Anti-Virus 2015

Περιεχόμενα

Εγκατάσταση

Θέματα:

1.1 Πριν από την πρώτη εγκατάσταση

Σας ευχαριστούμε που επιλέξατε το προϊόν μας.

Για να εγκαταστήσετε το προϊόν, χρειάζεστε τα ακόλουθα:

- Το CD εγκατάστασης ή πακέτο εγκατάστασης.
- Το κλειδί συνδρομής σας.
- Μια σύνδεση στο Internet.

Εάν διαθέτετε προϊόν ασφαλείας από άλλον προμηθευτή, το πρόγραμμα εγκατάστασης θα επιχειρήσει να το καταργήσει αυτόματα. Εάν δεν συμβεί αυτό, καταργήστε το μη αυτόματα.

Σημείωση: Εάν έχετε περισσότερους από έναν λογαριασμούς στον υπολογιστή, κατά την εγκατάσταση συνδεθείτε με δικαιώματα διαχειριστή.

1.2 Εγκατάσταση του προϊόντος για πρώτη φορά

Οδηγίες εγκατάστασης του προϊόντος.

Για να εγκαταστήσετε το προϊόν, ακολουθήστε τις εξής οδηγίες:

1. Τοποθετήστε το CD ή κάντε διπλό κλικ στο πρόγραμμα εγκατάστασης που λάβατε.

   Εάν δεν πραγματοποιηθεί αυτόματη εκκίνηση του CD, μεταβείτε στην Εξερεύνηση των Windows, κάντε διπλό κλικ στο εικονίδιο του CD-ROM και έπειτα κάντε διπλό κλικ στο αρχείο εγκατάστασης για να ξεκινήσει η εγκατάσταση.

2. Ακολουθήστε τις οδηγίες στην οθόνη.

   - Εάν αγοράσατε το προϊόν σε CD από ένα κατάστημα, μπορείτε να βρείτε το κλειδί της συνδρομής στο κάλυμμα του Οδηγού γρήγορης εγκατάστασης.
   - Εάν εκτελέσατε λήψη του προϊόντος από το F-Secure eStore, το κλειδί της συνδρομής περιλαμβάνεται στο μήνυμα ηλεκτρονικού ταχυδρομείου επιβεβαίωσης της παραγγελίας αγοράς.

   Μπορεί να χρειαστεί επανεκκίνηση του υπολογιστή πριν από την επικύρωση της συνδρομής σας και τη λήψη των πιο πρόσφατων ενημερώσεων από το Internet. Εάν εκτελείτε την εγκατάσταση από το CD, φροντίστε να αφαιρέσετε το CD εγκατάστασης πριν επανεκκινήσετε τον υπολογιστή.

1.3 Εγκατάσταση και αναβάθμιση εφαρμογών

Οδηγίες για ενεργοποίηση της νέας συνδρομής σας.

Ακολουθήστε αυτές τις οδηγίες για να ενεργοποιήσετε τη νέα σας συνδρομή ή για να εγκαταστήσετε μια νέα εφαρμογή χρησιμοποιώντας το πλαίσιο εκκίνησης:

Σημείωση: Το εικονίδιο του πλαισίου εκκίνησης βρίσκεται στην περιοχή ειδοποιήσεων των Windows.

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων.
   Εμφανίζεται ένα αναδυόμενο μενού.
2. Επιλέξτε **Προβολή των συνδρομών μου**.
3. Στην περιοχή **Οι συνδρομές μου**, μεταβείτε στη σελίδα **Κατάσταση συνδρομής** και επιλέξτε **Ενεργοποίηση συνδρομής**.
   Ανοίγει το παράθυρο **Ενεργοποίηση συνδρομής**.
4. Πληκτρολογήστε το κλειδί συνδρομής σας για την εφαρμογή και επιλέξτε **OK**.
5. Αφού επικυρωθεί και ενεργοποιηθεί η συνδρομή σας, επιλέξτε **Κλείσιμο**.
6. Στην περιοχή **Οι συνδρομές μου**, μεταβείτε στη σελίδα **Κατάσταση εγκατάστασης**. Εάν δεν ξεκινήσει αυτόματα η εγκατάσταση, ακολουθήστε τις εξής οδηγίες:
   a) Επιλέξτε **Εγκατάσταση**.
      Ανοίγει το παράθυρο εγκατάστασης.

b) Κάντε κλικ στην επιλογή **Επόμενο**.
Πραγματοποιείται λήψη της εφαρμογής και ξεκινά η εγκατάσταση.
c) Όταν ολοκληρωθεί η εγκατάσταση, επιλέξτε **Κλείσιμο**.

Η νέα συνδρομή έχει ενεργοποιηθεί.

1.4 Βοήθεια και υποστήριξη

Μπορείτε να αποκτήσετε πρόσβαση στην online βοήθεια του προϊόντος κάνοντας κλικ στο εικονίδιο "Βοήθεια" ή πατώντας `F1` σε οποιαδήποτε οθόνη του προϊόντος.

Έναρξη

Θέματα:

Πληροφορίες σχετικά με το πώς θα ξεκινήσετε με το προϊόν.

Αυτή η ενότητα περιγράφει πώς μπορείτε να αλλάξετε κοινές ρυθμίσεις και να διαχειριστείτε τις συνδρομές σας για το προϊόν.

Στις ρυθμίσεις περιλαμβάνονται:

- Λήψεις, όπου μπορείτε να δείτε πληροφορίες για τις ενημερώσεις που έχουν ληφθεί και να ελέγξετε μη αυτόματα εάν υπάρχουν διαθέσιμες νέες ενημερώσεις.
- Ρυθμίσεις σύνδεσης, όπου μπορείτε να αλλάξετε τον τρόπο με τον οποίο ο υπολογιστής σας συνδέεται στο Internet.
- Ειδοποιήσεις, όπου μπορείτε να δείτε προηγούμενες ειδοποιήσεις και να ορίσετε τι είδους ειδοποιήσεις θέλετε να βλέπετε.
- Συνδρομές για τα προγράμματα που είναι εγκατεστημένα.

2.1 Πού μπορώ να βρω το αναγνωριστικό του λογαριασμού μου;

Η υποστήριξη πελατών μας μπορεί να ζητήσει το αναγνωριστικό λογαριασμού σας εάν χρειαστεί να επικοινωνήσετε μαζί μας.

Για προβολή του λογαριασμού σας και των κωδικών ταυτότητας συσκευής:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων.
   Εμφανίζεται ένα αναδυόμενο μενού.
2. Επιλέξτε **Προβολή των συνδρομών μου**.
3. Επιλέξτε **Κωδικοί ταυτότητας**.

Η σελίδα εμφανίζει το λογαριασμό σας και τους τρέχοντες κωδικούς ταυτότητας συσκευής που μπορείτε να χρησιμοποιείτε για τη διαχείριση των συνδρομών σας.

2.2 Χρήση του κέντρου ενεργειών

Το Κέντρο ενεργειών εμφανίζει σημαντικές ειδοποιήσεις που απαιτούν την προσοχή σας.

Εάν το Κέντρο ενεργειών έχει τυχόν εκκρεμείς ενέργειες, θα σας τις υπενθυμίζει κατά διαστήματα.

2.2.1 Άνοιγμα του κέντρου ενεργειών

Ανοίξτε το κέντρο ενεργειών για προβολή όλων των ειδοποιήσεων που απαιτούν την προσοχή σας.

Για να ανοίξετε το κέντρο ενεργειών:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων.
   Το στοιχείο **Άνοιγμα του Κέντρου ενεργειών** στο αναδυόμενο μενού εμφανίζει τις εκκρεμείς ενέργειες.
2. Επιλέξτε **Άνοιγμα του κέντρου ενεργειών**.
   Το κέντρο ενεργειών εμφανίζει μια λίστα όλων των στοιχείων που πρέπει να επιλυθούν.
3. Κάντε κλικ στο στοιχείο που βρίσκεται στη λίστα για να δείτε περισσότερες πληροφορίες για αυτό.
4. Εάν δεν θέλετε να πραγματοποιήσετε καμία ενέργεια σε στοιχεία που δεν έχουν επιλυθεί αυτή τη στιγμή, κάντε κλικ στην επιλογή **Αναβολή** για να τα επιλύσετε αργότερα.

   Σημείωση: Εάν έχετε πολλά στοιχεία στο Κέντρο ενεργειών, κάντε κλικ στην επιλογή **Αναβολή όλων** για να κλείσετε το Κέντρο ενεργειών και να επιλύσετε όλα τα στοιχεία αργότερα.

2.2.2 Εγκατάσταση αναβάθμισης προϊόντος

Όταν είναι διαθέσιμη μια δωρεάν αναβάθμιση ενός προϊόντος που έχετε εγκαταστήσει, πρέπει να την εγκαταστήσετε για να μπορέσετε να χρησιμοποιήσετε τη νέα έκδοση.

Για αναβάθμιση του προϊόντος:

1. Ανοίξτε το Κέντρο ενεργειών.
   Το Κέντρο ενεργειών εμφανίζει το στοιχείο **Διαθέσιμη αναβάθμιση προϊόντος**. Εάν έχετε πολλά στοιχεία στο Κέντρο ενεργειών, κάντε κλικ στο στοιχείο για να το ανοίξετε.
2. Κάντε κλικ στο κουμπί **Αναβάθμιση**.

   Σημείωση: Πρέπει να αποδεχτείτε τους νέους όρους άδειας χρήσης για να πραγματοποιήσετε αναβάθμιση του προϊόντος εάν έχουν αλλάξει.

Όταν ολοκληρωθεί η αναβάθμιση, μπορεί να χρειαστεί να επανεκκινήσετε τον υπολογιστή σας.

