανοίγετε έναν δικτυακό τόπο με πιστοποιητικό EV για πρώτη φορά, η κρυπτογραφημένη σύνδεση θα αποκρυπτογραφείται, ανεξάρτητα από το εάν είναι επιλεγμένο ή όχι το πλαίσιο ελέγχου.
Ρυθμίσεις διακομιστή μεσολάβησης	Ρυθμίσεις του διακομιστή μεσολάβησης που χρησιμοποιείται για πρόσβαση στο Διαδίκτυο των χρηστών υπολογιστών- πελατών. Το Kaspersky Total Security χρησιμοποιεί αυτές τις ρυθμίσεις για ορισμένα στοιχεία προστασίας, συμπεριλαμβανομένης της ενημέρωσης βάσεων δεδομένων και λειτουργικών μονάδων εφαρμογών. Για αυτόματη διαμόρφωση διακομιστή μεσολάβησης, το Kaspersky Total Security χρησιμοποιεί το ποωτόκολλο WPAD
	(Web Proxy Auto-Discovery Protocol). Εάν η διεύθυνση IP του διακομιστή μεσολάβησης δεν μπορεί να προσδιοριστεί χρησιμοποιώντας αυτό το πρωτόκολλο, το Kaspersky Total Security χρησιμοποιεί τη διεύθυνση διακομιστή μεσολάβησης που καθορίζεται στις ρυθμίσεις του προγράμματος περιήγησης Microsoft Internet Explorer.
Σάρωση ασφαλούς κυκλοφορίας σε εφαρμογές Mozilla	Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security σαρώνει την κρυπτογραφημένη κυκλοφορία στο πρόγραμμα περιήγησης Mozilla Firefox και στο πρόγραμμα email Thunderbird. Η πρόσβαση σε ορισμένες τοποθεσίες web μέσω του πρωτοκόλλου HTTPS ενδέχεται να είναι αποκλεισμένη.
	Το Kaspersky Total Security χρησιμοποιεί το πιστοποιητικό ρίζας Kaspersky για την αποκρυπτογράφηση και ανάλυση της κρυπτογραφημένης κυκλοφορίας. Μπορείτε να επιλέξετε τον χώρο αποθήκευσης πιστοποιητικών που θα περιλαμβάνει το πιστοποιητικό ρίζας Kaspersky.
	 Χρήση του χώρου αποθήκευσης πιστοποιητικών των Windows. Το πιστοποιητικό ρίζας Kaspersky προστίθεται σε αυτόν τον χώρο αποθήκευσης κατά την εγκατάσταση του Kaspersky Total Security.

 Χρήση του χώρου αποθήκευσης πιστοποιητικών του Mozilla. Τα Mozilla Firefox και Thunderbird χρησιμοποιούν τους δικούς τους χώρους αποθήκευσης πιστοποιητικών. Εάν είναι επιλεγμένος ο χώρος αποθήκευσης πιστοποιητικών Mozilla, πρέπει να προσθέσετε με μη αυτόματο τρόπο το πιστοποιητικό ρίζας Kaspersky σε αυτόν τον χώρο πιστοποιητικών μέσω των ιδιοτήτων του προγράμματος περιήγησης.

Διαχείριση ρυθμίσεων εφαρμογής

Ρυθμίσεις	Περιγραφή
Εισαγωγή	Εξαγωγή των ρυθμίσεων της εφαρμογής από ένα αρχείο σε μορφή CFG και εφαρμογή τους.
Εξαγωγή	Αποθήκευση των τρεχουσών ρυθμίσεων της εφαρμογής σε ένα αρχείο μορφής CFG.
Επαναφορά	Μπορείτε να επαναφέρετε οποιαδήποτε στιγμή τις προεπιλεγμένες ρυθμίσεις της εφαρμογής που συνιστώνται από την Kaspersky για το Kaspersky Total Security. Όταν γίνεται επαναφορά των ρυθμίσεων, ορίζεται για όλα τα στοιχεία προστασίας το επίπεδο ασφάλειας Συνιστάται .

Τείχος προστασίας

Ρυθμίσεις	Περιγραφή
Να εμφανίζονται ειδοποιήσεις για τρωτά σημεία στα	Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security εμφανίζει ειδοποιήσεις όταν εντοπίζονται τρωτά σημεία σε ένα δίκτυο Wi-Fi.
δίκτυα Wi-Fi	Η πρόσβαση σε αυτό το πλαίσιο ελέγχου είναι δυνατή αν το Kaspersky VPN Secure Connection δεν είναι εγκατεστημένο στον υπολογιστή.
	Κάνοντας κλικ στη σύνδεση Επιλογή κατηγοριών , ανοίγει το παράθυρο Κατηγορίες στο οποίο μπορείτε να καθορίσετε τους τύπους τρωτών σημείων σε δίκτυα Wi-Fi. Η εφαρμογή σάς ειδοποιεί όταν προσπαθείτε να συνδεθείτε σε δίκτυο Wi-Fi που έχει ένα συγκεκριμένο τρωτό σημείο.
Να επιτρέπονται	Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, το Τείχος προστασίας

οι συνδέσεις σε τυχαίες θύρες για λειτουργία ενεργού FTP	επιτρέπει να γίνονται συνδέσεις στον υπολογιστή σας σε τυχαίες θύρες, εάν η εναλλαγή στη λειτουργία ενεργού FTP εντοπίστηκε στη σύνδεση κεντρικού υπολογιστή.
Να μην απενεργοποιείται το Τείχος προστασίας μέχρι το λειτουργικό σύστημα να τερματιστεί εντελώς	Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Τείχος προστασίας δεν σταματά να λειτουργεί έως ότου τερματιστεί πλήρως το λειτουργικό σύστημα.
Αποκλεισμός συνδέσεων δικτύου αν ο χρήστης δεν μπορεί να ερωτηθεί για ενέργεια	Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Τείχος προστασίας δεν σταματά όταν δεν έχει φορτωθεί η διασύνδεση του Kaspersky Total Security.
Κανόνες εφαρμογής	Κάνοντας κλικ σε αυτήν τη σύνδεση, ανοίγει το παράθυρο Κανόνες δικτύου εφαρμογής . Αυτό το παράθυρο εμφανίζει πληροφορίες που σχετίζονται με τον έλεγχο της δραστηριότητας δικτύου των εφαρμογών και των ομάδων εφαρμογών.
	το στοιχείο Ελεγχος εφαρμογών ροθμίζει τη οραστηριοτητά δικτύου των εφαρμογών σύμφωνα με τους κανόνες δικτύου των εφαρμογών και των ομάδων εφαρμογών.
	Μπορείτε να ρυθμίσετε τις παραμέτρους δικαιωμάτων για δραστηριότητα δικτύου μιας εφαρμογής ή ομάδας εφαρμογών μέσω του μενού ενός κελιού στη στήλη Δίκτυο . Τα στοιχεία μενού περιγράφονται στην ενότητα <u>Κανόνες ελέγχου εφαρμογών</u> . Επιλέγοντας Λεπτομέρειες και κανόνες στο μενού περιβάλλοντος μιας σειράς, μπορείτε να προχωρήσετε στη διαμόρφωση <u>κανόνων δικτύου για μια εφαρμογή ή ομάδα</u>
Κανόνες πακέτου	<u>Εφαρμογων</u> . Κάνοντας κλικ σε αυτήν τη σύνδεση, ανοίγει το παράθυρο Κανόνες πακέτου . Από προεπιλογή, το παράθυρο εμφανίζει προκαθορισμένους κανόνες πακέτων δικτύου που συνιστούν οι
δικτύου αν ο χρήστης δεν μπορεί να ερωτηθεί για ενέργεια Κανόνες εφαρμογής Κανόνες πακέτου	 Κάνοντας κλικ σε αυτήν τη σύνδεση, ανοίγει το παράθυρο Κανόνες δικτύου εφαρμογής. Αυτό το παράθυρο εμφανίζει πληροφορίες που σχετίζονται με τον έλεγχο της δραστηριότητας δικτύου των εφαρμογών και των ομάδων εφαρμογών. Το στοιχείο Έλεγχος εφαρμογών ρυθμίζει τη δραστηριότητα δικτύου των εφαρμογών σύμφωνα με τους κανόνες δικτύου των εφαρμογών και των ομάδων εφαρμογών. Μπορείτε να ρυθμίσετε τις παραμέτρους δικαιωμάτων για δραστηριότητα δικτύου μιας εφαρμογής ή ομάδας εφαρμογών μέσω του μενού ενός κελιού στη στήλη Δίκτυο. Τα στοιχεία μενού περιγράφονται στην ενότητα Κανόνες ελέγχου εφαρμογών. Επιλέγοντας Λεπτομέρειες και κανόνες στο μενού περιβάλλοντος μιας σειράς, μπορείτε να προχωρήσετε στη διαμόρφωση κανόνων δικτύου για μια εφαρμογή ή ομάδα εφαρμογών. Κάνοντας κλικ σε αυτήν τη σύνδεση, ανοίγει το παράθυρο Κανόνες πακέτου. Από προεπιλογή, το παράθυρο εμφανίζει προκαθορισμένους κανόνες πακέτων δικτύου που συνιστούν οι

ειδικοί της Kaspersky για βέλτιστη προστασία της κυκλοφορίας δικτύου υπολογιστών που λειτουργούν με λειτουργικά συστήματα Microsoft Windows.

Οι κανόνες πακέτων δικτύου χρησιμεύουν στην επιβολή περιορισμών στα πακέτα δικτύου, ανεξάρτητα από την εφαρμογή. Τέτοιοι κανόνες περιορίζουν την εισερχόμενη και εξερχόμενη κυκλοφορία του δικτύου μέσω συγκεκριμένων θυρών του επιλεγμένου πρωτοκόλλου δεδομένων.

Οι κανόνες πακέτων δικτύου έχουν υψηλότερη προτεραιότητα από τους κανόνες δικτύου για εφαρμογές.

Κατά την προσθήκη ή την επεξεργασία ενός κανόνα πακέτου, μπορείτε να ορίσετε τις ακόλουθες ρυθμίσεις:

- Ενέργεια:
 - Να επιτρέπεται. Το Kaspersky Total Security επιτρέπει τη σύνδεση δικτύου.
 - Αποκλεισμός. Το Kaspersky Total Security αποκλείει τη σύνδεση δικτύου.
 - Κατά κανόνες εφαρμογής. Το Kaspersky Total Security δεν επεξεργάζεται τη ροή δεδομένων σύμφωνα με τον κανόνα του πακέτου, αλλά αντ' αυτού εφαρμόζει έναν κανόνα εφαρμογής (βλέπε Κανόνες εφαρμογής παραπάνω).
- Όνομα.
- Κατεύθυνση:
 - Εισερχόμενη. Το Kaspersky Total Security εφαρμόζει τον κανόνα στις συνδέσεις δικτύου που ανοίγουν από τον απομακρυσμένο υπολογιστή.
 - Εξερχόμενη. Το Kaspersky Total Security εφαρμόζει τον κανόνα στη σύνδεση δικτύου που ανοίγει από τον υπολογιστή σας.

- Εισερχόμενη/Εξερχόμενη. Το Kaspersky Total Security εφαρμόζει τον κανόνα τόσο στα εισερχόμενα όσο και στα εξερχόμενα πακέτα δεδομένων ή ροές δεδομένων, ανεξάρτητα από το ποιος υπολογιστής (ο δικός σας ή ένας απομακρυσμένος υπολογιστής) ξεκίνησε τη σύνδεση δικτύου.
- Εισερχόμενη (πακέτο). Το Kaspersky Total Security εφαρμόζει τον κανόνα στα πακέτα δεδομένων που λαμβάνει ο υπολογιστής σας.
- Εξερχόμενη (πακέτο). Το Kaspersky Total Security εφαρμόζει τον κανόνα στα πακέτα δεδομένων που αποστέλλονται από τον υπολογιστή σας.
- Πρωτόκολλο.
- Ρυθμίσεις ICMP. Μπορείτε να καθορίσετε τον τύπο και τον κωδικό των πακέτων δεδομένων που θα σαρωθούν. Η ενότητα ρυθμίσεων είναι διαθέσιμη αν τα πρωτόκολλα ICMP ή ICMPv6 είναι επιλεγμένα.
- Απομακρυσμένες θύρες (θύρες απομακρυσμένου υπολογιστή).
- Τοπικές θύρες (θύρες του υπολογιστή σας).