2.2.3 Εγκατάσταση νέου προϊόντος

Εάν ένα νέο προϊόν προστεθεί στη συνδρομή σας, μπορείτε να το εγκαταστήσετε για να το χρησιμοποιήσετε.

Τα νέα προϊόντα μπορούν να προστεθούν στη συνδρομή σας ενώ είναι ακόμη έγκυρη.

Για εγκατάσταση ενός νέου προϊόντος:

1. Ανοίξτε το Κέντρο ενεργειών.
   Το Κέντρο ενεργειών εμφανίζει το στοιχείο **Εγκατάσταση νέου προϊόντος**. Εάν έχετε πολλά στοιχεία στο Κέντρο ενεργειών, κάντε κλικ στο στοιχείο για να το ανοίξετε.
2. Επιλέξτε **Εγκατάσταση**.

   Σημείωση: Εάν δεν θέλετε να εγκαταστήσετε το προϊόν, μπορείτε να κάνετε κλικ στο εικονίδιο του κάδου απορριμμάτων που βρίσκεται στην πάνω δεξιά γωνία για να κλείσετε την υπενθύμιση και να την καταργήσετε από το Κέντρο ενεργειών.

3. Ακολουθήστε τις οδηγίες του οδηγού εγκατάστασης για να εγκαταστήσετε το προϊόν.

Όταν ολοκληρωθεί η εγκατάσταση, μπορεί να χρειαστεί να επανεκκινήσετε τον υπολογιστή σας.

2.2.4 Αντικαταστήστε ένα προϊόν που λήγει

Εάν η συνδρομή σας λήγει και το προϊόν που έχετε εγκαταστήσει δεν είναι πλέον διαθέσιμο, δεν μπορείτε να συνεχίσετε τη συνδρομή σας αλλά μπορείτε να πραγματοποιήσετε αναβάθμιση στο νέο προϊόν δωρεάν.

Για αναβάθμιση του προϊόντος:

1. Ανοίξτε το Κέντρο ενεργειών.
   Το Κέντρο ενεργειών εμφανίζει το στοιχείο **Αναβάθμιση προϊόντος**. Εάν έχετε πολλά στοιχεία στο Κέντρο ενεργειών, κάντε κλικ στο στοιχείο για να το ανοίξετε.
2. Κάντε κλικ στο κουμπί **Αναβάθμιση**.

Όταν ολοκληρωθεί η αναβάθμιση, μπορεί να χρειαστεί να επανεκκινήσετε τον υπολογιστή σας.

2.3 Πώς μπορώ να μάθω εάν η συνδρομή μου είναι έγκυρη;

Ο τύπος και η κατάσταση της συνδρομής σας εμφανίζονται στη σελίδα **Συνδρομές**.

Όταν η συνδρομή πρόκειται να λήξει ή έχει λήξει, η συνολική κατάσταση προστασίας του προγράμματος αλλάζει.

Για να ελέγξετε την ισχύ της συνδρομής σας:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων.
   Εμφανίζεται ένα αναδυόμενο μενού.
2. Επιλέξτε **Προβολή των συνδρομών μου**.
3. Επιλέξτε ένα από τα εξής:
   - Επιλέξτε **Συνδρομές** για να δείτε πληροφορίες για τις συνδρομές σας όσον αφορά εγκατεστημένα προγράμματα.
   - Επιλέξτε **Εγκατάσταση** για να δείτε ποια προγράμματα είναι διαθέσιμα για εγκατάσταση.

Εάν η συνδρομή σας έχει λήξει, πρέπει να την ανανεώσετε για να συνεχίσετε να λαμβάνετε ενημερώσεις και να χρησιμοποιείτε το προϊόν.

2.3.1 Ενεργοποίηση συνδρομής

Όταν έχετε ένα κλειδί συνδρομής ή έναν κωδικό καμπάνιας για ένα προϊόν, θα πρέπει να το ενεργοποιήσετε.

Για ενεργοποίηση συνδρομής:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων.
   Εμφανίζεται ένα αναδυόμενο μενού.
2. Επιλέξτε **Προβολή των συνδρομών μου**.
3. Κάντε κλικ στην επιλογή **Προσθήκη νέας συνδρομής**.
4. Στο πλαίσιο διαλόγου που ανοίγει, εισαγάγετε το νέο κλειδί συνδρομής ή τον κωδικό καμπάνιας και επιλέξτε **Επικύρωση**.

Συμβουλή: Εάν λάβατε το κλειδί συνδρομής μέσω ηλεκτρονικού ταχυδρομείου, μπορείτε να αντιγράψετε το κλειδί από το μήνυμα ηλεκτρονικού ταχυδρομείου και να το επικολλήσετε στο πεδίο.

Αφού εισαγάγετε το νέο κλειδί συνδρομής, η νέα ημερομηνία ισχύος της συνδρομής εμφανίζεται στη σελίδα **Συνδρομές**.

2.3.2 Ανανέωση της συνδρομής σας

Όταν η συνδρομή προϊόντος πρόκειται να λήξει, πρέπει να την ανανεώσετε για να συνεχίσετε να χρησιμοποιείτε το προϊόν.

Για να ανανεώσετε τη συνδρομή σας:

1. Ανοίξτε το Κέντρο ενεργειών.
   Το Κέντρο ενεργειών εμφανίζει το στοιχείο **Ανανέωση συνδρομής**. Εάν έχετε πολλά στοιχεία στο Κέντρο ενεργειών, κάντε κλικ στο στοιχείο για να το ανοίξετε.
2. Χρειάζεστε ένα νέο κλειδί συνδρομής για να ανανεώσετε τη συνδρομή σας.
   - Εάν έχετε ήδη μια διαθέσιμη συνδρομή που μπορείτε να χρησιμοποιήσετε για αυτό τον υπολογιστή, κάντε κλικ στην επιλογή **Ενεργοποίηση** για να χρησιμοποιήσετε τη νέα συνδρομή.
   - Εάν έχετε ήδη προμηθευτεί ένα νέο κλειδί συνδρομής, κάντε κλικ στην επιλογή **Εισαγωγή κλειδιού**.

     Στο παράθυρο διαλόγου που ανοίγει, πληκτρολογήστε το νέο κλειδί συνδρομής και κάντε κλικ στο κουμπί **OK**.
   - Διαφορετικά, κάντε κλικ στο κουμπί **Ανανέωση τώρα**.

     Μπορείτε να ανανεώσετε τη συνδρομή σας στο ηλεκτρονικό μας κατάστημα. Όταν ανανεώνετε τη συνδρομή σας, λαμβάνετε ένα νέο κλειδί συνδρομής.

Σημείωση: Εάν η συνδρομή σας δεν έχει λήξει ακόμη, μπορείτε να κάνετε κλικ στο εικονίδιο του κάδου απορριμμάτων που βρίσκεται στην πάνω δεξιά γωνία για να κλείσετε την υπενθύμιση και να την καταργήσετε από το Κέντρο ενεργειών.

Εάν δεν θέλετε να ανανεώσετε τη συνδρομή σας, καταργήστε την εγκατάσταση του προϊόντος με τη συνδρομή που έχει λήξει.

2.4 Χρήση αυτόματων ενημερώσεων

Οι Αυτόματες ενημερώσεις διατηρούν τον υπολογιστή σας προστατευμένο από τις πιο πρόσφατες απειλές.

Το προϊόν πραγματοποιεί αυτόματα ανάκτηση των τελευταίων ενημερώσεων στον υπολογιστή σας όταν είστε συνδεδεμένοι στο Internet. Εντοπίζει την κυκλοφορία του δικτύου και δεν διαταράσσει άλλη χρήση του Internet ακόμα και με αργή σύνδεση δικτύου.

2.4.1 Έλεγχος της κατάστασης ενημέρωσης

Προβάλετε την ημερομηνία και την ώρα της τελευταίας ενημέρωσης.

Συνήθως, δεν χρειάζεται να ελέγχετε τις ενημερώσεις μόνοι σας καθώς το προϊόν λαμβάνει αυτόματα τις πιο πρόσφατες ενημερώσεις όταν είστε συνδεδεμένοι στο Internet και είναι ενεργοποιημένες οι Αυτόματες ενημερώσεις.

Για να βεβαιωθείτε ότι έχετε τις τελευταίες ενημερώσεις:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων.
   Εμφανίζεται ένα αναδυόμενο μενού.
2. Επιλέξτε **Άνοιγμα κοινών ρυθμίσεων**.
3. Επιλέξτε **Στοιχεία λήψης**.
4. Πατήστε **Άμεσος έλεγχος**.
   Το προϊόν πραγματοποιεί ανάκτηση των τελευταίων ενημερώσεων, εάν υπάρχουν.

Σημείωση: Η σύνδεσή σας στο Internet πρέπει να είναι ενεργή όταν θέλετε να ελέγξετε για τις τελευταίες ενημερώσεις.

2.4.2 Αλλαγή των ρυθμίσεων σύνδεσης στο Internet

Συνήθως δεν χρειάζεται να αλλάξετε τις προεπιλεγμένες ρυθμίσεις, αλλά μπορείτε να ρυθμίσετε τον τρόπο με τον οποίο είναι συνδεδεμένος ο υπολογιστής στο Internet ώστε να μπορείτε να λαμβάνετε ενημερώσεις αυτόματα.

Για να αλλάξετε τις ρυθμίσεις της σύνδεσης στο Internet:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων. Εμφανίζεται ένα αναδυόμενο μενού.
2. Επιλέξτε **Άνοιγμα κοινών ρυθμίσεων**.
3. Επιλέξτε **Σύνδεση**.
4. Στη λίστα **Σύνδεση Internet**, επιλέξτε τον τρόπο σύνδεσης του υπολογιστή σας στο Internet..
   - Επιλέξτε **Να θεωρείται ότι η σύνδεση είναι μόνιμη** εάν έχετε μια μόνιμη σύνδεση δικτύου.

     Σημείωση: Εάν ο υπολογιστής δεν έχει μόνιμη σύνδεση δικτύου και είναι ρυθμισμένος για κλήση κατ' απαίτηση, η επιλογή **Να θεωρείται ότι η σύνδεση είναι μόνιμη** μπορεί να καταλήξει σε πολλαπλές κλήσεις μέσω τηλεφώνου.
   - Επιλέξτε **Εντοπισμός σύνδεσης** για να ανακτήσετε ενημερώσεις μόνον όταν το προϊόν εντοπίσει μια ενεργή σύνδεση δικτύου.
   - Επιλέξτε **Εντοπισμός κυκλοφορίας** για να ανακτήσετε ενημερώσεις μόνο όταν το προϊόν εντοπίσει άλλη κυκλοφορία δικτύου.

     Συμβουλή: Εάν έχετε μια ασυνήθιστη διαμόρφωση παραμέτρων υλικού που περιλαμβάνει τη ρύθμιση **Εντοπισμός σύνδεσης** για τον εντοπισμό μιας ενεργής σύνδεσης δικτύου ακόμα και όταν δεν υπάρχει, επιλέξτε **Εντοπισμός κυκλοφορίας**.
5. Στη λίστα **Διακομιστής μεσολάβησης HTTP**, επιλέξτε εάν ο υπολογιστής σας θα χρησιμοποιεί ή όχι *διακομιστή μεσολάβησης* για σύνδεση στο Internet.
   - Επιλέξτε **Χωρίς διακομ. μεσολάβησης HTTP** εάν ο υπολογιστής σας συνδέεται απευθείας στο Internet.
   - Επιλέξτε **Μη αυτόματη ρύθμιση διακομιστή μεσολάβ. HTTP** για να διαμορφώσετε τις ρυθμίσεις του *διακομιστή μεσολάβησης HTTP*.
   - Επιλέξτε **Χρήση διακομιστή μεσολάβησης HTTP του προγράμματος περιήγησής μου** για να χρησιμοποιήσετε τις ίδιες ρυθμίσεις *διακομιστή μεσολάβησης HTTP* που έχετε ορίσει στο πρόγραμμα περιήγησης web που διαθέτετε.

2.4.3 Αλλαγή των ρυθμίσεων κινητού Internet ευρείας ζώνης

Επιλέξτε εάν θέλετε να πραγματοποιείτε λήψη ενημερώσεων ασφαλείας όταν χρησιμοποιείτε κινητό Internet ευρείας ζώνης.

Σημείωση: Αυτό το χαρακτηριστικό είναι διαθέσιμο μόνο στα Microsoft Windows 7 και σε νεότερες εκδόσεις των Windows.

Από προεπιλογή, η λήψη των ενημερώσεων ασφαλείας πραγματοποιείται πάντα όταν βρίσκεστε στο δίκτυο του οικιακού παρόχου σας. Ωστόσο, οι ενημερώσεις αναστέλλονται όταν επισκέπτεστε ένα δίκτυο άλλου παρόχου. Αυτό συμβαίνει διότι οι τιμές των συνδέσεων μπορεί να ποικίλλουν ανάλογα με τον πάροχο, για παράδειγμα, σε διαφορετικές χώρες. Ίσως να μην πρέπει να αλλάξετε αυτή τη ρύθμιση, εάν θέλετε να εξοικονομήσετε εύρος ζώνης και πιθανόν και έξοδα, κατά τη διάρκεια της επίσκεψής σας.

Σημείωση: Αυτή η ρύθμιση ισχύει μόνο για συνδέσεις κινητού Internet ευρείας ζώνης. Όταν ο υπολογιστής είναι συνδεδεμένος σε ένα ενσύρματο ή ασύρματο δίκτυο, το προϊόν ενημερώνεται αυτόματα.

Για να αλλάξετε τη ρύθμιση:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων.
   Εμφανίζεται ένα αναδυόμενο μενού.
2. Επιλέξτε **Άνοιγμα κοινών ρυθμίσεων**.
3. Επιλέξτε **Σύνδεση**.
4. Ενεργοποιήστε την επιθυμητή επιλογή ενημέρωσης για συνδέσεις κινητού Internet:
   - **Ποτέ**

     Δεν λαμβάνονται ενημερώσεις όταν χρησιμοποιείτε κινητό Internet ευρείας ζώνης.
   - **Μόνο στο δίκτυο του φορέα μου**

     Η λήψη ενημερώσεων θα πραγματοποιείται πάντα στο δίκτυο του οικιακού πάροχου. Όταν επισκέπτεστε ένα δίκτυο άλλου πάροχου, οι ενημερώσεις θα αναστέλλονται. Σας προτείνουμε να ενεργοποιήσετε αυτή την επιλογή για να διατηρήσετε το προϊόν ασφαλείας ενημερωμένο στο αναμενόμενο κόστος.
   - **Πάντα**

     Η λήψη των ενημερώσεων θα πραγματοποιείται πάντα, ανεξαρτήτως δικτύου. Ενεργοποιήστε αυτή την επιλογή εάν θέλετε να βεβαιωθείτε ότι η ασφάλεια του υπολογιστή σας θα είναι πάντα ενημερωμένη ανεξαρτήτως κόστους.

     Σημείωση: Εάν θέλετε να αποφασίζετε κάθε φορά που πραγματοποιείτε έξοδο από το δίκτυο του οικείου παρόχου σας, επιλέξτε **Να γίνεται ερώτηση πριν την περιαγωγή σε νέο δίκτυο** .

Ενημερώσεις ασφαλείας σε αναστολή

Οι ενημερώσεις ασφαλείας μπορεί να ανασταλούν όταν χρησιμοποιείτε κινητό Internet ευρείας ζώνης εκτός του δικτύου του οικιακού τελεστή σας.

Στην περίπτωση αυτή, μπορείτε να δείτε την ειδοποίηση **Σε αναστολή** στην κάτω δεξιά γωνία της οθόνης σας. Οι ενημερώσεις αναστέλλονται επειδή οι τιμές των συνδέσεων ενδέχεται να διαφέρουν μεταξύ των τελεστών, για παράδειγμα, σε διαφορετικές χώρες. Μπορείτε να εξετάσετε το ενδεχόμενο να διατηρήσετε ίδια αυτή τη ρύθμιση, εάν θέλετε εξοικονόμηση του εύρους ζώνης και πιθανόν του κόστους, κατά τη διάρκεια της επίσκεψής σας. Ωστόσο, εάν εξακολουθείτε να θέλετε να αλλάξετε τις ρυθμίσεις, κάντε κλικ στη σύνδεση **Αλλαγή**.

Σημείωση: Αυτό το χαρακτηριστικό είναι διαθέσιμο μόνο στα Microsoft Windows 7 και σε νεότερες εκδόσεις των Windows.

2.5 Πώς μπορώ να δω τις ενέργειες του προϊόντος;

Μπορείτε να δείτε τις ενέργειες του προϊόντος για την προστασία του υπολογιστή σας στη σελίδα **Λωρίδα χρόνου προϊόντος**.

Το προϊόν θα εμφανίσει μια ειδοποίηση όταν προβεί σε μια ενέργεια, όπως για παράδειγμα για να προστατέψει αρχεία που είναι αποθηκευμένα στον υπολογιστή σας. Ορισμένες ειδοποιήσεις μπορούν επίσης να σταλούν μέσω του πάροχου υπηρεσιών σας, ώστε να σας ενημερώσουν, για παράδειγμα, για νέες διαθέσιμες υπηρεσίες.

Για να προβάλλετε τη λωρίδα χρόνου προϊόντος:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων.
   Εμφανίζεται ένα αναδυόμενο μενού.
2. Κάντε κλικ στην επιλογή **Άνοιγμα λωρίδας χρόνου προϊόντος**.
   Ανοίγει η λίστα ειδοποιήσεων της λωρίδας χρόνου του προϊόντος.

2.6 Λειτουργία παιχνιδιών

Ενεργοποιήστε τη *λειτουργία παιχνιδιών* όταν θέλετε να απελευθερώσετε πόρους του συστήματος ενώ παίζετε παιχνίδια στον υπολογιστή.

Τα παιχνίδια υπολογιστή συχνά απαιτούν πολλούς πόρους συστήματος για να εκτελούνται ομαλά. Άλλες εφαρμογές που εκτελούνται στο παρασκήνιο μπορούν να μειώσουν την απόδοση του παιχνιδιού καθώς καταναλώνουν πόρους του συστήματος και χρησιμοποιούν το δίκτυό σας.

Η *λειτουργία παιχνιδιών* μειώνει την επίδραση του προϊόντος στον υπολογιστή σας καθώς και τη χρήση του δικτύου. Έτσι, απελευθερώνει περισσότερους πόρους συστήματος για τα παιχνίδια υπολογιστή ενώ παράλληλα διατηρεί την ουσιαστική λειτουργικότητα του προϊόντος. Για παράδειγμα, αναστέλλει τις αυτόματες ενημερώσεις, τις προγραμματισμένες σαρώσεις και άλλες λειτουργίες που ενδέχεται να απαιτούν πολλούς πόρους του συστήματος και κυκλοφορία δικτύου.