Μπορείτε να καθορίσετε ένα εύρος απομακρυσμένων ή τοπικών θυρών (για παράδειγμα, 6660-7000), να παραθέσετε πολλές θύρες διαχωρισμένες με κόμματα ή να συνδυάσετε και τις δύο μεθόδους (για παράδειγμα, 80-83,443,1080).

- Διεύθυνση:
 - Οποιαδήποτε διεύθυνση.
 - Διευθύνσεις υποδικτύων. Το Kaspersky Total Security θα εφαρμόσει τον κανόνα σε διευθύνσεις IP όλων των δικτύων που είναι συνδεδεμένα τη συγκεκριμένη στιγμή και είναι του καθορισμένου τύπου (Δημόσιο, Τοπικό ή

Αξιόπιστο). Ο τύπος δικτύου μπορεί να επιλεγεί από την αναπτυσσόμενη λίστα που εμφανίζεται παρακάτω εάν έχει ενεργοποιηθεί η επιλογή **Διευθύνσεις υποδικτύων**.

- Διευθύνσεις από τη λίστα. Το Kaspersky Total Security εφαρμόζει τον κανόνα σε διευθύνσεις IP εντός του καθορισμένου εύρους. Μπορείτε να καθορίσετε διευθύνσεις IP στα πεδία Απομακρυσμένες διευθύνσεις και Τοπικές διευθύνσεις, τα οποία εμφανίζονται παρακάτω εάν είναι ενεργοποιημένη η επιλογή Διευθύνσεις IP θα πρέπει να διαχωρίζονται με κόμμα.
- Κατάσταση. Το τείχος προστασίας εφαρμόζει μόνο κανόνες πακέτου που έχουν την κατάσταση Ενεργό. Μπορείτε να ορίσετε την κατάσταση Ανενεργό για να απενεργοποιήσετε προσωρινά έναν κανόνα πακέτου χωρίς να τον διαγράψετε από τη λίστα κανόνων πακέτου.
- Προσαρμογείς δικτύου που διασχίζονται από πακέτα δικτύου.
- Χρήση του TTL. Το Kaspersky Total Security ελέγχει τη μετάδοση πακέτων δικτύου των οποίων ο χρόνος ζωής (TTL) δεν υπερβαίνει την καθορισμένη τιμή.
- Καταγραφή συμβάντων σε μια <u>αναφορά Kaspersky Total</u> <u>Security</u>.

Για να προσθέσετε γρήγορα έναν κανόνα, μπορείτε να επιλέξετε ένα από τα προκαθορισμένα πρότυπα στην αναπτυσσόμενη λίστα στο κάτω μέρος του παραθύρου.

Διαθέσιμα δίκτυα Κάνοντας κλικ σε αυτήν τη σύνδεση, ανοίγει το παράθυρο **Δίκτυα** το οποίο περιέχει μια λίστα συνδέσεων δικτύου που εντοπίζονται στον υπολογιστή από το Τείχος προστασίας.

Στη λίστα, μπορείτε να αλλάξετε τον τύπο δικτύου (Δημόσιο, Αξιόπιστο ή Τοπικό) χρησιμοποιώντας το μενού στο κελί **Τύπος** δικτύου. Μπορείτε να επεξεργαστείτε τις ρυθμίσεις δικτύου στο παράθυρο **Ιδιότητες δικτύου**, το οποίο μπορείτε να ανοίξετε κάνοντας διπλό κλικ στη σειρά του δικτύου. Ο τύπος Δημόσιο εκχωρείται στο Διαδίκτυο από προεπιλογή. Δεν μπορείτε να αλλάξετε τον τύπο δικτύου ή άλλες ρυθμίσεις για το Διαδίκτυο.

Στο παράθυρο **Ιδιότητες δικτύου**, μπορείτε να επεξεργαστείτε τις ακόλουθες ρυθμίσεις δικτύου:

- Όνομα δικτύου.
- Τύπος δικτύου.
- Εμφάνιση ειδοποιήσεων σχετικά με τα ακόλουθα:
 - Σύνδεση στο δίκτυο.
 - Αλλαγμένη διεύθυνση MAC (για παράδειγμα, εάν αντικατασταθεί ο προσαρμογέας δικτύου).
 - Αλλαγή ζεύξης διεύθυνσης MAC/διεύθυνσης IP (για παράδειγμα, όταν η υπηρεσία DHCP εκχωρεί διαφορετική διεύθυνση IP).
- Επιλογή εκτυπωτή που θα πρέπει να συνιστάται από προεπιλογή κατά τη σύνδεση σε αυτό το δίκτυο. Αυτή η ρύθμιση είναι διαθέσιμη εάν έχει εγκατασταθεί εκτυπωτής στο λειτουργικό σύστημα του υπολογιστή σας.
- Λίστα πρόσθετων υποδικτύων (διαχωρισμένα με κόμματα).

Κανόνες εφαρμογής / Κανόνες ομάδας

Ρυθμίσεις	Περιγραφή
Αρχείο (μόνο στο παράθυρο Κανόνες εφαρμογής)	Πληροφορίες αναφοράς για μια εφαρμογή και για το εκτελέσιμο αρχείο της εφαρμογής. Το Kaspersky Total Security λαμβάνει πληροφορίες σχετικά με μια εφαρμογή από το εκτελέσιμο αρχείο της εφαρμογής και από το <u>Kaspersky Security Network</u> .
Αρχεία και μητρώο	Κανόνες πρόσβασης στα κλειδιά μητρώου του συστήματος και στα αρχεία που σχετίζονται με τη λειτουργία του λειτουργικού συστήματος

συστήματος ή με τα προσωπικά σας δεδομένα.

Οι μεμονωμένες ρυθμίσεις πρόσβασης για λειτουργίες ανάγνωσης, εγγραφής, δημιουργίας και διαγραφής μπορούν να καθοριστούν ανεξάρτητα χρησιμοποιώντας το μενού στα κελιά των αντίστοιχων στηλών πίνακα. Τα στοιχεία μενού περιγράφονται στην ενότητα <u>Κανόνες</u> <u>ελέγχου εφαρμογών</u>.

Δικαιώματα Δικαιώματα πρόσβασης σε πόρους και διαδικασίες του λειτουργικού συστήματος και δικαιώματα εκκίνησης. Μπορείτε να ορίσετε δικαιώματα πρόσβασης χρησιμοποιώντας το μενού στα κελιά της στήλης **Ενέργεια**. Τα στοιχεία μενού περιγράφονται στην ενότητα Κανόνες ελέγχου εφαρμογών.

ΚανόνεςΚανόνες που εφαρμόζονται από το Kaspersky Total Security για τηδικτύουρύθμιση της δραστηριότητας δικτύου μιας εφαρμογής ή μιας ομάδας
εφαρμογών.

Από προεπιλογή, η λίστα εμφανίζει τους προκαθορισμένους κανόνες δικτύου εφαρμογών που συνιστούν οι ειδικοί της Kaspersky. Δεν μπορείτε να διαγράψετε ή να επεξεργαστείτε προκαθορισμένους κανόνες δικτύου (εκτός από την αλλαγή της ενέργειας στη στήλη **Δικαιώματα**. Ανατρέξτε στην περιγραφή των διαθέσιμων ενεργειών στην ενότητα <u>Κανόνες Ελέγχου εφαρμογών</u>).

Κατά την προσθήκη ή την επεξεργασία ενός κανόνα, μπορείτε να ορίσετε τις ακόλουθες ρυθμίσεις:

- Ενέργεια:
 - Να επιτρέπεται. Το Kaspersky Total Security επιτρέπει τη σύνδεση δικτύου.
 - Αποκλεισμός. Το Kaspersky Total Security αποκλείει τη σύνδεση δικτύου.
 - Προτροπή χρήστη. Εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στις Ρυθμίσεις → Γενικά, το Kaspersky Total Security ζητά από τον χρήστη να αποφασίσει εάν θα επιτρέψει ή όχι τη σύνδεση δικτύου. Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, η ενέργεια επιλέγεται αυτόματα. Μπορείτε να ακολουθήσετε την υποσημείωση στο παράθυρο της εφαρμογής για να διαβάσετε ακριβώς ποια ενέργεια θα επιλεγεί.
- Όνομα.

- Κατεύθυνση:
 - Εισερχόμενη. Το Kaspersky Total Security εφαρμόζει τον κανόνα στις συνδέσεις δικτύου που ανοίγουν από τον απομακρυσμένο υπολογιστή.
 - **Εξερχόμενη**. Το Kaspersky Total Security εφαρμόζει τον κανόνα στη σύνδεση δικτύου που ανοίγει από τον υπολογιστή σας.
 - Εισερχόμενη/Εξερχόμενη. Το Kaspersky Total Security εφαρμόζει τον κανόνα τόσο στα εισερχόμενα όσο και στα εξερχόμενα πακέτα δεδομένων ή ροές δεδομένων, ανεξάρτητα από το ποιος υπολογιστής (ο δικός σας ή ένας απομακρυσμένος υπολογιστής) ξεκίνησε τη σύνδεση δικτύου.
- Πρωτόκολλο.
- Ρυθμίσεις ICMP. Μπορείτε να καθορίσετε τον τύπο και τον κωδικό των πακέτων δεδομένων που θα σαρωθούν. Η ενότητα ρυθμίσεων είναι διαθέσιμη αν τα πρωτόκολλα ICMP ή ICMPv6 είναι επιλεγμένα.
- Απομακρυσμένες θύρες (θύρες απομακρυσμένου υπολογιστή).
- Τοπικές θύρες (θύρες του υπολογιστή σας).

Μπορείτε να καθορίσετε ένα εύρος απομακρυσμένων ή τοπικών θυρών (για παράδειγμα, 6660-7000), να παραθέσετε πολλές θύρες διαχωρισμένες με κόμματα ή να συνδυάσετε και τις δύο μεθόδους (για παράδειγμα, 80-83,443,1080).

- Διεύθυνση:
 - Οποιαδήποτε διεύθυνση.
 - Διευθύνσεις υποδικτύων. Το Kaspersky Total Security θα εφαρμόσει τον κανόνα σε διευθύνσεις IP όλων των δικτύων που είναι συνδεδεμένα τη συγκεκριμένη στιγμή και είναι του καθορισμένου τύπου (Δημόσιο, Τοπικό ή Αξιόπιστο). Ο τύπος δικτύου μπορεί να επιλεγεί από την αναπτυσσόμενη λίστα που εμφανίζεται παρακάτω εάν έχει ενεργοποιηθεί η επιλογή Διευθύνσεις υποδικτύων.

	 Διευθύνσεις από τη λίστα. Το Kaspersky Total Security εφαρμόζει τον κανόνα σε διευθύνσεις IP εντός του καθορισμένου εύρους. Μπορείτε να καθορίσετε διευθύνσεις IP στο πεδίο Απομακρυσμένες διευθύνσεις, το οποίο εμφανίζεται παρακάτω εάν είναι ενεργοποιημένη η επιλογή Διευθύνσεις από τη λίστα.
	 Προσαρμογείς δικτύου που διασχίζονται από πακέτα δικτύου.
	 Χρήση του TTL. Το Kaspersky Total Security ελέγχει τη μετάδοση πακέτων δικτύου των οποίων ο χρόνος ζωής (TTL) δεν υπερβαίνει την καθορισμένη τιμή.
	• Καταγραφή συμβάντων σε μια <u>αναφορά Kaspersky Total Security</u> .
	Για να προσθέσετε γρήγορα έναν κανόνα, μπορείτε να επιλέξετε ένα από τα προκαθορισμένα πρότυπα στην αναπτυσσόμενη λίστα στο κάτω μέρος του παραθύρου.
Εξαιρέσεις (μόνο στο παράθυρο Κανόνες εφαρμογής)	Μπορείτε να επιλέξετε κανόνες που θα χρησιμοποιηθούν από το Kaspersky Total Security για την εξαίρεση μιας εφαρμογής από τις σαρώσεις:
	 Να μη γίνει σάρωση ανοιγμένων αρχείων.
	 Να μην παρακολουθείται η δραστηριότητα της εφαρμογής. Ο Έλεγχος εφαρμογών δεν παρακολουθεί καμία δραστηριότητα εφαρμογής.
	 Να μην γίνει μεταβίβαση περιορισμών της γονικής διεργασίας (της εφαρμογής) Εάν οι περιορισμοί μιας γονικής διεργασίας δεν μεταβιβάζονται, η δραστηριότητα της εφαρμογής παρακολουθείται σύμφωνα με τους κανόνες που ορίσατε ή σύμφωνα με τους κανόνες της ομάδας αξιόπιστων εφαρμογών στην οποία ανήκει η εφαρμογή.
	 Να μην παρακολουθείται η δραστηριότητα των θυγατρικών εφαρμογών.
	 Μην αποκλείετε την αλληλεπίδραση με τη διεπαφή Kaspersky Total Security. Η εφαρμογή επιτρέπεται να διαχειρίζεται το Kaspersky Total Security χρησιμοποιώντας τη γραφική διεπαφή Kaspersky Total Security. Μπορεί να χρειαστεί να επιτρέψετε σε μια εφαρμογή να διαχειριστεί το περιβάλλον εργασίας του Kaspersky Total Security όταν χρησιμοποιείτε μια εφαρμογή σύνδεσης απομακρυσμένης επιφάνειας εργασίας ή μια εφαρμογή που υποστηρίζει τη λειτουρνία

συσκευής εισόδου δεδομένων. Αυτές οι συσκευές μπορεί να είναι, για παράδειγμα, ένα touch pad ή tablet.