Όταν χρησιμοποιείτε οποιαδήποτε εφαρμογή πλήρους οθόνης, για παράδειγμα βλέπετε μια παρουσίαση, μια παρουσίαση διαφανειών ή ένα βίντεο σε λειτουργία πλήρους οθόνης, ή παίζετε ένα παιχνίδι σε λειτουργία πλήρους οθόνης, εμφανίζουμε μόνο τις σημαντικές ειδοποιήσεις εάν απαιτούν την άμεση προσοχή σας. Άλλες ειδοποιήσεις εμφανίζονται μόνο κατά την έξοδο από τη λειτουργία πλήρους οθόνης ή τη *λειτουργία παιχνιδιού*.

2.6.1 Ενεργοποίηση λειτουργίας παιχνιδιών

Ενεργοποιήστε τη *λειτουργία παιχνιδιών* για να βελτιώσετε την απόδοση των παιχνιδιών στον υπολογιστή σας.

Για να ενεργοποιήσετε τη *λειτουργία παιχνιδιών*:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων.
   Εμφανίζεται ένα αναδυόμενο μενού.
2. Επιλέξτε **Λειτουργία παιχνιδιών**.
   Η χρήση των πόρων συστήματος από το προϊόν έχει τώρα βελτιστοποιηθεί ώστε τα παιχνίδια να εκτελούνται ομαλά στον υπολογιστή σας.

Μην ξεχνάτε να απενεργοποιείτε τη *λειτουργία παιχνιδιών* αφού σταματήσετε το παιχνίδι. Η *λειτουργία παιχνιδιών* απενεργοποιείται αυτόματα κατά την επανεκκίνηση του υπολογιστή σας ή την επαναφορά από κατάσταση αναστολής λειτουργίας.

Security Cloud

Θέματα:

Το παρόν έγγραφο περιγράφει το *Security Cloud*, μια online υπηρεσία της F-Secure Corporation που εντοπίζει καθαρές εφαρμογές και τοποθεσίες web ενώ παρέχει προστασία από κακόβουλο λογισμικό και προγράμματα εκμετάλλευσης ευπαθειών τοποθεσιών web.

3.1 Τι είναι το *Security Cloud*;

Το *Security Cloud* είναι μια online υπηρεσία που παρέχει ταχεία απόκριση ενάντια στις πιο πρόσφατες απειλές του Internet.

Ως συμμετέχων, επιτρέπετε στο *Security Cloud* να συλλέξει δεδομένα που μας βοηθούν να ενισχύσουμε την προστασία σας από νέες, πρωτοεμφανιζόμενες απειλές. Το *Security Cloud* συλλέγει πληροφορίες σχετικά με κάποιες άγνωστες, κακόβουλες ή ύποπτες εφαρμογές και μη κατηγοριοποιημένες τοποθεσίες web. Οι πληροφορίες αυτές είναι ανώνυμες και αποστέλλονται στην F-Secure Corporation για ανάλυση συνδυασμού δεδομένων. Χρησιμοποιούμε τις πληροφορίες που αναλύθηκαν για να βελτιώσουμε την προστασία σας από τις πιο πρόσφατες απειλές και κακόβουλα αρχεία.

Πώς λειτουργεί το *Security Cloud*

Το *Security Cloud* συλλέγει πληροφορίες σχετικά με άγνωστες εφαρμογές και τοποθεσίες web καθώς και κακόβουλες εφαρμογές και προγράμματα εκμετάλλευσης ευπαθειών σε τοποθεσίες web. Το *Security Cloud* δεν παρακολουθεί τη δραστηριότητά σας στο web, ούτε συλλέγει πληροφορίες σχετικά με τοποθεσίες web που έχουν ήδη υποβληθεί σε ανάλυση. Επίσης, δεν συλλέγει πληροφορίες σχετικά με καθαρές εφαρμογές που είναι εγκατεστημένες στον υπολογιστή σας.

Εάν δεν θέλετε να συμβάλλετε δεδομένα, το *Security Cloud* δεν συλλέγει πληροφορίες σχετικά με εγκατεστημένες εφαρμογές ή τοποθεσίες web που έχετε επισκεφτεί. Ωστόσο, το προϊόν πρέπει να θέτει ερώτημα στους διακομιστές της F-Secure για τη φήμη των εφαρμογών, των τοποθεσιών web, των μηνυμάτων και άλλων αντικειμένων. Το ερώτημα δημιουργείται με τη βοήθεια ενός αθροίσματος ελέγχου κρυπτογράφησης, ενώ το ίδιο το αντικείμενο για το οποίο δημιουργείται το ερώτημα, δεν αποστέλλεται στην F-Secure. Δεν παρακολουθούμε τα δεδομένα ανά χρήστη. Μόνο ο μετρητής επισκέψεων του αρχείου ή της τοποθεσίας web αυξάνεται.

Δεν είναι δυνατή η πλήρης διακοπή όλης της κυκλοφορίας δικτύου στο *Security Cloud*, καθώς αποτελεί αναπόσπαστο μέρος της προστασίας που παρέχεται από το προϊόν.

3.1.1 Έλεγχος της κατάστασης του *Security Cloud*

Πολλές λειτουργίες του προγράμματος εξαρτώνται από τη συνδεσιμότητα του *Security Cloud* για τη σωστή λειτουργία τους.

Εάν υπάρχουν προβλήματα δικτύου ή εάν το τείχος προστασίας σας εμποδίζει την κυκλοφορία του *Security Cloud*, η κατάσταση είναι "αποσυνδεδεμένο". Εάν δεν έχουν εγκατασταθεί λειτουργίες προϊόντος που απαιτούν πρόσβαση στο *Security Cloud*, η κατάσταση είναι "δεν χρησιμοποιείται".

Για έλεγχο της κατάστασης:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων.
   Εμφανίζεται ένα αναδυόμενο μενού.
2. Επιλέξτε **Άνοιγμα κοινών ρυθμίσεων**.
3. Επιλέξτε **Σύνδεση**.

Στην περιοχή **Security Cloud**, μπορείτε να δείτε την τρέχουσα κατάσταση του *Security Cloud*.

3.2 Πλεονεκτήματα *Security Cloud*

Με το *Security Cloud*, θα έχετε ταχύτερη και ακριβέστερη προστασία από τις πιο πρόσφατες απειλές και δεν θα λαμβάνετε περιττές προειδοποιήσεις σχετικά με ύποπτες εφαρμογές που δεν είναι κακόβουλες.

Ως συμβάλλων στο *Security Cloud*, μπορείτε να μας βοηθήσετε να βρούμε νέο κακόβουλο λογισμικό που δεν έχει εντοπιστεί και να καταργήσουμε πιθανές ψευδείς θετικές αξιολογήσεις.

Όλοι οι συμμετέχοντες στο *Security Cloud* βοηθούν ο ένας τον άλλο. Όταν το *Security Cloud* εντοπίσει μια ύποπτη εφαρμογή, επωφελείστε από τα αποτελέσματα της ανάλυσης εάν η ίδια εφαρμογή έχει ήδη εντοπιστεί από κάποιον άλλο. Το *Security Cloud* βελτιώνει τη συνολική απόδοση καθώς το προϊόν ασφαλείας που έχετε εγκαταστήσει δεν χρειάζεται να σαρώσει εφαρμογές που έχουν αναλυθεί και αξιολογηθεί ως καθαρές από το *Security Cloud*. Παρόμοια, μέσω του *Security Cloud*, κοινοποιούνται πληροφορίες σχετικά με κακόβουλες τοποθεσίες web και αυτόκλητα μηνύματα μαζικής αποστολής και

έχουμε τη δυνατότητα να σας παρέχουμε ακριβέστερη προστασία από τα προγράμματα εκμετάλλευσης ευπαθειών τοποθεσιών web και τα μηνύματα ανεπιθύμητης αλληλογραφίας.

Όσο περισσότεροι συμβάλλουν στο *Security Cloud*, τόσο καλύτερα προστατεύονται οι μεμονωμένοι συμμετέχοντες.

3.3 Τι είδους δεδομένα παραχωρείτε

Ως συμβάλλων, επιτρέπετε στο *Security Cloud* να συλλέγει πληροφορίες σχετικά με εφαρμογές που έχετε εγκαταστήσει και τις τοποθεσίες web που επισκέπτεστε, ώστε το *Security Cloud* να μπορεί να παρέχει καλύτερη προστασία από τις πιο πρόσφατες κακόβουλες εφαρμογές και ύποπτες τοποθεσίες web.

Ανάλυση της φήμης των αρχείων

Το *Security Cloud* συλλέγει πληροφορίες μόνο σχετικά με εφαρμογές που δεν έχουν διαδεδομένη φήμη και με αρχεία που είναι ύποπτα ή γνωστά ως επιβλαβές λογισμικό.

Συλλέγονται αποκλειστικά πληροφορίες σχετικά με (εκτελέσιμα) αρχεία εφαρμογών και όχι σχετικά με κανέναν άλλο τύπο αρχείων.

Ανάλογα με το προϊόν, οι πληροφορίες που συλλέγονται μπορεί να περιλαμβάνουν:

- τη διαδρομή αρχείου της εφαρμογής (εξαιρούνται τυχόν αναγνωρίσιμα προσωπικά στοιχεία),
- το μέγεθος του αρχείου και η ημερομηνία δημιουργίας ή τροποποίησής του,
- χαρακτηριστικά και δικαιώματα αρχείου,
- πληροφορίες υπογραφής αρχείου,
- η τρέχουσα έκδοση του αρχείου και η εταιρία που το δημιούργησε,
- την προέλευση του αρχείου ή το URL λήψης του (εξαιρούνται τυχόν αναγνωρίσιμα προσωπικά στοιχεία),
- Αποτελέσματα ανάλυσης του F-Secure DeepGuard και του προγράμματος προστασίας από ιούς, και
- άλλες παρόμοιες πληροφορίες.

Το *Security Cloud* δεν συλλέγει ποτέ πληροφορίες των προσωπικών σας εγγράφων, εκτός και εάν διαπιστώθηκε ότι είναι μολυσμένα. Για όλους τους τύπους μολυσμένων αρχείων, συλλέγει το όνομα του ιού και την κατάσταση επιδιόρθωσης από μόλυνση του αρχείου.

Υποβολή αρχείων για ανάλυση

Σε ορισμένα προϊόντα, μπορείτε επίσης να υποβάλλετε ύποπτες εφαρμογές για ανάλυση στο *Security Cloud*.

Μπορείτε να υποβάλλετε μεμονωμένες ύποπτες εφαρμογές μη αυτόματα όταν σας το ζητάει το προϊόν ή να ενεργοποιήσετε την αυτόματη μεταφορά ύποπτων εφαρμογών στις ρυθμίσεις του προϊόντος. Το *Security Cloud* δεν αποστέλλει ποτέ τα προσωπικά σας έγγραφα.

Ανάλυση της φήμης της τοποθεσίας web

Το *Security Cloud* δεν παρακολουθεί τη δραστηριότητά σας στο web. Διασφαλίζει ότι οι τοποθεσίες web που επισκέπτεστε είναι ασφαλείς κατά την περιήγηση στο web. Όταν επισκέπτεστε μια τοποθεσία web, το *Security Cloud* ελέγχει την ασφάλεια της και σας ειδοποιεί εάν η τοποθεσία αξιολογείται ως ύποπτη ή επιβλαβής.

Για τη βελτίωση της υπηρεσίας και τη διατήρηση της υψηλής ακρίβειας των αξιολογήσεων, το *Security Cloud* μπορεί να συλλέξει πληροφορίες σχετικά με τοποθεσίες web που έχετε επισκεφτεί. Πληροφορίες συλλέγονται εάν η τοποθεσία που επισκέπτεστε περιέχει κακόβουλο ή ύποπτο περιεχόμενο ή γνωστό πρόγραμμα εκμετάλλευσης ευπαθειών ή εάν το περιεχόμενο της τοποθεσίας δεν έχει αξιολογηθεί ή κατηγοριοποιηθεί ακόμη. Στις πληροφορίες που συλλέγονται περιλαμβάνεται η URL και τα μεταδεδομένα που σχετίζονται με την επίσκεψη και την τοποθεσία web.

Το *Security Cloud* έχει αυστηρούς ελέγχους για να διασφαλίσει ότι δεν γίνεται αποστολή ιδιωτικών δεδομένων. Ο αριθμός των URL που συλλέγονται είναι περιορισμένος. Τα δεδομένα που υποβάλλονται φιλτράρονται για πληροφορίες σχετικά με το απόρρητο πριν από την αποστολή τους και καταργούνται όλα τα πεδία που είναι πιθανό να περιέχουν πληροφορίες οι οποίες μπορεί να συσχετιστούν με το πρόσωπό σας σε μορφή που επιτρέπει την ταυτοποίηση. Το *Security Cloud* δεν αξιολογεί, ούτε αναλύει

ιστοσελίδες σε ιδιωτικά δίκτυα και δεν συλλέγει ποτέ πληροφορίες σχετικά με διευθύνσεις ιδιωτικών δικτύων ή ψευδώνυμα.

Ανάλυση των πληροφοριών του συστήματος

Το *Security Cloud* συλλέγει το όνομα και την έκδοση του λειτουργικού σας συστήματος, πληροφορίες σχετικά με τη σύνδεση Internet και στατιστικά στοιχεία σχετικά με τη χρήση του *Security Cloud* (για παράδειγμα, πόσες φορές έχει τεθεί ερώτημα σχετικά με τη φήμη της τοποθεσίας web και ο μέσος χρόνος που απαιτείται για να εμφανιστεί αποτέλεσμα για το ερώτημα) ώστε να μπορούμε να παρακολουθούμε και να βελτιώνουμε την υπηρεσία.

3.4 Πώς προστατεύεται το απόρρητό σας

Μεταφέρουμε τις πληροφορίες με ασφάλεια και διαγράφουμε αυτόματα οποιαδήποτε προσωπική πληροφορία ενδέχεται να περιέχουν τα δεδομένα.

Η επεξεργασία των πληροφοριών που συλλέχθηκαν δεν γίνεται μεμονωμένα. Ομαδοποιούνται με τις πληροφορίες από άλλους συμβάλλοντες στο *Security Cloud*. Όλα τα δεδομένα αναλύονται στατιστικά και ανώνυμα και αυτό σημαίνει ότι δεν θα συνδεθούν με εσάς με οποιονδήποτε τρόπο.

Οι πληροφορίες που ενδέχεται να οδηγούν στην αναγνώρισή σας, δεν περιλαμβάνονται στα δεδομένα που συλλέγονται. Το *Security Cloud* δεν συλλέγει ιδιωτικές διευθύνσεις IP ή άλλες προσωπικές πληροφορίες, όπως διευθύνσεις ηλεκτρονικού ταχυδρομείου, ονόματα χρήστη και κωδικούς πρόσβασης. Ενώ καταβάλλουμε κάθε προσπάθεια να διαγράψουμε όλα τα δεδομένα αναγνώρισης, είναι πιθανό ορισμένα δεδομένα αναγνώρισης να παραμείνουν στις πληροφορίες που έχουν συλλεχθεί. Στις περιπτώσεις αυτές, δεν θα χρησιμοποιήσουμε τέτοιου είδους πληροφορίες που συλλέχθηκαν χωρίς πρόθεση, για να σας εντοπίσουμε.

Εφαρμόζουμε αυστηρά μέτρα ασφάλειας και φυσικά, διαχειριστικά και τεχνικά μέτρα προστασίας για την προστασία των πληροφοριών που έχουν συλλεχθεί κατά τη μεταφορά, αποθήκευση και επεξεργασία τους. Οι πληροφορίες αποθηκεύονται σε ασφαλείς θέσεις και σε διακομιστές που ελέγχονται από εμάς και βρίσκονται είτε στα γραφεία μας, είτε στα γραφεία των υπεργολάβων μας. Η πρόσβαση στις πληροφορίες που έχουν συλλεχθεί είναι δυνατή μόνο από εξουσιοδοτημένο προσωπικό.

Η F-Secure μπορεί να μοιραστεί τις πληροφορίες που έχουν συλλεχθεί με τις θυγατρικές, τους υπεργολάβους, τους διανομείς και τους συνεργάτες της, όμως, πάντα, με μορφή ανώνυμη, με την οποία δεν θα είναι δυνατή η αναγνώρισή σας.

3.5 Συμβολή στο *Security Cloud*.

Μας βοηθάτε να βελτιώνουμε την προστασία που παρέχεται μέσω του *Security Cloud* παρέχοντας πληροφορίες σχετικά με προγράμματα κακόβουλης λειτουργίας και τοποθεσίες web.

Μπορείτε να επιλέξετε να συμμετέχετε στο *Security Cloud* κατά την εγκατάσταση. Με τις προεπιλεγμένες ρυθμίσεις εγκατάστασης, παρέχετε δεδομένα στο *Security Cloud*. Μπορείτε να αλλάξετε τη ρύθμιση αυτή αργότερα στο προϊόν.

Ακολουθήστε τις παρακάτω οδηγίες για να αλλάξετε τις ρυθμίσεις του *Security Cloud*:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων.
   Εμφανίζεται ένα αναδυόμενο μενού.
2. Επιλέξτε **Άνοιγμα κοινών ρυθμίσεων**.
3. Επιλέξτε **Άλλο** > **Απόρρητο**.
4. Ενεργοποιήστε το πλαίσιο ελέγχου συμμετοχής για να γίνετε συμμετέχων στο *Security Cloud*.

3.6 Ερωτήσεις σχετικά με το *Security Cloud*

Πληροφορίες επικοινωνίας για ερωτήσεις σχετικά με το *Security Cloud*.

Εάν έχετε περισσότερες ερωτήσεις σχετικά με το *Security Cloud*, επικοινωνήστε με την:

F-Secure Corporation

Tammasaarenkatu 7
PL 24
00181 Helsinki
Finland
http://www.f-secure.com/en/web/home_global/support/contact

Η πιο πρόσφατη έκδοση αυτής της πολιτικής είναι διαθέσιμη στην τοποθεσία μας στο web.

Σάρωση του υπολογιστή για επιβλαβή αρχεία

Θέματα:

Η Προστασία από ιούς προστατεύει τον υπολογιστή σας από προγράμματα που μπορεί να κλέψουν προσωπικές πληροφορίες, να προκαλέσουν βλάβη στον υπολογιστή σας ή να τον χρησιμοποιήσουν για παράνομους σκοπούς.

Από προεπιλογή, πραγματοποιείται αυτόματος χειρισμός όλων των τύπων επιβλαβούς λογισμικού όταν εντοπιστούν, ώστε να μην προκαλέσουν ζημία.

Από προεπιλογή, το προϊόν σαρώνει τις μονάδες τοπικού δίσκου, τυχόν αφαιρούμενα μέσα (όπως φορητές μονάδες και CD) και υλικό που έχει ληφθεί αυτόματα.

Μπορείτε επίσης να ορίσετε το προϊόν να σαρώνει αυτόματα τα μηνύματα ηλεκτρονικού ταχυδρομείου σας.