Να μην γίνει σάρωση όλης της κυκλοφορίας (ή της κρυπτογραφημένης κυκλοφορίας). Ανάλογα με την ενεργοποιημένη επιλογή (Να μην γίνει σάρωση όλης της κυκλοφορίας ή Να μην γίνει σάρωση κρυπτογραφημένης κυκλοφορίας), το Kaspersky Total Security αποκλείει τη σάρωση όλης της κυκλοφορίας δικτύου της εφαρμογής ή της κυκλοφορίας που μεταδίδεται μέσω SSL. Η τιμή αυτής της ρύθμισης δεν επηρεάζει τη λειτουργία του Τείχους προστασίας: Το Τείχος προστασίας σαρώνει την κυκλοφορία εφαρμογής σύμφωνα με τις ρυθμίσεις του Τείχους προστασίας. Οι εξαιρέσεις επηρεάζουν την Προστασία email από ιούς, την Προστασία από ιούς στο Web και το Πρόγραμμα Anti-Spam. Μπορείτε να καθορίσετε τις διευθύνσεις ΙΡ ή τις θύρες δικτύου στις οποίες πρέπει να ισχύει ο περιορισμός ελέγχου κυκλοφορίας.

Ιστορικό Πληροφορίες αναφοράς σχετικά με τις ενέργειες που εκτελέστηκαν στην εφαρμογή, όπως εκκίνηση της εφαρμογής ή εκχώρηση ομάδας αξιοπιστίας ?.
 Κανόνες εφαρμογής)

Κανόνες Ελέγχου εφαρμογών

Ένας *κανόνας* είναι ένα σύνολο αντιδράσεων από τον Έλεγχο εφαρμογών ως απόκριση σε ενέργειες που εκτελεί μια εφαρμογή σε διάφορες κατηγορίες πόρων λειτουργικού συστήματος και προσωπικά δεδομένα.

Είναι δυνατές οι ακόλουθες αποκρίσεις του Ελέγχου εφαρμογών σε ενέργειες εφαρμογών:

 Μεταβίβαση. Ο Έλεγχος Εφαρμογών ρυθμίζει τη δραστηριότητα μιας εφαρμογής βάσει ενός κανόνα που ορίστηκε για την ίδια κατάσταση την οποία ο Έλεγχος Εφαρμογών εκχώρησε στην εφαρμογή.

Αυτή η ενέργεια εφαρμόζεται ως προεπιλογή. Από προεπιλογή, ο Έλεγχος εφαρμογών μεταβιβάζει δικαιώματα πρόσβασης από την κατάσταση που ο Έλεγχος εφαρμογών εκχώρησε στη συγκεκριμένη εφαρμογή.

Εάν επεξεργαστήκατε έναν κανόνα για μια εφαρμογή, οι ρυθμίσεις του κανόνα εφαρμογής θα έχουν υψηλότερη προτεραιότητα από τις ρυθμίσεις του κανόνα για την κατάσταση που εκχωρήθηκε στην εφαρμογή.

- Να επιτρέπεται. Ο Έλεγχος εφαρμογών επιτρέπει σε μια εφαρμογή να εκτελεί την ενέργεια.
- Αποκλεισμός. Ο Έλεγχος εφαρμογών δεν επιτρέπει σε μια εφαρμογή να εκτελέσει την ενέργεια.
- Προτροπή χρήστη. Εάν δεν είναι επιλεγμένο το πλαίσιο ελέγχου Αυτόματη εκτέλεση των συνιστώμενων ενεργειών στις Ρυθμίσεις → Γενικά ο Έλεγχος εφαρμογών ζητά από τον χρήστη να αποφασίσει. Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, η ενέργεια επιλέγεται αυτόματα. Μπορείτε να ακολουθήσετε την υποσημείωση στο παράθυρο της εφαρμογής για να διαβάσετε ακριβώς ποια ενέργεια θα επιλεγεί.
- Καταγραφή συμβάντων. Ο Έλεγχος εφαρμογών καταγράφει πληροφορίες σχετικά με τη δραστηριότητα της εφαρμογής και τις αποκρίσεις σε αυτήν σε μια αναφορά. Σε μια αναφορά μπορούν να προστεθούν και πληροφορίες, εκτός από οποιαδήποτε άλλη ενέργεια που αναλαμβάνεται από τον Έλεγχος εφαρμογών.

Πρόσθετα

Ρυθμίσεις	Περιγραφή
Χρήση λειτουργίας αναπαράστασης υλικού εάν είναι διαθέσιμη	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, χρησιμοποιείται η εικονικοποίηση υλικού (hypervisor ?) για τη λειτουργία στο Προστατευμένο πρόγραμμα περιήγησης. Η εφαρμογή χρησιμοποιεί την τεχνολογία hypervisor για πρόσθετη προστασία απέναντι σε προηγμένο κακόβουλο λογισμικό που μπορεί να υποκλέψει προσωπικά δεδομένα με χρήση του προχείρου ή phishing. Αυτό το πλαίσιο ελέγχου εμφανίζεται όταν η εφαρμογή εγκαθίσταται σε έκδοση 64-bit των Windows 8, Windows 8.1 και Windows 10. Για περισσότερες λεπτομέρειες σχετικά με την εικονικοποίηση υλικού και τον τρόπο που λειτουργεί, κάντε κλικ στη σύνδεση.
Καταχώρηση σε ασφαλές πληκτρολόγιο	Η Καταχώρηση σε ασφαλές πληκτρολόγιο σας βοηθά να εμποδίσετε τους εγκληματίες του κυβερνοχώρου να παρακολουθούν τα δεδομένα που εισάγετε από το πληκτρολόγιο κατά την επίσκεψη σε ιστότοπους (για περισσότερες λεπτομέρειες, ανατρέξτε στην ενότητα <u>Σχετικά με την Καταχώρηση σε ασφαλές πληκτρολόγιο</u>). Κάντε κλικ στη σύνδεση Επεξεργασία κατηγοριών για να ανοίξετε το παράθυρο Κατηγορίες . Σε αυτό το παράθυρο, μπορείτε να καθορίσετε σε ποιες τοποθεσίες web χρειάζεται να ενεργοποιήσετε την Καταχώρηση σε ασφαλές πληκτρολόγιο.

	Κάντε κλικ στη σύνδεση Διαχείριση εξαιρέσεων στο παράθυρο Κατηγορίες για να δημιουργήσετε λίστες τοποθεσιών web στις οποίες θέλετε να ενεργοποιήσετε ή να απενεργοποιήσετε την Καταχώρηση σε ασφαλές πληκτρολόγιο ανεξάρτητα από τις επιλεγμένες κατηγορίες τοποθεσιών web. Μπορείτε να χρησιμοποιήσετε μάσκες κατά την προσθήκη εξαιρέσεων.
Πληκτρολόγιο οθόνης	Πολλά από τα προγράμματα που κατηγοριοποιούνται ως λογισμικό υποκλοπής έχουν τη δυνατότητα λήψης στιγμιότυπων οθόνης, τα οποία στη συνέχεια μεταδίδονται σε κάποιον εισβολέα για περαιτέρω ανάλυση και κλοπή προσωπικών δεδομένων του χρήστη. Το Πληκτρολόγιο οθόνης προστατεύει τα προσωπικά δεδομένα που καταχωρούνται από απόπειρες υποκλοπής με λήψη στιγμιοτύπων οθόνης. (Για περισσότερες λεπτομέρειες, ανατρέξτε στην ενότητα <u>Σχετικά με το Πληκτρολόγιο οθόνης</u>).
	Για να βεβαιωθείτε ότι το Πληκτρολόγιο οθόνης είναι ενεργοποιημένο, πρέπει να κάνετε επανεκκίνηση του υπολογιστή σας μετά την εγκατάσταση του Kaspersky Total Security.
	Μπορείτε να επιλέξετε πώς θα μπορείτε να ανοίγετε το Πληκτρολόγιο οθόνης:
	 Άνοιγμα του Πληκτρολογίου οθόνης πατώντας τον συνδυασμό πλήκτρων CTRL+ALT+SHIFT+P.
	 Εμφάνιση εικονιδίου γρήγορης εκκίνησης σε πεδία εισαγωγής δεδομένων. Το εικονίδιο γρήγορης εκκίνησης του Πληκτρολογίου οθόνης εμφανίζεται στα πεδία εισαγωγής κωδικού πρόσβασης στις ιστοσελίδες.
	Κάντε κλικ στη σύνδεση Επεξεργασία κατηγοριών για να ανοίξετε το παράθυρο Κατηγορίες . Σε αυτό το παράθυρο, μπορείτε να καθορίσετε σε ποιες τοποθεσίες web θα πρέπει να εμφανίζεται το εικονίδιο γρήγορης εκκίνησης.

	Κάντε κλικ στη σύνδεση Διαχείριση εξαιρέσεων στο παράθυρο Κατηγορίες για να δημιουργήσετε λίστες τοποθεσιών web στις οποίες θέλετε να ενεργοποιήσετε ή να απενεργοποιήσετε το εικονίδιο γρήγορης εκκίνησης του Πληκτρολογίου οθόνης ανεξάρτητα από τις επιλεγμένες κατηγορίες τοποθεσιών web. Μπορείτε να χρησιμοποιήσετε μάσκες κατά την προσθήκη εξαιρέσεων.
Εμφάνιση της ισχύος του κωδικό πρόσβασης στο πρόγραμμα περιήγησης	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου, το Kaspersky Total Security ελέγχει την ισχύ ενός κωδικού πρόσβασης που εισάγετε στο πρόγραμμα περιήγησης για πρώτη φορά και σας ειδοποιεί σχετικά.
Προστασία από τη χρήση ίδιων κωδικών πρόσβασης	Όταν εισάγετε έναν κωδικό πρόσβασης σε μια τοποθεσία web όπου η ασφάλεια του κωδικού πρόσβασης είναι ιδιαίτερα σημαντική (όπως σε ένα κοινωνικό δίκτυο), το Kaspersky Total Security σάς ζητά να ενεργοποιήσετε την προστασία από τη χρήση των ίδιων κωδικών πρόσβασης.
	Εάν είναι επιλεγμένο το πλαίσιο ελέγχου Να γίνεται προειδοποίηση σχετικά με τη χρήση ίδιων κωδικών πρόσβασης σε τοποθεσίες web, η προστασία από τη χρήση των ίδιων κωδικών πρόσβασης είναι ενεργοποιημένη. Μπορείτε να επιλέξετε τις κατηγορίες των τοποθεσιών web που θα πρέπει να προστατεύονται από τη χρήση των ίδιων κωδικών πρόσβασης. Αυτές οι κατηγορίες περιλαμβάνουν τοποθεσίες web τραπεζών και συστημάτων πληρωμής, τοποθεσίες web κοινωνικών δικτύων και τοποθεσίες web υπηρεσιών αλληλογραφίας.
	Μπορείτε να κάνετε κλικ στη σύνδεση Διαγραφή αποθηκευμένων δεδομένων για να διαγράψετε όλους τους κωδικούς πρόσβασης που έχουν αποθηκευτεί στο παρελθόν.

Παράθυρο επιλογής αρχείων προς διαγραφή

Ανάπτυξη όλων | Σύμπτυξη όλων

Πεδίο εισαγωγής της διαδρομής στο αρχείο ή τον φάκελο ?

Το πεδίο περιλαμβάνει τη διαδρομή προς ένα αρχείο ή φάκελο για οριστική διαγραφή. Μπορείτε να επιλέξετε ένα αρχείο ή έναν φάκελο από τη δενδροειδή δομή που βρίσκεται πάνω από το πεδίο εισαγωγής ή να το καθορίσετε χειροκίνητα.

Παράθυρο Επιλογή δεδομένων για κρυπτογράφηση

Ανάπτυξη όλων | Σύμπτυξη όλων

Πεδίο εισαγωγής της διαδρομής στο αρχείο ή τον φάκελο ?

Το πεδίο περιλαμβάνει τη διαδρομή προς ένα αρχείο ή φάκελο που θέλετε να προσθέσετε σε θάλαμο δεδομένων. Μπορείτε να επιλέξετε ένα αρχείο ή έναν φάκελο από τη δενδροειδή δομή που βρίσκεται πάνω από το πεδίο εισαγωγής ή να το καθορίσετε χειροκίνητα.

Παράθυρο Άνοιγμα θαλάμου δεδομένων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κωδικός πρόσβασης θαλάμου δεδομένων 💿</u>

Κωδικός πρόσβασης στα αρχεία του θαλάμου δεδομένων.

Άνοιγμα στην Εξερεύνηση 🖓

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένας φάκελος στην Εξερεύνηση που περιέχει τη λίστα με τα αρχεία και τους φακέλους που έχουν αποθηκευτεί στον θάλαμο δεδομένων.

Παράθυρο Διαγραφή θαλάμου δεδομένων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Κωδικός πρόσβασης θαλάμου δεδομένων 💿</u>

Κωδικός πρόσβασης στα αρχεία του θαλάμου δεδομένων.

<u>Διαγραφή θαλάμου δεδομένων 🖓</u>

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security διαγράφει τον θάλαμο δεδομένων και όλα τα αρχεία που είναι αποθηκευμένα σε αυτόν.

Τα αρχεία και οι φάκελοι στον θάλαμο δεδομένων διαγράφονται οριστικά.

Παράθυρο Μετονομασία θαλάμου δεδομένων

Ανάπτυξη όλων | Σύμπτυξη όλων

Νέο όνομα για τον θάλαμο δεδομένων 🖓

Το νέο όνομα που θα εκχωρηθεί στον θάλαμο δεδομένων.

<u>Αποθήκευση</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security εκχωρεί ένα νέο όνομα στον θάλαμο δεδομένων.

Παράθυρο Αλλαγή κωδικού πρόσβασης θαλάμου δεδομένων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Παλαιός κωδικός πρόσβασης ?</u>

Τρέχων κωδικός πρόσβασης θαλάμου δεδομένων.

<u>Νέος κωδικός πρόσβασης</u> 🖓

Νέος κωδικός πρόσβασης θαλάμου δεδομένων.

<u>Επιβεβαίωση κωδικού πρόσβασης </u>

Πληκτρολογήστε πάλι τον κωδικό πρόσβασης που εισαγάγατε στο πεδίο **Νέος κωδικός πρόσβασης**.

<u>Αποθήκευση </u>

Κάνοντας κλικ σε αυτό το κουμπί, ο τρέχων κωδικός πρόσβασης του θαλάμου δεδομένων αντικαθίσταται από τον νέο κωδικό.

Παράθυρο Επιλογή αρχείου θαλάμου δεδομένων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Πεδίο εισαγωγής της διαδρομής στο αρχείο</u> ?

Το πεδίο περιέχει τη διαδρομή προς το αρχείο του θαλάμου δεδομένων. Μπορείτε να επιλέξετε ένα αρχείο από τη δενδροειδή δομή που βρίσκεται πάνω από το πεδίο εισαγωγής ή να εισαγάγετε χειροκίνητα τη διαδρομή προς το αρχείο.

Παράθυρο Δημιουργία αντιγράφων ασφαλείας

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

Επιλογή αρχείων για αντίγραφα ασφαλείας 💿

Κάνοντας κλικ σε αυτό το κουμπί, εκκινείται ο Οδηγός δημιουργίας εργασίας αντιγράφων ασφαλείας.

Να γίνει επαναφορά των αρχείων από το σύνολο των αντιγράφων ασφαλείας μου 💿

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο με τη λίστα των χώρων αποθήκευσης αντιγράφων ασφαλείας. Σε αυτό το παράθυρο μπορείτε να επιλέξετε έναν χώρο αποθήκευσης με ένα σύνολο αντιγράφων ασφαλείας που έχετε δημιουργήσει στο παρελθόν.



Τα κουμπιά μπορούν να χρησιμοποιηθούν για τη διαχείριση της διαδικασίας δημιουργίας αντιγράφου ασφαλείας:

- διακοπή μιας εργασίας δημιουργίας αντιγράφων ασφαλείας. Το κουμπί αυτό εμφανίζεται εάν εκείνη τη στιγμή εκτελείται ή είναι σε παύση μια εργασία δημιουργίας αντιγράφων ασφαλείας.

– παύση εργασίας δημιουργίας αντιγράφων ασφαλείας. Το κουμπί αυτό εμφανίζεται εάν εκείνη τη στιγμή εκτελείται μια εργασία δημιουργίας αντιγράφων ασφαλείας.

- εκκίνηση μιας εργασίας δημιουργίας αντιγράφων ασφαλείας ή συνέχιση μιας εργασίας δημιουργίας αντιγράφων ασφαλείας που έχει διακοπεί. Αυτό το κουμπί είναι διαθέσιμο εάν μια εργασία δημιουργίας αντιγράφου ασφαλείας έχει ολοκληρωθεί ή διακοπεί.

Εκτέλεση δημιουργίας αντιγράφων ασφαλείας ව

Κάνοντας κλικ σε αυτό το κουμπί, ξεκινά η διαδικασία δημιουργίας αντιγράφων ασφαλείας των αρχείων. Το κουμπί αυτό εμφανίζεται εάν εκείνη τη στιγμή δεν εκτελείται εργασία δημιουργίας αντιγράφων ασφαλείας.

Κάνοντας κλικ στο κουμπί , ανοίγει ένα μενού από το οποίο μπορείτε να επιλέξετε μια πρόσθετη ενέργεια με τις καθορισμένες ρυθμίσεις δημιουργίας αντιγράφων ασφαλείας:

- Αλλαγή ρυθμίσεων ξεκινά τον οδηγό επεξεργασίας ρυθμίσεων δημιουργίας αντιγράφων ασφαλείας.
- Διαγραφή ρυθμίσεων διαγράφει τις ρυθμίσεις δημιουργίας αντιγράφων ασφαλείας.

<u>Επαναφορά αρχείων </u>?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο **Επαναφορά αρχείων από αντίγραφα ασφαλείας**. Αυτό το παράθυρο σας δίνει τη δυνατότητα να επιλέξετε αντίγραφα ασφαλείας από τα οποία θέλετε να επαναφέρετε αρχεία.

Σύνδεση στο Dropbox 🖓

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο σύνδεσης στον δικτυακό τόπο του Dropbox. Εάν δεν έχετε λογαριασμό, μπορείτε να εγγραφείτε στον δικτυακό τόπο του Dropbox.

Το κουμπί εμφανίζεται εάν δεν έχετε συνδεθεί ήδη στον δικτυακό τόπο του Dropbox από αυτόν τον υπολογιστή.

<u>Ενημέρωση κατάστασης</u> 🖓

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security συνδέεται στον online χώρο αποθήκευσης και ενημερώνει τις πληροφορίες σχετικά με το μέγεθος του χώρου και το μέγεθος των αρχείων που είναι αποθηκευμένα σε αυτόν.

Το κουμπί αυτό εμφανίζεται εάν η εφαρμογή δεν είχε καταφέρει προηγουμένως να ανακτήσει πληροφορίες σχετικά με τον online χώρο αποθήκευσης (για παράδειγμα, εάν ο υπολογιστής δεν ήταν συνδεδεμένος στο Διαδίκτυο).

<u>Λεπτομέρειες ?</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Λεπτομερείς αναφορές**. Στο παράθυρο αυτό εμφανίζονται λεπτομερέστερες πληροφορίες σχετικά με τις ολοκληρωμένες εργασίες δημιουργίας αντιγράφων ασφαλείας.

<u>Λειτουργία εκτέλεσης ?</u>

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Χρονοδιάγραμμα δημιουργίας αντιγράφων ασφαλείας**. Σε αυτό το παράθυρο μπορείτε να αλλάξετε τον τρόπο λειτουργίας της εργασίας δημιουργίας αντιγράφων ασφαλείας.

<u>Εκκαθάριση</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο **Εκκαθάριση χώρου αποθήκευσης** στο οποίο μπορείτε να καταργήσετε τα ανεπιθύμητα αντίγραφα ασφαλείας από τον χώρο αποθήκευσης αντιγράφων ασφαλείας.

Δημιουργία αντιγράφων ασφαλείας άλλων αρχείων 💿
Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο του Οδηγού δημιουργίας εργασίας αντιγράφων ασφαλείας στο οποίο μπορείτε να προσθέσετε αρχεία για να δημιουργηθούν τα αντίγραφα ασφαλείας τους.

Επαναφορά αρχείων από σύνολο αντιγράφων ασφαλείας που δεν είναι στη λίστα 🖓

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Αναζήτηση αντιγράφων ασφαλείας**. Σε αυτό το παράθυρο μπορείτε να προσδιορίσετε έναν χώρο αποθήκευσης αντιγράφων ασφαλείας με αντίγραφα ασφαλείας που έχετε δημιουργήσει στο παρελθόν.

<u>Διαχείριση χώρων αποθήκευσης</u> 🖓

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει ένα παράθυρο με τη λίστα των διαθέσιμων χώρων αποθήκευσης αντιγράφων ασφαλείας. Σε αυτό το παράθυρο μπορείτε να επαναφέρετε αρχεία από αντίγραφο ασφαλείας στον επιλεγμένο χώρο αποθήκευσης, να επεξεργαστείτε τις ρυθμίσεις του επιλεγμένου χώρου αποθήκευσης, να διαγράψετε αυτόν τον χώρο αποθήκευσης ή να προσθέσετε έναν χώρο αποθήκευσης στη λίστα.

Παράθυρο Επιλογή φακέλου για δημιουργία αντιγράφων ασφαλείας

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Πεδίο εισαγωγής της διαδρομής στον φάκελο </u>?

Το πεδίο περιέχει την διαδρομή προς τον φάκελο για τον οποίο θα δημιουργηθεί αντίγραφο ασφαλείας. Μπορείτε να επιλέξετε έναν φάκελο από τη δενδροειδή δομή που βρίσκεται πάνω από το πεδίο εισαγωγής ή να το καθορίσετε χειροκίνητα.

Παράθυρο Βοηθητικό πρόγραμμα επαναφοράς

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Αντιγραφή του Kaspersky Restore Utility στον χώρο αποθήκευσης ?</u>

Εάν το πλαίσιο ελέγχου είναι επιλεγμένο, το Kaspersky Total Security αντιγράφει το Kaspersky Restore Utility στον χώρο αποθήκευσης κατά τη διάρκεια της διαδικασίας δημιουργίας αντιγράφου ασφαλείας. Αυτό το βοηθητικό πρόγραμμα μπορεί να χρησιμοποιηθεί για την επαναφορά αρχείων από αντίγραφα ασφαλείας όταν το Kaspersky Total Security είναι κατεστραμμένο ή δεν έχει εγκατασταθεί.

Παράθυρο Αρχεία που επιλέχθηκαν για δημιουργία αντιγράφων ασφαλείας

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

<u>Λίστα τύπων αρχείων</u> 🖓

Περιέχει τα ονόματα των τύπων αρχείων και τον αριθμό των αρχείων κάθε τύπου.