Η Προστασία από ιούς επίσης ελέγχει τον υπολογιστή σας για τυχόν αλλαγές που μπορεί να υποδεικνύουν *κακόβουλο λογισμικό*. Εάν εντοπιστούν επικίνδυνες αλλαγές του συστήματος, για παράδειγμα αλλαγές ρυθμίσεων ή απόπειρες αλλαγής σημαντικών διαδικασιών του συστήματος, το DeepGuard διακόπτει τη λειτουργία αυτού του προγράμματος καθώς μπορεί να αποτελεί *κακόβουλο λογισμικό*.

4.1 Προστασία του υπολογιστή από επιβλαβείς εφαρμογές

Το προϊόν αυτό προστατεύει τον υπολογιστή σας από ιούς και άλλες επιβλαβείς εφαρμογές.

Το προϊόν προστατεύει τον υπολογιστή σας από εφαρμογές που ενδέχεται να υποκλέπτουν τις προσωπικές σας πληροφορίες, να καταστρέφουν τα αρχεία σας ή να χρησιμοποιούν τον υπολογιστή σας για παράνομους σκοπούς.

Η προστασία από ιούς εκτελεί αυτόματα σάρωση του υπολογιστή σας για επιβλαβή αρχεία.

Το DeepGuard παρακολουθεί τις εφαρμογές για τον εντοπισμό και την αποτροπή πιθανώς επιβλαβών αλλαγών στο σύστημά σας και εμποδίζει τους εισβολείς και τις επιβλαβείς εφαρμογές να εισβάλουν στον υπολογιστή σας από το Internet.

Το προϊόν διατηρεί την προστασία ενημερωμένη. Πραγματοποιεί λήψη βάσεων δεδομένων που περιέχουν πληροφορίες σχετικά με τον τρόπο αυτόματης εύρεσης και κατάργησης επιβλαβούς περιεχομένου.

Σημείωση: Το προϊόν πραγματοποιεί λήψη των πιο πρόσφατων βάσεων δεδομένων αφού ολοκληρωθεί η εγκατάσταση. Κατά τη διαδικασία αυτή, η Προστασία από ιούς μπορεί να μην εντοπίσει όλες τις απειλές αλλά άλλες λειτουργίες του προϊόντος, όπως είναι το DeepGuard, διατηρούν τον υπολογιστή σας προστατευμένο.

4.1.1 Εικονίδια κατάστασης προστασίας

Τα εικονίδια της σελίδας **Κατάσταση** σας παρουσιάζουν τη συνολική κατάσταση του προϊόντος και τα χαρακτηριστικά του.

Τα παρακάτω εικονίδια εμφανίζουν την κατάσταση του προϊόντος και τα χαρακτηριστικά ασφαλείας του.

Εικονίδιο κατάστασης	Όνομα κατάστασης	Περιγραφή
	OK	Ο υπολογιστής σας προστατεύεται. Οι λειτουργίες είναι ενεργοποιημένες και λειτουργούν σωστά.
	Πληροφορίες	Το προϊόν σάς ενημερώνει για μια ειδική κατάσταση. Όλες οι λειτουργίες λειτουργούν κανονικά αλλά, για παράδειγμα, το προϊόν πραγματοποιεί λήψη ενημερώσεων.
	Προειδοποίηση	Ο υπολογιστής σας δεν προστατεύεται πλήρως. Το προϊόν απαιτεί την προσοχή σας. Για παράδειγμα, δεν έχει λάβει ενημερώσεις για αρκετό καιρό.
	Σφάλμα	Ο υπολογιστής σας δεν προστατεύεται. Για παράδειγμα, η συνδρομή σας έχει λήξει ή κάποια σημαντική δυνατότητα είναι απενεργοποιημένη.

Εικονίδιο κατάστασης	Όνομα κατάστασης	Περιγραφή
	Απενεργοποίηση	Μια μη κρίσιμη λειτουργία είναι απενεργοποιημένη.

4.1.2 Προβολή των στατιστικών του προϊόντος

Μπορείτε να δείτε τη δραστηριότητα του προϊόντος μετά την εγκατάσταση στη σελίδα **Στατιστικά**.

Για να ανοίξετε τη σελίδα **Στατιστικά**:

Κάντε κλικ στην επιλογή **Στατιστικά**.

Η σελίδα **Στατιστικά** εμφανίζει τα παρακάτω:

- Η επιλογή **Προστασία από ιούς** εμφανίζει τον αριθμό των αρχείων που το προϊόν έχει σαρώσει και καθαρίσει από την εγκατάσταση.
- Η επιλογή **Εφαρμογές** δείχνει πόσα προγράμματα έχει επιτρέψει ή αποκλείσει το DeepGuard από την εγκατάσταση και μετά.

4.1.3 Χειρισμός των ενημερώσεων του προϊόντος

Το προϊόν διατηρεί αυτόματα ενημερωμένη την προστασία.

Προβολή εκδόσεων βάσης δεδομένων

Μπορείτε να δείτε τις ώρες των πιο πρόσφατων ενημερώσεων και τους αριθμούς έκδοσης στη σελίδα **Εκδόσεις βάσης δεδομένων**.

Για να ανοίξετε τη σελίδα **Εκδόσεις βάσης δεδομένων**:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **Εκδόσεις βάσης δεδομένων**.

Η σελίδα **Εκδόσεις βάσης δεδομένων** εμφανίζει την πιο πρόσφατη ημερομηνία ενημέρωσης των ορισμών ιών και κατασκοπευτικών προγραμμάτων, του DeepGuard και του φιλτραρίσματος ανεπιθύμητης αλληλογραφίας και ηλεκτρονικού "ψαρέματος" καθώς και οι αριθμοί εκδόσεών τους.

Αλλαγή των ρυθμίσεων κινητού Internet ευρείας ζώνης

Επιλέξτε εάν θέλετε να πραγματοποιείτε λήψη ενημερώσεων ασφαλείας όταν χρησιμοποιείτε κινητό Internet ευρείας ζώνης.

Σημείωση: Αυτό το χαρακτηριστικό είναι διαθέσιμο μόνο στα Microsoft Windows 7 και σε νεότερες εκδόσεις των Windows.

Από προεπιλογή, η λήψη των ενημερώσεων ασφαλείας πραγματοποιείται πάντα όταν βρίσκεστε στο δίκτυο του οικιακού παρόχου σας. Ωστόσο, οι ενημερώσεις αναστέλλονται όταν επισκέπτεστε ένα δίκτυο άλλου παρόχου. Αυτό συμβαίνει διότι οι τιμές των συνδέσεων μπορεί να ποικίλλουν ανάλογα με τον πάροχο, για παράδειγμα, σε διαφορετικές χώρες. Ίσως να μην πρέπει να αλλάξετε αυτή τη ρύθμιση, εάν θέλετε να εξοικονομήσετε εύρος ζώνης και πιθανόν και έξοδα, κατά τη διάρκεια της επίσκεψής σας.

Σημείωση: Αυτή η ρύθμιση ισχύει μόνο για συνδέσεις κινητού Internet ευρείας ζώνης. Όταν ο υπολογιστής είναι συνδεδεμένος σε ένα ενσύρματο ή ασύρματο δίκτυο, το προϊόν ενημερώνεται αυτόματα.

Για να αλλάξετε τη ρύθμιση:

1. Κάντε δεξί κλικ στο εικονίδιο του προϊόντος στην περιοχή ειδοποιήσεων. Εμφανίζεται ένα αναδυόμενο μενού.
2. Επιλέξτε **Άνοιγμα κοινών ρυθμίσεων**.

3. Επιλέξτε **Σύνδεση**.
4. Ενεργοποιήστε την επιθυμητή επιλογή ενημέρωσης για συνδέσεις κινητού Internet:
   - **Ποτέ**

     Δεν λαμβάνονται ενημερώσεις όταν χρησιμοποιείτε κινητό Internet ευρείας ζώνης.
   - **Μόνο στο δίκτυο του φορέα μου**

     Η λήψη ενημερώσεων θα πραγματοποιείται πάντα στο δίκτυο του οικιακού πάροχου. Όταν επισκέπτεστε ένα δίκτυο άλλου πάροχου, οι ενημερώσεις θα αναστέλλονται. Σας προτείνουμε να ενεργοποιήσετε αυτή την επιλογή για να διατηρήσετε το προϊόν ασφαλείας ενημερωμένο στο αναμενόμενο κόστος.
   - **Πάντα**

     Η λήψη των ενημερώσεων θα πραγματοποιείται πάντα, ανεξαρτήτως δικτύου. Ενεργοποιήστε αυτή την επιλογή εάν θέλετε να βεβαιωθείτε ότι η ασφάλεια του υπολογιστή σας θα είναι πάντα ενημερωμένη ανεξαρτήτως κόστους.

     Σημείωση: Εάν θέλετε να αποφασίζετε κάθε φορά που πραγματοποιείτε έξοδο από το δίκτυο του οικείου παρόχου σας, επιλέξτε **Να γίνεται ερώτηση πριν την περιαγωγή σε νέο δίκτυο** .

Ενημερώσεις ασφαλείας σε αναστολή

Οι ενημερώσεις ασφαλείας μπορεί να ανασταλούν όταν χρησιμοποιείτε κινητό Internet ευρείας ζώνης εκτός του δικτύου του οικιακού τελεστή σας.

Στην περίπτωση αυτή, μπορείτε να δείτε την ειδοποίηση **Σε αναστολή** στην κάτω δεξιά γωνία της οθόνης σας. Οι ενημερώσεις αναστέλλονται επειδή οι τιμές των συνδέσεων ενδέχεται να διαφέρουν μεταξύ των τελεστών, για παράδειγμα, σε διαφορετικές χώρες. Μπορείτε να εξετάσετε το ενδεχόμενο να διατηρήσετε ίδια αυτή τη ρύθμιση, εάν θέλετε εξοικονόμηση του εύρους ζώνης και πιθανόν του κόστους, κατά τη διάρκεια της επίσκεψής σας. Ωστόσο, εάν εξακολουθείτε να θέλετε να αλλάξετε τις ρυθμίσεις, κάντε κλικ στη σύνδεση **Αλλαγή**.