Όταν επιλεγεί ένα στοιχείο λίστας, παρατίθενται όλα τα αρχεία αυτού του τύπου.

<u>Λίστα αρχείων του επιλεγμένου τύπου 💿</u>

Περιέχει πληροφορίες σχετικά με τα αρχεία ενός συγκεκριμένου τύπου που έχουν επιλεγεί για δημιουργία αντιγράφων ασφαλείας: όνομα, θέση και μέγεθος αρχείου.

Εάν το πλαίσιο ελέγχου δίπλα στο όνομα ενός αρχείου είναι επιλεγμένο, το Kaspersky Total Security δημιουργεί αντίγραφο ασφαλείας αυτού του αρχείου.

Εάν το πλαίσιο ελέγχου δίπλα στο όνομα ενός αρχείου είναι αποεπιλεγμένο, το Kaspersky Total Security δεν δημιουργεί αντίγραφο ασφαλείας αυτού του αρχείου.

Ενότητα Μονάδα δίσκου δικτύου

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Δίσκος</u> ?

Διαδρομή προς έναν φάκελο δικτύου που θα χρησιμοποιηθεί ως χώρος αποθήκευσης αντιγράφων ασφαλείας.

<u>Αναζήτηση</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο **Επιλογή φακέλου**. Σε αυτό το παράθυρο μπορείτε να επιλέξετε έναν φάκελο δικτύου που θα χρησιμοποιηθεί ως χώρος αποθήκευσης αντιγράφων ασφαλείας.

<u>Όνομα χρήστη ?</u>

Όνομα του λογαριασμού για την πρόσβαση στον φάκελο δικτύου. Το όνομα χρήστη πρέπει να συμπληρωθεί με τη μορφή *<όνομα υπολογιστή>*|*<όνομα χρήστη>* (για παράδειγμα, *kl-12345*|*ivanov*).

<u>Κωδικός πρόσβασης</u> 🕐

Κωδικός πρόσβασης στον φάκελο δικτύου.

Ενότητα Τοπική μονάδα δίσκου

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Λίστα τοπικών μονάδων δίσκου</u> 🖓

Η λίστα αυτή περιλαμβάνει τις τοπικές μονάδες δίσκου του υπολογιστή. Μπορείτε να επιλέξετε μία από τις τοπικές μονάδες δίσκου ως χώρο αποθήκευσης για τα αντίγραφα ασφαλείας.

Εάν η τοπική μονάδα δίσκου δεν εμφανίζεται στη λίστα, μπορείτε να ορίσετε τη διαδρομή της στο πεδίο που βρίσκεται παρακάτω ή να κάνετε κλικ στο κουμπί **Αναζήτηση** και να επιλέξετε την τοπική μονάδα δίσκου στο παράθυρο **Επιλογή φακέλου για αντίγραφα ασφαλείας** που θα ανοίξει.

<u>Αναζήτηση</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο **Επιλογή φακέλου για αντίγραφα ασφαλείας**. Σε αυτό το παράθυρο μπορείτε να επιλέξετε μια τοπική μονάδα δίσκου που θα χρησιμοποιηθεί ως χώρος αποθήκευσης αντιγράφων ασφαλείας.

Ενότητα Αφαιρούμενη μονάδα δίσκου

Η λίστα αυτή περιλαμβάνει τις αφαιρούμενες μονάδες δίσκου που είναι συνδεδεμένες στον υπολογιστή. Μπορείτε να επιλέξετε μία από τις αφαιρούμενες μονάδες δίσκου ως χώρο αποθήκευσης για τα αντίγραφα ασφαλείας.

Εάν η αφαιρούμενη μονάδα δίσκου δεν εμφανίζεται στη λίστα, μπορείτε να ορίσετε τη διαδρομή της στο πεδίο που βρίσκεται παρακάτω ή να κάνετε κλικ στο κουμπί **Αναζήτηση** και να επιλέξετε την αφαιρούμενη μονάδα δίσκου στο παράθυρο **Επιλογή φακέλου για αντίγραφα ασφαλείας** που θα ανοίξει.

<u>Αναζήτηση</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο **Επιλογή φακέλου για αντίγραφα ασφαλείας**. Σε αυτό το παράθυρο μπορείτε να επιλέξετε μια αφαιρούμενη μονάδα δίσκου που θα χρησιμοποιηθεί ως χώρος αποθήκευσης αντιγράφων ασφαλείας.

Ενότητα Online χώρος αποθήκευσης

Ανάπτυξη όλων | Σύμπτυξη όλων

Για να χρησιμοποιήσετε τον online χώρο αποθήκευσης, συνδεθείτε στον δικτυακό τόπο dropbox.com. Επιλέγοντας **ΟΚ**, ανοίγει αυτόματα μια ιστοσελίδα με τη φόρμα σύνδεσης του δικτυακού τόπου dropbox.com.

Παράθυρο Χώροι αποθήκευσης

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Λίστα χώρων αποθήκευσης</u> ව

Παραθέτει τους χώρους αποθήκευσης αντιγράφων ασφαλείας που έχουν δημιουργηθεί. Οι πληροφορίες που εμφανίζονται για κάθε χώρο αποθήκευσης περιλαμβάνουν τον συνολικό και κατειλημμένο χώρο αποθήκευσης, τη θέση του χώρου αποθήκευσης, τις εργασίες που χρησιμοποιούν τον συγκεκριμένο χώρο και τις διαθέσιμες λειτουργίες.

<u>Επαναφορά αρχείων</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο με μια λίστα των συνόλων αντιγράφων ασφαλείας που έχουν αποθηκευτεί σε αυτόν τον χώρο αποθήκευσης. Σε αυτό το παράθυρο μπορείτε να επιλέξετε ένα σύνολο αντιγράφων ασφαλείας από το οποίο θέλετε να επαναφέρετε αρχεία.

Κάνοντας κλικ στο κουμπί , ανοίγει ένα μενού από το οποίο μπορείτε να επιλέξετε μια πρόσθετη ενέργεια:

- Αλλαγή ρυθμίσεων ξεκινά τον οδηγό επεξεργασίας ρυθμίσεων χώρου αποθήκευσης.
- Διαγραφή χώρου αποθήκευσης σταματά τη χρήση της επιλεγμένης μονάδας δίσκου ή των online πόρων ως χώρο αποθήκευσης των αντιγράφων ασφαλείας και διαγράφει όλα τα αντίγραφα ασφαλείας των αρχείων από τον χώρο αποθήκευσης.
- Εκκαθάριση χώρου αποθήκευσης ανοίγει το παράθυρο Εκκαθάριση χώρου αποθήκευσης. Σε αυτό το παράθυρο μπορείτε να επιλέξετε τα αντίγραφα ασφαλείας των αρχείων που θα καταργηθούν από τον χώρο αποθήκευσης για να απελευθερωθεί χώρος.

<u>Προσθήκη χώρου δικτύου</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Προσθήκη χώρου δικτύου**. Σε αυτό το παράθυρο, μπορείτε να καθορίσετε τις ρυθμίσεις μιας μονάδας δίσκου δικτύου που θέλετε να προσθέσετε στη λίστα των χώρων αποθήκευσης.

<u>Σύνδεση υφιστάμενου χώρου</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Σύνδεση χώρου αποθήκευσης**. Σε αυτό το παράθυρο, μπορείτε να καθορίσετε τις ρυθμίσεις μιας τοπικής μονάδας δίσκου, μιας αφαιρούμενης μονάδας δίσκου, μιας μονάδας δίσκου δικτύου ή ενός online χώρου αποθήκευσης που θέλετε να προσθέσετε στη λίστα των χώρων αποθήκευσης.

Παράθυρο με τη λίστα των συνόλων αντιγράφων ασφαλείας στον χώρο αποθήκευσης Περιέχει πληροφορίες σχετικά με τα σύνολα αντιγράφων ασφαλείας στον χώρο αποθήκευσης:

- Όνομα συνόλου αντιγράφων ασφαλείας
- Χώρος στον δίσκο που απαιτείται για την επαναφορά αρχείων από αυτό το σύνολο

<u>Επαναφορά αρχείων</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει το παράθυρο **Επαναφορά αρχείων από αντίγραφα ασφαλείας**. Αυτό το παράθυρο σας δίνει τη δυνατότητα να επιλέξετε αντίγραφα ασφαλείας από τα οποία θέλετε να επαναφέρετε αρχεία.

Παράθυρο Εκκαθάριση χώρου αποθήκευσης

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Τα αντίγραφα ασφαλείας δημιουργήθηκαν πριν από 🖓</u>

Μια δυνατότητα που καταργεί από τον χώρο αποθήκευσης τα αντίγραφα ασφαλείας των αρχείων που έχουν δημιουργηθεί πριν από την ημερομηνία που καθορίζεται στο πεδίο δίπλα στο πλαίσιο ελέγχου.

<u>Προηγούμενες εκδόσεις αντιγράφων ασφαλείας αρχείου 💿</u>

Εάν είναι επιλεγμένο αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security διαγράφει παλαιές εκδόσεις των αντιγράφων ασφαλείας κατά την εκκαθάριση του χώρου αποθήκευσης. Ο αριθμός των πιο πρόσφατων εκδόσεων των αντιγράφων ασφαλείας που θα διατηρηθούν καθορίζεται στο πεδίο **Αριθμός αντιγράφων ασφαλείας που πρέπει να διατηρηθούν**.

Αντίγραφα ασφαλείας αρχείων των οποίων τα πρωτότυπα διαγράφηκαν ?

Αυτό το πλαίσιο ελέγχου ενεργοποιεί / απενεργοποιεί μια λειτουργία, η οποία καταργεί από τον χώρο αποθήκευσης τα αντίγραφα ασφαλείας αρχείων που έχουν διαγραφεί από τον υπολογιστή.

Παράθυρο Επιλογή έκδοσης αντιγράφου ασφαλείας

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Λίστα εκδόσεων αντιγράφων ασφαλείας 🖻</u>

Περιέχει πληροφορίες σχετικά με τις διαθέσιμες εκδόσεις των αντιγράφων ασφαλείας του αρχείου. Κάθε στοιχείο της λίστας περιέχει το όνομα αρχείου, τον αριθμό έκδοσης και την ημερομηνία δημιουργίας της έκδοσης αντιγράφου ασφαλείας.

Κάνοντας δεξί κλικ σε ένα στοιχείο της λίστας, ανοίγει ένα μενού περιβάλλοντος με τα εξής στοιχεία:

- Άνοιγμα η έκδοση του αντιγράφου ασφαλείας του αρχείου ανοίγει στο παράθυρο της εφαρμογής που αντιστοιχεί στη μορφή του αρχείου.
- Επαναφορά έκδοσης αντιγράφου ασφαλείας ανοίγει το παράθυρο Επιλέξτε πού θέλετε να τοποθετηθούν τα αρχεία μετά την επαναφορά. Σε αυτό το παράθυρο μπορείτε να επιλέξετε έναν φάκελο στον οποίο θα τοποθετηθεί το αρχείο που θα επαναφέρετε.

<u>Επαναφορά</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο στο οποίο μπορείτε να αλλάξετε τις ρυθμίσεις για την επαναφορά των αρχείων.

Παράθυρο Επιλέξτε πού θέλετε να τοποθετηθούν τα αρχεία μετά την επαναφορά τους

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Πεδίο εισαγωγής της διαδρομής στον φάκελο</u> ?

Το πεδίο περιέχει τη διαδρομή προς τον φάκελο στον οποίο πρέπει να εκτελεστεί η επαναφορά των αρχείων. Μπορείτε να επιλέξετε έναν φάκελο από τη δενδροειδή δομή που βρίσκεται πάνω από το πεδίο εισαγωγής ή να εισαγάγετε χειροκίνητα τη διαδρομή προς τον φάκελο.

Παράθυρο Επαναφορά αρχείων

<u>Διακοπή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security σταματά την επαναφορά αρχείων από τα αντίγραφα ασφαλείας.

Παράθυρο "Το αρχείο που επαναφέρετε υπάρχει ήδη"

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Αντικατάσταση αρχείου με αντίγραφο ασφαλείας 🖻</u>

Το Kaspersky Total Security διαγράφει το υπάρχον αρχείο και το αντικαθιστά με το αρχείο που επαναφέρετε από το αντίγραφο ασφαλείας.