Σημείωση: Αυτό το χαρακτηριστικό είναι διαθέσιμο μόνο στα Microsoft Windows 7 και σε νεότερες εκδόσεις των Windows.

4.1.4 Τι είναι οι ιοί και το επιβλαβές λογισμικό;

Το επιβλαβές λογισμικό είναι προγράμματα τα οποία έχουν σχεδιαστεί ειδικά για να προκαλέσουν βλάβη στον υπολογιστή σας, να χρησιμοποιήσουν τον υπολογιστή σας για παράνομους σκοπούς εν αγνοία σας ή να κλέψουν πληροφορίες από τον υπολογιστή σας.

Το επιβλαβές λογισμικό μπορεί:

- να αναλάβει τον έλεγχο του προγράμματος περιήγησης στο Web,
- να ανακατευθύνει τις προσπάθειές σας για αναζήτηση,
- να εμφανίσει ανεπιθύμητες διαφημίσεις
- να παρακολουθεί τις τοποθεσίες που επισκέπτεστε στο Web,
- να κλέψει προσωπικές πληροφορίες, όπως τραπεζικά στοιχεία,
- να χρησιμοποιεί τον υπολογιστή σας για αποστολή ανεπιθύμητης αλληλογραφίας, και
- να χρησιμοποιεί τον υπολογιστή σας για επίθεση σε άλλους υπολογιστές.

Το επιβλαβές λογισμικό μπορεί επίσης να προκαλέσει αργή και ασταθή λειτουργία του υπολογιστή σας. Μπορείτε να υποψιαστείτε ότι έχετε κάποιο *επιβλαβές λογισμικό* στον υπολογιστή σας αν ξαφνικά γίνει πολύ αργός και η λειτουργία του διακόπτεται συχνά.

Ιοί

Οι ιοί είναι συνήθως προγράμματα που μπορούν να προσαρτηθούν σε αρχεία και να αναπαράγονται επανειλημμένα. Μπορούν να τροποποιήσουν και να αντικαταστήσουν τα περιεχόμενα άλλων αρχείων με τρόπο που ενδέχεται να βλάψει τον υπολογιστή σας.

Ένας *ιός* είναι ένα πρόγραμμα του οποίου η εγκατάσταση γίνεται στον υπολογιστή χωρίς να το γνωρίζετε. Όταν εγκατασταθεί, ο ιός επιχειρεί να αναπαραχθεί. Ο ιός:

- χρησιμοποιεί κάποιους από τους πόρους συστήματος του υπολογιστή σας,
- μπορεί να τροποποιήσει ή να προκαλέσει βλάβη σε αρχεία του υπολογιστή σας,
- πιθανώς προσπαθεί να χρησιμοποιήσει τον υπολογιστή σας για να μολύνει άλλους υπολογιστές,
- μπορεί να επιτρέψει τη χρήση του υπολογιστή σας για παράνομους σκοπούς.

Κατασκοπευτικό λογισμικό

Το κατασκοπευτικό λογισμικό είναι προγράμματα που συλλέγουν τα προσωπικά σας στοιχεία.

Το κατασκοπευτικό λογισμικό είναι προγράμματα μπορεί να συλλέγουν προσωπικές πληροφορίες, όπως:

- τοποθεσίες Internet που έχετε επισκεφθεί,
- διευθύνσεις ηλεκτρονικού ταχυδρομείου από τον υπολογιστή σας,
- κωδικούς πρόσβασης, ή
- αριθμούς πιστωτικών καρτών.

Το κατασκοπευτικό λογισμικό εγκαθίσταται μόνο του σχεδόν πάντα χωρίς τη ρητή άδειά σας. Το κατασκοπευτικό λογισμικό μπορεί να εγκατασταθεί μαζί με ένα χρήσιμο πρόγραμμα ή εξαπατώντας σας ώστε να κάνετε κλικ σε κάποια επιλογή ενός παραπλανητικού αναδυόμενου παραθύρου.

Rootkit

Τα rootkit είναι προγράμματα που δυσχεραίνουν την ανεύρεση άλλου *επιβλαβούς λογισμικού*.

Τα rootkit αποκρύπτουν αρχεία και διεργασίες.Γενικά, το κάνουν αυτό για να αποκρύψουν κακόβουλη δραστηριότητα στον υπολογιστή. Όταν ένα rootkit αποκρύπτει *επιβλαβές λογισμικό*, δεν μπορείτε να ανακαλύψετε εύκολα την ύπαρξή του στον υπολογιστή σας.

Αυτό το προϊόν διαθέτει ένα πρόγραμμα σάρωσης για rootkit, το οποίο πραγματοποιεί σαρώσεις ειδικά για rootkit. Με αυτόν τον τρόπο δεν είναι δυνατή η εύκολη απόκρυψη του *επιβλαβούς λογισμικού*.

Λογισμικό Riskware

Το λογισμικό riskware δεν είναι ειδικά σχεδιασμένο για να βλάψει τον υπολογιστή σας, αλλά μπορεί να τον βλάψει αν χρησιμοποιηθεί με λανθασμένο τρόπο.

Το λογισμικό riskware δεν είναι αυστηρά επιβλαβές λογισμικό. Τα προγράμματα riskware εκτελούν κάποιες χρήσιμες αλλά πιθανώς επικίνδυνες λειτουργίες.

Παραδείγματα προγραμμάτων riskware είναι τα εξής:

- προγράμματα για άμεση αποστολή μηνυμάτων όπως το IRC (Internet relay chat),
- προγράμματα για μεταφορά αρχείων μέσω του Internet από έναν υπολογιστή σε άλλο,
- Προγράμματα τηλεφώνου μέσω Internet, όπως το VoIP (*Πρωτόκολλο Voice Over Internet*).
- Λογισμικό απομακρυσμένης πρόσβασης, όπως το VNC.
- Λογισμικό scareware, το οποίο μπορεί να προσπαθήσει να εκφοβίσει ή να εξαπατήσει άτομα προκειμένου να αγοράσουν ψεύτικο λογισμικό ασφαλείας.
- λογισμικό σχεδιασμένο για την παράκαμψη ελέγχων CD ή προστασίας αντιγραφής.

Εάν έχετε ξεκάθαρα εγκαταστήσει το πρόγραμμα και το έχετε ρυθμίσει σωστά, είναι λιγότερο πιθανό να είναι επιβλαβές.

Εάν η εγκατάσταση του λογισμικού riskware έγινε χωρίς να το γνωρίζετε, είναι πολύ πιθανό να έχει εγκατασταθεί με κακόβουλο σκοπό και πρέπει να το καταργήσετε.

4.2 Πώς μπορώ να σαρώσω τον υπολογιστή μου;

Όταν ενεργοποιηθεί η Προστασία από ιούς, σαρώνει αυτόματα τον υπολογιστή σας για επιβλαβή αρχεία. Μπορείτε επίσης να σαρώσετε αρχεία με μη αυτόματο τρόπο και να ρυθμίσετε προγραμματισμένες σαρώσεις.

Συνιστάται να διατηρείτε μονίμως ενεργοποιημένη την Προστασία από ιούς. Πραγματοποιείτε σάρωση των αρχείων σας μη αυτόματα όταν θέλετε να είστε σίγουροι ότι δεν υπάρχουν επιβλαβή αρχεία στον υπολογιστή σας ή εάν θέλετε να σαρώσετε αρχεία που έχετε εξαιρέσει από τη σάρωση σε πραγματικό χρόνο.

Ορίζοντας μια προγραμματισμένη σάρωση, η Προστασία από ιούς καταργεί τα επιβλαβή αρχεία από τον υπολογιστή σας τις καθορισμένες ώρες.

4.2.1 Αυτόματη σάρωση αρχείων

Η σάρωση σε πραγματικό χρόνο προστατεύει τον υπολογιστή σας σαρώνοντας όλα τα αρχεία όταν πραγματοποιείται πρόσβαση σε αυτά και αποκλείοντας την πρόσβαση στα αρχεία *επιβλαβούς λογισμικού*.

Όταν ο υπολογιστής προσπαθεί να αποκτήσει πρόσβαση σε ένα αρχείο, η Σάρωση σε πραγματικό χρόνο σαρώνει το αρχείο για λογισμικό κακόβουλης λειτουργίας για να επιτρέψει στον υπολογιστή την πρόσβαση στο αρχείο.

Εάν η Σάρωση σε πραγματικό χρόνο εντοπίσει κακόβουλο περιεχόμενο, θέτει το αρχείο σε καραντίνα πριν βλάψει τον υπολογιστή σας.

Η Σάρωση σε πραγματικό χρόνο επηρεάζει την απόδοση του υπολογιστή μου;

Κανονικά, δεν αντιλαμβάνεστε τη διαδικασία σάρωσης επειδή διαρκεί για μικρό χρονικό διάστημα και απαιτούνται λίγοι πόροι του συστήματος. Το σύνολο του χρόνου και των πόρων του συστήματος που είναι απαραίτητα για τη σάρωση σε πραγματικό χρόνο εξαρτάται, για παράδειγμα, από το περιεχόμενο, τη θέση και τον τύπο του αρχείου.