<u>Να μην γίνει επαναφορά αυτού του αρχείου 🖻</u>

To Kaspersky Total Security αφήνει το υπάρχον αρχείο αμετάβλητο και δεν εκτελεί επαναφορά του αρχείου με το ίδιο όνομα από το αντίγραφο ασφαλείας.

<u>Αποθήκευση και των δύο αρχείων 🖓</u>

To Kaspersky Total Security αφήνει το υπάρχον αρχείο αμετάβλητο και αποθηκεύει το αρχείο που επαναφέρετε από το αντίγραφο ασφαλείας με νέο όνομα στον ίδιο φάκελο.

<u>Εφαρμογή αυτής της ενέργειας σε όλες τις παρόμοιες περιπτώσεις 🖻</u>

Εάν επιλεγεί αυτό το πλαίσιο ελέγχου, το Kaspersky Total Security θα εφαρμόζει την επιλεγμένη ενέργεια σε όλα τα αρχεία που επαναφέρει.

Παράθυρο Επαναφορά αρχείων

Ανάπτυξη όλων | Σύμπτυξη όλων

<u>Διακοπή</u> 🕐

Κάνοντας κλικ σε αυτό το κουμπί, το Kaspersky Total Security σταματά την επαναφορά αρχείων από τα αντίγραφα ασφαλείας.

Παράθυρο Ρυθμίσεις χώρου αποθήκευσης

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

<u>Όνομα χώρου αποθήκευσης</u> 💿

Το πεδίο περιέχει το όνομα ενός χώρου αποθήκευσης αντιγράφων ασφαλείας.

Παράθυρο Kaspersky Restore Utility

<u>Ανάπτυξη όλων</u> | <u>Σύμπτυξη όλων</u>

Εργασία δημιουργίας αντιγράφου ασφαλείας 🖻

Από αυτήν την αναπτυσσόμενη λίστα μπορείτε να επιλέξετε τα δεδομένα προς επαναφορά.

<u>Ημερομηνία/ώρα δημιουργίας αντιγράφων ασφαλείας </u>

Αυτή η αναπτυσσόμενη λίστα σας δίνει τη δυνατότητα να επιλέξετε την ημερομηνία και ώρα που δημιουργήθηκαν τα αντίγραφα ασφαλείας των αρχείων που θέλετε να επαναφέρετε. Η επαναφορά των επιλεγμένων αρχείων θα πραγματοποιηθεί στην κατάσταση στην οποία βρίσκονταν εκείνη την ημερομηνία και ώρα.

<u>Αναζήτηση</u> 🕐

Πεδίο για την αναζήτηση του αντιγράφου ασφαλείας ενός αρχείου χρησιμοποιώντας το όνομα του αρχείου. Η αναζήτηση πραγματοποιείται όσο πληκτρολογείτε τους χαρακτήρες.



Αυτός ο διακόπτης εναλλαγής αλλάζει την προβολή της λίστας των αντιγράφων ασφαλείας των αρχείων: δέντρο φακέλων ή λίστα αρχείων με αλφαβητική ταξινόμηση.

<u>Λίστα αρχείων</u> ?

Η λίστα περιλαμβάνει τα αντίγραφα ασφαλείας των αρχείων που μπορείτε να επαναφέρετε.

Ανάλογα με τη θέση του διακόπτη εναλλαγής 🔚 📃 / 🔚 🚍 , το παράθυρο εμφανίζει ένα δέντρο φακέλων ή όλα τα αντίγραφα ασφαλείας των αρχείων με αλφαβητική ταξινόμηση.

Η λίστα αυτή εμφανίζει πληροφορίες σχετικά με το όνομα του αντιγράφου ασφαλείας ενός αρχείου, τη θέση του αρχείου προέλευσης, τον τύπο, την επέκταση ονόματος, το μέγεθος και τον αριθμό των αντιγράφων ασφαλείας του αρχείου. Κάνοντας κλικ στη στήλη **Έκδοση**, ανοίγει το παράθυρο **Επιλογή έκδοσης αντιγράφου ασφαλείας**. Αυτό το παράθυρο σας επιτρέπει να επιλέξετε την έκδοση του αντιγράφου ασφαλείας από το οποίο θα επαναφέρετε το αρχείο.

Εάν επιλεγεί το πλαίσιο ελέγχου απέναντι από το όνομα ενός αντιγράφου ασφαλείας, το Kaspersky Total Security επαναφέρει αυτό το αρχείο.

Εάν δεν επιλεγεί το πλαίσιο ελέγχου απέναντι από το όνομα ενός αντιγράφου ασφαλείας, το Kaspersky Total Security δεν επαναφέρει αυτό το αρχείο.

Κάνοντας δεξί κλικ σε ένα στοιχείο της λίστας, ανοίγει ένα μενού περιβάλλοντος με τα εξής στοιχεία:

- Άνοιγμα αρχείου το αρχείο ανοίγει με την εφαρμογή που προορίζεται για τη διαχείριση των αρχείων αυτού του τύπου.
- Επαναφορά στην τελευταία έκδοση αντιγράφου ασφαλείας ανοίγει το παράθυρο Επιλέξτε πού θέλετε να τοποθετηθούν τα αρχεία μετά την επαναφορά στο οποίο μπορείτε να ορίσετε τον φάκελο προορισμού για την επαναφορά του αρχείου από την τελευταία έκδοση αντιγράφου ασφαλείας.
- Εκδόσεις αντιγράφων ασφαλείας αρχείου ανοίγει το παράθυρο Επιλογή έκδοσης αντιγράφου ασφαλείας. Αυτό το παράθυρο σας επιτρέπει να επιλέξετε την έκδοση του αντιγράφου ασφαλείας από το οποίο θα επαναφέρετε το αρχείο.

<u>Έκδοση</u> ?

Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο **Επιλογή έκδοσης αντιγράφου ασφαλείας** στο οποίο μπορείτε να δείτε όλες τις εκδόσεις του επιλεγμένου αρχείου που μπορούν να ανακτηθούν. Κάνοντας κλικ σε αυτή τη σύνδεση, ανοίγει το παράθυρο επιλογής του χώρου αποθήκευσης αντιγράφων ασφαλείας.

<u>Επαναφορά επιλεγμένων δεδομένων</u> ?

Κάνοντας κλικ σε αυτό το κουμπί, ανοίγει ένα παράθυρο στο οποίο μπορείτε να αλλάξετε τις ρυθμίσεις για την επαναφορά των αρχείων.

Χρήση Γονικού ελέγχου

Ο *Γονικός έλεγχος* επιτρέπει την παρακολούθηση των ενεργειών που εκτελούνται από χρήστες στον τοπικό υπολογιστή και το διαδίκτυο. Μπορείτε να χρησιμοποιήσετε τον Γονικό Έλεγχο για να εφαρμόσετε περιορισμούς στην πρόσβαση σε πόρους του διαδικτύου και εφαρμογές, καθώς και για να δείτε αναφορές ως προς τις δραστηριότητες των χρηστών.

Στις μέρες μας, ολοένα περισσότερα παιδιά και έφηβοι έχουν πρόσβαση σε υπολογιστές και πόρους στο Web. Η χρήση των υπολογιστών και του Διαδικτύου συνοδεύεται από μια σειρά κινδύνων και απειλών για τα παιδιά:

- Η απώλεια χρόνου ή/και χρημάτων κατά τις επισκέψεις σε κανάλια συνομιλίας, πόρους παιχνιδιών, ηλεκτρονικά καταστήματα και δημοπρασίες
- Πρόσβαση σε δικτυακούς τόπους που απευθύνονται σε ενηλίκους, όπως δικτυακοί τόποι με πορνογραφία, εξτρεμιστικές απόψεις, όπλα, ναρκωτικά και βία
- Λήψη αρχείων που έχουν μολυνθεί με κακόβουλο λογισμικό
- Βλάβες στην υγεία που προκαλείται από την υπερβολική χρήση του υπολογιστή
- Επαφές με άγνωστα άτομα, τα οποία παριστάνουν τους συνομήλικους με σκοπό να αποκτήσουν πρόσβαση σε προσωπικά στοιχεία ανήλικων χρηστών, όπως πραγματικό όνομα, φυσική διεύθυνση, ώρες της ημέρας κατά τις οποίες δεν βρίσκεται κανείς στο σπίτι

Ο Γονικός έλεγχος σας επιτρέπει να μειώσετε τους κινδύνους που δημιουργούνται από την χρήση του υπολογιστή και του Διαδικτύου. Για να γίνει αυτό, χρησιμοποιούνται οι παρακάτω λειτουργίες:

• Περιορισμός του χρόνου χρήσης του υπολογιστή και του Διαδικτύου

- Δημιουργία καταλόγων επιτρεπόμενων και αποκλεισμένων παιχνιδιών και εφαρμογών, καθώς και προσωρινός περιορισμό της χρήσης των επιτρεπόμενων εφαρμογών
- Δημιουργία καταλόγων των επιτρεπόμενων και αποκλεισμένων δικτυακών τόπων και επιλεκτική φραγή κατηγοριών δικτυακών τόπων με ακατάλληλο περιεχόμενο
- Ενεργοποίηση της λειτουργίας ασφαλούς αναζήτησης μέσω μηχανών αναζήτησης (οι σύνδεσμοι προς δικτυακούς τόπους με ύποπτο περιεχόμενο δεν εμφανίζονται στα αποτελέσματα των αναζητήσεων)
- Περιορισμός της λήψης αρχείων από το Διαδίκτυο
- Αποκλεισμός της αποστολής συγκεκριμένων προσωπικών δεδομένων

Μπορείτε να ρυθμίσετε τα χαρακτηριστικά του γονικού ελέγχου για κάθε λογαριασμό χρήστη σε έναν υπολογιστή ξεχωριστά. Εάν ένας χρήστης χρησιμοποιεί δύο λογαριασμούς, π.χ., έναν τοπικό λογαριασμό του λειτουργικού συστήματος και έναν λογαριασμό χρήστη Microsoft, θα πρέπει να προσαρμοστούν οι ρυθμίσεις Γονικού ελέγχου για το λογαριασμό χρήστη Microsoft.

Μπορείτε επίσης να δείτε αναφορές του Γονικού ελέγχου σχετικά με τις δραστηριότητες της παρακολούθησης των χρηστών.

Όταν αλλάζει η ζώνη ώρας ή στην αλλαγή μεταξύ χειμερινής και θερινής ώρας, ισχύουν οι ακόλουθοι κανόνες για τη χρήση του υπολογιστή και του Διαδικτύου, καθώς και για την εκκίνηση παιχνιδιών και εφαρμογών:

- Εάν δεν αλλάξει η ημερομηνία με την αλλαγή ζώνης ώρας, η τρέχουσα αντίστροφη μέτρηση μέχρι τον αποκλεισμό συνεχίζεται χωρίς αλλαγές. Ο ίδιος κανόνας ισχύει κατά την αλλαγή μεταξύ χειμερινής και θερινής ώρας.
- Εάν η ημερομηνία αλλάζει προς τα πάνω ή κάτω με την αλλαγή της ζώνης ώρας, μηδενίζεται ο χρόνος που δαπάνησε ο χρήστης και ξεκινά πάλι η αντίστροφη μέτρηση μέχρι τον αποκλεισμό.

Μετάβαση στις ρυθμίσεις Γονικού ελέγχου

Για να μεταβείτε στις ρυθμίσεις Γονικού ελέγχου:

- 1. Ανοίξτε το κύριο παράθυρο της εφαρμογής.
- 2. Στο κύριο παράθυρο της εφαρμογής, κάντε κλικ στο κουμπί **Γονικός έλεγχος**.

- 3. Εάν η πρόσβαση στις ρυθμίσεις του Γονικού Ελέγχου δεν προστατεύεται με κωδικό πρόσβασης, η εφαρμογή προτρέπει τον χρήστη να ορίσει κωδικό πρόσβασης. Επιλέξτε ένα από τα παρακάτω:
 - Για να προστατεύσετε την πρόσβαση στις ρυθμίσεις του Γονικού Ελέγχου με κωδικό πρόσβασης:
 - a. Συμπληρώστε τα πεδία **Κωδικός πρόσβασης** και **Επιβεβαίωση κωδικού πρόσβασης** και κάντε κλικ στη **Συνέχεια**.
 - b. Στο παράθυρο **Ισχύς κωδικού πρόσβασης**, κάντε κλικ στο κουμπί **Δημιουργία κωδικού**.
 - c. Στο παράθυρο **Εισαγωγή κωδικού πρόσβασης**, επιβεβαιώστε τον κωδικό πρόσβασης και κάντε κλικ στο κουμπί **Σύνδεση**.
 - Εάν δεν θέλετε να προστατεύσετε με κωδικό την πρόσβαση στις ρυθμίσεις Γονικού ελέγχου, κάντε κλικ στη σύνδεση Παράλειψη για να συνεχίσετε στις ρυθμίσεις Γονικού ελέγχου.

Ανοίγει το παράθυρο **Γονικός έλεγχος**.

4. Επιλέξτε έναν λογαριασμό χρήστη και κάντε κλικ στη σύνδεση **Ρύθμιση παραμέτρων περιορισμών** για να ανοίξετε το παράθυρο ρυθμίσεων Γονικού ελέγχου.

Έλεγχος της χρήσης του υπολογιστή

Ο Γονικός έλεγχος σας επιτρέπει να περιορίσετε το χρόνο που δαπανάται από τον χρήστη στον υπολογιστή. Μπορείτε να καθορίσετε ένα χρονικό διάστημα κατά το οποίο ο Γονικός έλεγχος δεν θα επιτρέπει την πρόσβαση στον υπολογιστή (ώρα ύπνου), καθώς και ένα ημερήσιο χρονικό όριο για τη συνολική χρήση του υπολογιστή. Μπορείτε να καθορίσετε διαφορετικές τιμές για τις καθημερινές και τα Σαββατοκύριακα.

Για να ρυθμίσετε τα χρονικά όρια χρήσης υπολογιστή:

- 1. Μετάβαση στο <u>παράθυρο ρυθμίσεων Γονικού ελέγχου</u>.
- 2. Στο παράθυρο ρυθμίσεων Γονικού ελέγχου, επιλέξτε την ενότητα **Υπολογιστής**.
- 3. Για να καθορίσετε ένα χρονικό διάστημα κατά το οποίο ο Γονικός έλεγχος δεν θα επιτρέπει την πρόσβαση στον υπολογιστή, στις ενότητες Εργάσιμες και Σαββατοκύριακα επιλέξτε το πλαίσιο ελέγχου Αποκλεισμός πρόσβασης από.

- 4. Στην αναπτυσσόμενη λίστα δίπλα στο πλαίσιο ελέγχου **Αποκλεισμός πρόσβασης από**, προσδιορίστε την ώρα έναρξης της φραγής.
- 5. Στην αναπτυσσόμενη λίστα **έως**, προσδιορίστε την ώρα λήξης της φραγής.

Ο Γονικός έλεγχος θα αποκλείσει την πρόσβαση του χρήστη στον υπολογιστή για το καθορισμένο χρονικό διάστημα.

6. Μπορείτε επίσης να δημιουργήσετε ένα χρονοδιάγραμμα χρήσης του υπολογιστή χρησιμοποιώντας έναν πίνακα. Για να εμφανίσετε τον πίνακα, κάντε κλικ στο κουμπί



Ο Γονικός έλεγχος θα αποκλείσει την πρόσβαση του χρήστη στον υπολογιστή **βάσει προγράμματος** που καθορίζεται στον πίνακα.

7. Για να ορίσετε ένα χρονικό όριο για τη συνολική χρήση του υπολογιστή κατά τη διάρκεια της ημέρας, στις ενότητες Εργάσιμες και Σαββατοκύριακα επιλέξτε τα πλαίσια ελέγχου Να επιτρέπεται η πρόσβαση το πολύ και, από την αναπτυσσόμενη λίστα δίπλα στο πλαίσιο ελέγχου, επιλέξτε ένα χρονικό διάστημα.

Ο Γονικός έλεγχος δεν θα επιτρέπει την πρόσβαση του χρήστη στον υπολογιστή όταν η συνολική χρήση του υπολογιστή κατά τη διάρκεια της ημέρας υπερβαίνει το καθορισμένο χρονικό διάστημα.

- 8. Για να ρυθμίσετε διαλείμματα στη χρήση του υπολογιστή, στην ενότητα Διαλείμματα, επιλέξτε το πλαίσιο ελέγχου Διάλειμμα και, στη συνέχεια, επιλέξτε τιμές για τη συχνότητα των διαλειμμάτων από τις αναπτυσσόμενες λίστες δίπλα από το πλαίσιο ελέγχου (κάθε ώρα, για παράδειγμα) και τη διάρκειά τους (10 λεπτά, π.χ.).
- 9. Ρυθμίστε τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου στο **Ο έλεγχος είναι** ενεργοποιημένος.

Ο Γονικός έλεγχος θα εμποδίσει την πρόσβαση του χρήστη στον υπολογιστή, σύμφωνα με τις καθορισμένες ρυθμίσεις.

Έλεγχος της χρήσης του Διαδικτύου

Με τη χρήση του Γονικού ελέγχου, μπορείτε να περιορίσετε το χρόνο χρήσης του Διαδικτύου και να απαγορεύσετε στους χρήστες να έχουν πρόσβαση σε ορισμένες κατηγορίες δικτυακών τόπων ή συγκεκριμένες ιστοσελίδες. Επιπλέον, μπορείτε να απαγορεύσετε στο χρήστη να κατεβάσει αρχεία συγκεκριμένων τύπων (όπως συμπιεσμένα αρχεία ή βίντεο) από το Διαδίκτυο. Για να περιορίσετε τον χρόνο χρήσης του Διαδικτύου:

- 1. Μετάβαση στο παράθυρο ρυθμίσεων Γονικού ελέγχου.
- 2. Στο παράθυρο ρυθμίσεων Γονικού ελέγχου, επιλέξτε την ενότητα **Διαδίκτυο**.
- 3. Αν θέλετε να περιορίσετε το συνολικό χρόνο χρήσης του Διαδικτύου τις καθημερινές, στην ενότητα Περιορισμός πρόσβασης στο Διαδίκτυο, επιλέξτε το πλαίσιο ελέγχου Περιορισμός πρόσβασης τις καθημερινές σε και, στη συνέχεια, επιλέξτε μια τιμή για το χρονικό όριο από την αναπτυσσόμενη λίστα δίπλα στο πλαίσιο ελέγχου.
- 4. Αν θέλετε να περιορίσετε το συνολικό χρόνο χρήσης του Διαδικτύου τα Σαββατοκύριακα, επιλέξτε το πλαίσιο ελέγχου Περιορισμός πρόσβασης τα σαββατοκύριακα σε και, στη συνέχεια, επιλέξτε μια τιμή για το χρονικό όριο από την αναπτυσσόμενη λίστα δίπλα στο πλαίσιο ελέγχου.
- 5. Ρυθμίστε τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου στο **Ο έλεγχος** είναι ενεργοποιημένος.

Ο Γονικός έλεγχος θα περιορίσει το συνολικό χρόνο που δαπανάται στο διαδίκτυο από το χρήστη, σύμφωνα με τις τιμές που καθορίσατε.

<u>Πώς να περιορίσετε την επίσκεψη σε συγκεκριμένους δικτυακούς τόπους</u> 🕑

Για να περιορίσετε την επίσκεψη σε συγκεκριμένους δικτυακούς τόπους:

- 1. Μετάβαση στο παράθυρο ρυθμίσεων Γονικού ελέγχου.
- 2. Στο παράθυρο ρυθμίσεων Γονικού ελέγχου, επιλέξτε την ενότητα **Διαδίκτυο**.
- Για να αποτρέψετε την εμφάνιση περιεχομένου για ενήλικες στα αποτελέσματα αναζήτησης, στην ενότητα Έλεγχος περιήγησης στο Web, ενεργοποιήστε το πλαίσιο ελέγχου Ενεργοποίηση ασφαλούς αναζήτησης.

Όταν αναζητείτε πληροφορίες σε δικτυακούς τόπους όπως Google, YouTube (μόνο για τους χρήστες που δεν έχουν συνδεθεί στο youtube.com με τον λογαριασμό τους) Bing, Yahoo!, Mail.ru, VKontakte και Yandex, δεν θα εμφανίζεται περιεχόμενο για ενήλικες στα αποτελέσματα της αναζήτησης.

4. Για να αποκλείσετε την πρόσβαση σε δικτυακούς τόπους ορισμένων κατηγοριών:

- a. Στην ενότητα Έλεγχος περιήγησης στο web, επιλέξτε το πλαίσιο ελέγχου Έλεγχος πρόσβασης σε τοποθεσίες web.
- b. Επιλέξτε το στοιχείο Αποκλεισμός πρόσβασης σε τοποθεσίες web επιλεγμένων κατηγοριών και κάντε κλικ στη σύνδεση Επιλογή κατηγοριών τοποθεσιών web για να ανοίξετε το παράθυρο Αποκλεισμός πρόσβασης σε κατηγορίες τοποθεσιών web.
- c. Επιλέξτε τα πλαίσια ελέγχου δίπλα στις κατηγορίες των δικτυακών τόπων που θέλετε να αποκλείσετε.

Ο Γονικός έλεγχος θα αποκλείσει όλες τις προσπάθειες του χρήστη να ανοίξει έναν δικτυακό τόπο, εάν το περιεχόμενό του κατατάσσεται σε οποιαδήποτε από τις απαγορευμένες κατηγορίες.

- 5. Για να αποκλείσετε την πρόσβαση σε συγκεκριμένους δικτυακούς τόπους:
 - a. Στην ενότητα **Έλεγχος περιήγησης στο web**, επιλέξτε το πλαίσιο ελέγχου **Έλεγχος πρόσβασης σε τοποθεσίες web**.
 - b. Κάντε κλικ στη σύνδεση **Διαχείριση εξαιρέσεων** για να ανοίξετε το παράθυρο **Εξαιρέσεις**.
 - c. Στο κάτω μέρος του παραθύρου, κάντε κλικ στο κουμπί **Προσθήκη**.

Ανοίγει ένα παράθυρο για την προσθήκη νέας μάσκας διεύθυνσης web.

- d. Στο πεδίο **Μάσκα διεύθυνσης web**, εισαγάγετε τη διεύθυνση ενός δικτυακού τόπου στον οποίο δεν θέλετε να επιτρέπεται η πρόσβαση.
- e. Στην ενότητα **Πεδίο**, ορίστε την έκταση του περιεχομένου που θέλετε να αποκλειστεί: ολόκληρος ο δικτυακός τόπος ή μια συγκεκριμένη σελίδα.
- f. Εάν θέλετε να αποκλείσετε το συγκεκριμένο δικτυακό τόπο, στην ενότητα **Ενέργεια**, επιλέξτε **Αποκλεισμός**.
- g. Κάντε κλικ στο κουμπί **Προσθήκη**.

Ο καθορισμένος δικτυακός τόπος εμφανίζεται στη λίστα στο παράθυρο **Εξαιρέσεις**. Κλείστε το παράθυρο **Εξαιρέσεις**.

6. Ρυθμίστε τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου στο **Ο έλεγχος** είναι ενεργοποιημένος Ο Γονικός έλεγχος θα αποκλείσει τις προσπάθειες ανοίγματος τοποθεσιών web, σύμφωνα με τις καθορισμένες ρυθμίσεις.

Πώς να αποκλείσετε τη λήψη συγκεκριμένων τύπων αρχείων 🖓

Για να απαγορεύσετε τη λήψη συγκεκριμένων τύπων αρχείων από το Διαδίκτυο:

- 1. Μετάβαση στο παράθυρο ρυθμίσεων Γονικού ελέγχου.
- 2. Στο παράθυρο ρυθμίσεων Γονικού ελέγχου, επιλέξτε την ενότητα **Διαδίκτυο**.
- Στην ενότητα Αποκλεισμός λήψης αρχείων, επιλέξτε τα πλαίσια ελέγχου δίπλα στους τύπους αρχείων που δεν θέλετε να επιτρέπεται η λήψη τους.
- 4. Ρυθμίστε τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου στο **Ο έλεγχος** είναι ενεργοποιημένος.

Ο Γονικός έλεγχος θα αποκλείσει τις λήψεις αρχείων του συγκεκριμένου τύπου από το Διαδίκτυο.

Έλεγχος εκκίνησης παιχνιδιών και εφαρμογών

Χρησιμοποιώντας το γονικό έλεγχο, μπορείτε να επιτρέπετε ή να εμποδίζετε το χρήστη να εκκινεί παιχνίδια ανάλογα με την ηλικιακή ομάδα του. Μπορείτε επίσης να μην επιτρέψετε στο χρήστη να εκτελεί συγκεκριμένες εφαρμογές (όπως παιχνίδια ή προγράμματα-πελάτη ΙΜ) ή να περιορίσετε το χρονικό διάστημα κατά το οποίο θα επιτρέπεται η χρήση εφαρμογών.

<u>Πώς να αποκλείσετε τη χρήση παιχνιδιών με περιεχόμενο που δεν είναι κατάλληλο για</u> <u>όλες τις ηλικίες</u> 🛛

Για να αποκλείσετε τη χρήση παιχνιδιών με περιεχόμενο που δεν είναι κατάλληλο για όλες τις ηλικίες:

- 1. Μετάβαση στο <u>παράθυρο ρυθμίσεων Γονικού ελέγχου</u>.
- 2. Στο παράθυρο ρυθμίσεων Γονικού ελέγχου, επιλέξτε την ενότητα **Εφαρμογές**.
- 3. Αν θέλετε να αποκλείσετε όλα τα παιχνίδια με ακατάλληλο περιεχόμενο για την ηλικία του χρήστη, επιλέξτε το πλαίσιο ελέγχου **Περιορισμός της έναρξης**

παιχνιδιών για ηλικίες μικρότερες από και επιλέξτε μια επιλογή περιορισμού ηλικίας από την αναπτυσσόμενη λίστα, δίπλα στο πλαίσιο ελέγχου.

- Αν θέλετε να αποκλείσετε παιχνίδια με περιεχόμενο μιας συγκεκριμένης κατηγορίας:
 - a. Ενεργοποιήστε το πλαίσιο ελέγχου **Αποκλεισμός παιχνιδιών από κατηγορίες** ενηλίκων.
 - b. Κάντε κλικ στη σύνδεση **Επιλογή κατηγοριών παιχνιδιών** για να ανοίξετε το παράθυρο **Αποκλεισμός παιχνιδιών κατά κατηγορίες**.
 - c. Ενεργοποιήστε τα πλαίσια ελέγχου δίπλα από τις κατηγορίες περιεχομένου που αντιστοιχεί σε παιχνίδια που θέλετε να αποκλείσετε.
- 5. Επιστρέψτε στην ενότητα **Εφαρμογές**.
- 6. Εάν θέλετε να χρησιμοποιήσετε το σύστημα αξιολόγησης για τον αποκλεισμό παιχνιδιών, επιλέξτε τον τύπο αξιολογήσεων και κατηγοριοποίησης του περιεχομένου παιχνιδιών στην αναπτυσσόμενη λίστα Χρήση αυτού του συστήματος αξιολόγησης για τον αποκλεισμό παιχνιδιών:
 - Αυτόματος εντοπισμός ο Γονικός Έλεγχος επιλέγει τον τύπο αξιολόγησης παιχνιδιών ανάλογα με την τοποθεσία σας: το σύστημα αξιολόγησης PEGI (Πανευρωπαϊκό Σύστημα Πληροφόρησης για τα Παιχνίδια) ή το σύστημα ESRB (για τις ΗΠΑ και τον Καναδά).
 - PEGI Ο Γονικός Έλεγχος χρησιμοποιεί το Ευρωπαϊκό σύστημα αξιολόγησης κατά τη διαμόρφωση των δικαιωμάτων εκκίνησης παιχνιδιών.
 - ESRB Ο Γονικός Έλεγχος χρησιμοποιεί αυτό το σύστημα αξιολόγησης για τις ΗΠΑ και τον Καναδά κατά τη διαμόρφωση των δικαιωμάτων εκκίνησης παιχνιδιών.
- 7. Ρυθμίστε τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου στο **Ο έλεγχος** είναι ενεργοποιημένος

<u>Πώς να περιορίσετε την εκκίνηση μιας συγκεκριμένης εφαρμογής 🖻</u>

Για να περιορίσετε την εκκίνηση μιας συγκεκριμένης εφαρμογής:

1. Μετάβαση στο <u>παράθυρο ρυθμίσεων Γονικού ελέγχου</u>.

- 2. Στο παράθυρο ρυθμίσεων Γονικού ελέγχου, επιλέξτε την ενότητα **Εφαρμογές**.
- 3. Κάντε κλικ στη σύνδεση **Ρύθμιση παραμέτρων** για να ανοίξετε το παράθυρο **Χρήση εφαρμογής**.
- Κάντε κλικ στο κουμπί Προσθήκη για να ανοίξετε το παράθυρο Αναζήτηση και επιλέξτε το εκτελέσιμο αρχείο της εφαρμογής.

Η επιλεγμένη εφαρμογή εμφανίζεται στη λίστα **Χρήση εφαρμογής**. Το Kaspersky Total Security προσθέτει αυτόματα την εφαρμογή σε μια συγκεκριμένη κατηγορία, όπως για παράδειγμα, *Παιχνίδια*.

- 5. Πραγματοποιήστε τις ακόλουθες ενέργειες:
 - Για να αποκλείσετε την έναρξη της εφαρμογής, επιλέξτε το στοιχείο
 Αποκλεισμός στην αναπτυσσόμενη λίστα δίπλα στο όνομα της εφαρμογής.
 - Για να αποκλείσετε όλες τις εφαρμογές που ανήκουν σε συγκεκριμένη κατηγορία, επιλέξτε το πλαίσιο ελέγχου δίπλα από το όνομα της συγκεκριμένης κατηγορίας στη λίστα (για παράδειγμα, μπορείτε να αποκλείσετε εφαρμογές της κατηγορίας Παιχνίδια).
 - Για να επιτρέψετε την έναρξη της εφαρμογής, επιλέξτε το στοιχείο Να επιτρέπεται στην αναπτυσσόμενη λίστα δίπλα στο όνομα της εφαρμογής.
 - Για να ορίσετε περιορισμούς για τη διάρκεια χρήσης των εφαρμογών, επιλέξτε το στοιχείο Περιορισμός στην αναπτυσσόμενη λίστα δίπλα στο όνομα της εφαρμογής.

Ανοίγει το παράθυρο Περιορισμός χρήσης εφαρμογής.

Πραγματοποιήστε τις ακόλουθες ενέργειες:

- a. Εάν θέλετε να ορίσετε χρονικό όριο στη χρήση μιας εφαρμογής τις καθημερινές και τα σαββατοκύριακα, από τις ενότητες Εργάσιμες και Σαββατοκύριακα, επιλέξτε το πλαίσιο ελέγχου Να επιτρέπεται η πρόσβαση το πολύ και καθορίστε στην αναπτυσσόμενη λίστα τον αριθμό των ωρών που επιτρέπεται ο χρήστης να χρησιμοποιεί την εφαρμογή κάθε μέρα. Μπορείτε επίσης να καθορίσετε τον χρόνο κατά τον οποίο ο χρήστης επιτρέπεται / απαγορεύεται να χρησιμοποιήσει την εφαρμογή, με τη χρήση του πίνακα Ακριβής χρόνος χρήσης.
- b. Εάν θέλετε να ορίσετε παύσεις στη χρήση μιας εφαρμογής, στην ενότητα Διαλείμματα, επιλέξτε το πλαίσιο ελέγχου Διάλειμμα και επιλέξτε τις τιμές για τη συχνότητα και τη διάρκεια του διαλείμματος από την αναπτυσσόμενη λίστα.

c. Κάντε κλικ στο κουμπί **Αποθήκευση**.

- 6. Κλείστε το παράθυρο **Χρήση εφαρμογής**.
- 7. Ρυθμίστε τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου στο Ο έλεγχος
 είναι ενεργοποιημένος

Ο Γονικός έλεγχος θα εφαρμόσει τους συγκεκριμένους περιορισμούς όταν ο χρήστης χρησιμοποιεί την εφαρμογή.

Παρακολούθηση περιεχομένου μηνυμάτων

Με τη χρήση του Γονικού Ελέγχου, μπορείτε να παρακολουθείτε και να εμποδίζετε τις προσπάθειες του χρήστη να καταχωρήσει συγκεκριμένα προσωπικά δεδομένα (όπως ονόματα, αριθμούς τηλεφώνου, αριθμούς τραπεζικών καρτών) σε μηνύματα.

Πώς να ρυθμίσετε τον έλεγχο της μεταφοράς προσωπικών δεδομένων 🕑

Για να ρυθμίσετε τον έλεγχο της μεταφοράς προσωπικών δεδομένων:

- 1. Μετάβαση στο <u>παράθυρο ρυθμίσεων Γονικού ελέγχου</u>.
- 2. Στο παράθυρο ρυθμίσεων Γονικού ελέγχου, επιλέξτε την ενότητα **Έλεγχος περιεχομένου**.
- Στην ενότητα Έλεγχος μεταφοράς προσωπικών δεδομένων, ενεργοποιήστε το πλαίσιο ελέγχου Να αποκλειστεί η μεταφορά προσωπικών δεδομένων σε τρίτους.
- 4. Κάντε κλικ στη σύνδεση **Επεξεργασία λίστας προσωπικών δεδομένων** για να ανοίξετε το παράθυρο **Λίστα προσωπικών δεδομένων**.
- 5. Στο κάτω μέρος του παραθύρου, κάντε κλικ στο κουμπί **Προσθήκη**. Ανοίγει ένα παράθυρο για την προσθήκη προσωπικών δεδομένων.
- 6. Επιλέξτε έναν τύπο προσωπικών δεδομένων (για παράδειγμα, "αριθμός τηλεφώνου") κάνοντας κλικ στον αντίστοιχο σύνδεσμο ή καταχωρίστε μια περιγραφή στο πεδίο Όνομα πεδίου.
- Καθορίστε τα προσωπικά σας δεδομένα (όπως το επώνυμο ή τον αριθμό τηλεφώνου σας) στο πεδίο Τιμή.

8. Κάντε κλικ στο κουμπί **Προσθήκη**.

Τα προσωπικά δεδομένα θα καταχωρηθούν στο παράθυρο **Λίστα προσωπικών δεδομένων**.

- 9. Κλείστε το παράθυρο **Λίστα προσωπικών δεδομένων**.
- 10. Ρυθμίστε τον διακόπτη εναλλαγής στο επάνω μέρος του παραθύρου στο **Ο έλεγχος** είναι ενεργοποιημένος.

Ο Γονικός έλεγχος ελέγχει και αποκλείει τις απόπειρες του χρήστη να χρησιμοποιήσει τα καθορισμένα προσωπικά δεδομένα κατά την ανταλλαγή μηνυμάτων μέσω του Διαδικτύου.

Η λειτουργία ελέγχου μεταφοράς προσωπικών δεδομένων δεν λειτουργεί στο Facebook.

Προβολή της αναφοράς σχετικά με τη δραστηριότητα ενός χρήστη

Μπορείτε να έχετε πρόσβαση σε αναφορές σχετικά με τη δραστηριότητα κάθε λογαριασμού χρήστη που υπόκειται στον Γονικό Έλεγχο, με ξεχωριστές αναφορές για κάθε κατηγορία των υπό έλεγχο συμβάντων.

Για να δείτε μια αναφορά σχετικά με τη δραστηριότητα ενός ελεγχόμενου λογαριασμού χρήστη:

- 1. Μετάβαση στο <u>παράθυρο ρυθμίσεων Γονικού ελέγχου</u>.
- Επιλέξτε έναν λογαριασμό χρήστη και κάντε κλικ στη σύνδεση Προβολή αναφοράς για να μεταβείτε στο παράθυρο των αναφορών.
- Στην ενότητα με τον αντίστοιχο τύπο περιορισμού (για παράδειγμα, Διαδίκτυο), ανοίξτε την αναφορά παρακολουθούμενων ενεργειών κάνοντας κλικ στη σύνδεση Λεπτομέρειες.

Το παράθυρο εμφανίζει μια αναφορά για τις παρακολουθούμενες ενέργειες του χρήστη.