Αρχεία που χρειάζονται περισσότερο χρόνο για τη σάρωση:

- Αρχεία σε αφαιρούμενες μονάδες δίσκου, όπως CD, DVD και φορητές μονάδες USB.
- Συμπιεσμένα αρχεία όπως αρχεία *.zip*.

> **Σημείωση:** Τα συμπιεσμένα αρχεία δεν σαρώνονται από προεπιλογή.

Η Σάρωση σε πραγματικό χρόνο μπορεί να επιβραδύνει τον υπολογιστή στις παρακάτω περιπτώσεις:

- έχετε έναν υπολογιστή που δεν πληροί τις απαιτήσεις του συστήματος ή
- αποκτάτε πρόσβαση σε πολλά αρχεία ταυτόχρονα. Για παράδειγμα, όταν ανοίγετε έναν κατάλογο που περιέχει πολλά αρχεία που πρέπει να σαρωθούν.

Απενεργοποίηση ή ενεργοποίηση σάρωσης σε πραγματικό χρόνο

Διατηρήστε ενεργοποιημένη τη Σάρωση σε πραγματικό χρόνο για να διακόψετε τη λειτουργία του *κακόβουλου λογισμικού* πριν αυτό προκαλέσει βλάβη στον υπολογιστή

Για να ενεργοποιήσετε ή να απενεργοποιήσετε τη Σάρωση σε πραγματικό χρόνο:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   > **Σημείωση:** Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Ενεργοποιήστε ή απενεργοποιήστε την **Προστασία από ιούς**.
3. Κάντε κλικ στο κουμπί **OK**.

Αυτόματος χειρισμός επιβλαβών αρχείων

Η Σάρωση σε πραγματικό χρόνο μπορεί να χειρίζεται αυτόματα επιβλαβή αρχεία χωρίς να σας υποβάλλει ερωτήσεις.

Για να επιτρέψετε στη Σάρωση σε πραγματικό χρόνο να διαχειρίζεται αυτόματα τα επιβλαβή αρχεία:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   > **Σημείωση:** Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **Προστασία από ιούς**.
3. Επιλέξτε **Αυτόματη διαχείριση επιβλαβών αρχείων**.

Εάν επιλέξετε να μην γίνεται αυτόματη διαχείριση των επιβλαβών αρχείων, η Σάρωση σε πραγματικό χρόνο σας ρωτά τι θέλετε να γίνει με ένα επιβλαβές αρχείο κατά τον εντοπισμό του.

Χειρισμός λογισμικού κατασκοπίας

Η Προστασία από ιούς αποκλείει το λογισμικό κατασκοπίας αμέσως μόλις αυτό προσπαθήσει να ξεκινήσει.

Προτού ξεκινήσει μια εφαρμογή λογισμικού κατασκοπίας, το προϊόν την αποκλείει και σας αφήνει να αποφασίσετε τι θέλετε να γίνει.

Όταν εντοπίζεται λογισμικό κατασκοπίας, επιλέξτε μία από τις ακόλουθες ενέργειες:

Ενέργεια προς εκτέλεση	Τι συμβαίνει στο κατασκοπευτικό λογισμικό
Αυτόματη διαχείριση	Αφήστε το προϊόν να αποφασίσει ποια είναι η καλύτερη ενέργεια βάσει του λογισμικού κατασκοπίας που εντοπίστηκε.
Βάλτε το λογισμικό κατασκοπίας σε καραντίνα	Μετακινήστε το λογισμικό κατασκοπίας στην καραντίνα όπου δεν μπορεί να βλάψει τον υπολογιστή σας.
Διαγράψτε το λογισμικό κατασκοπίας	Καταργήστε όλα τα αρχεία που σχετίζονται με το λογισμικό κατασκοπίας από τον υπολογιστή σας.
Αποκλείστε μόνο το λογισμικό κατασκοπίας	Αποκλείστε την πρόσβαση στο λογισμικό κατασκοπίας αλλά αφήστε το στον υπολογιστή σας.
Εξαιρέστε το λογισμικό κατασκοπίας από τη σάρωση	Αφήστε το λογισμικό κατασκοπίας να εκτελείται και εξαιρέστε το από τη σάρωση στο μέλλον.

Χειρισμός λογισμικού riskware

Η Προστασία από ιούς αποκλείει το λογισμικό riskware αμέσως μόλις αυτό προσπαθήσει να ξεκινήσει.

Προτού ξεκινήσει μια εφαρμογή λογισμικού riskware, το προϊόν την αποκλείει και σας αφήνει να αποφασίσετε τι θέλετε να γίνει.

Επιλέξτε μία από τις παρακάτω ενέργειες όταν εντοπιστεί λογισμικό riskware:

Ενέργεια προς εκτέλεση	Τι συμβαίνει στο λογισμικό riskware
Αποκλείστε μόνο το λογισμικό riskware	Αποκλείστε την πρόσβαση στο λογισμικό riskware αλλά αφήστε το στον υπολογιστή σας.
Βάλτε το λογισμικό riskware σε καραντίνα	Μεταφέρετε το λογισμικό riskware στην καραντίνα όπου δεν θα μπορεί να βλάψει τον υπολογιστή σας.
Διαγράψτε το λογισμικό riskware	Καταργήστε όλα τα αρχεία του λογισμικού riskware από τον υπολογιστή σας.
Αποκλείστε το λογισμικό riskware από τη σάρωση	Αφήστε το λογισμικό riskware να εκτελείται και εξαιρέστε το από τη σάρωση στο μέλλον.

Αυτόματη κατάργηση cookies εντοπισμού

Καταργώντας τα cookies εντοπισμού, εμποδίζετε τις τοποθεσίες να έχουν τη δυνατότητα να εντοπίζουν τις τοποθεσίες που επισκέπτεστε στο Internet.

Τα cookies εντοπισμού είναι μικρά αρχεία που επιτρέπουν στις τοποθεσίες web να καταγράφουν τις τοποθεσίες web που επισκέπτεστε. Ακολουθήστε αυτές τις οδηγίες για να απομακρύνετε τα cookies εντοπισμού από τον υπολογιστή σας.

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **Προστασία από ιούς**.
3. Επιλέξτε **Κατάργηση cookies εντοπισμού**.
4. Κάντε κλικ στο κουμπί **OK**.

4.2.2 Σάρωση αρχείων με μη αυτόματο τρόπο

Μπορείτε να σαρώσετε τα αρχεία σας με μη αυτόματο τρόπο όταν, για παράδειγμα, συνδέετε μια εξωτερική συσκευή στον υπολογιστή σας, ώστε να βεβαιωθείτε ότι δεν περιέχουν λογισμικό κακόβουλης λειτουργίας.

Έναρξη της μη αυτόματης σάρωσης

Μπορείτε να πραγματοποιήσετε σάρωση σε ολόκληρο τον υπολογιστή ή για ένα συγκεκριμένο τύπο *επιβλαβούς λογισμικού* ή σε μια συγκεκριμένη θέση.

Αν έχετε υποψία για ένα συγκεκριμένο τύπο *επιβλαβούς λογισμικού*, μπορείτε να πραγματοποιήσετε σάρωση μόνο για αυτόν τον τύπο. Αν έχετε υποψία για μια συγκεκριμένη θέση στον υπολογιστή σας, μπορείτε να πραγματοποιήσετε σάρωση μόνο σε αυτό το τμήμα. Αυτές οι σαρώσεις θα ολοκληρωθούν πιο γρήγορα σε σχέση με μια σάρωση σε ολόκληρο τον υπολογιστή σας.

Για να ξεκινήσετε μη αυτόματη σάρωση του υπολογιστή:

Σημείωση: Εάν θέλετε μια γρήγορη σάρωση του συστήματος, κάντε κλικ στην επιλογή **Σάρωση** στη σελίδα "Κατάσταση".

1. Στη σελίδα "Εργαλεία", κάντε κλικ στο βέλος δίπλα από την επιλογή **Προηγμένη σάρωση**.
   Εμφανίζονται οι επιλογές σάρωσης.
2. Επιλέξτε τύπο σάρωσης.
   Επιλέξτε **Αλλαγή ρυθμίσεων σάρωσης** για να βελτιστοποιήσετε τον τρόπο με τον οποίο εκτελείται η σάρωση του υπολογιστή σας για ιούς και άλλες επιβλαβείς εφαρμογές από τη μη αυτόματη σάρωση.
3. Εάν επιλέξατε **Επιλογή αντικειμένου σάρωσης**, ανοίγει ένα παράθυρο στο οποίο μπορείτε να επιλέξετε τη θέση που θέλετε να σαρώσετε.
   Εμφανίζεται ο **Οδηγός σάρωσης**.

Τύποι σάρωσης

Μπορείτε να πραγματοποιήσετε σάρωση σε ολόκληρο τον υπολογιστή ή για ένα συγκεκριμένο τύπο επιβλαβούς λογισμικού ή σε μια συγκεκριμένη θέση.
Ακολουθούν οι διαφορετικοί τύποι σάρωσης:

Τύπος σάρωσης	Τι σαρώνεται	Πότε να χρησιμοποιήσετε αυτόν τον τύπο
Σάρωση για ιούς και κατασκοπευτικά προγράμματα	Μέρη του υπολογιστή σας για ιούς, κατασκοπευτικό λογισμικό και λογισμικό riskware	Αυτός ο τύπος σάρωσης είναι πολύ πιο γρήγορος από την πλήρη σάρωση. Πραγματοποιεί αναζήτηση μόνο στα μέρη του συστήματός σας που περιέχουν εγκατεστημένα αρχεία προγράμματος. Αυτός ο τύπος σάρωσης συνιστάται εάν θέλετε να ελέγξετε γρήγορα αν ο υπολογιστής σας είναι καθαρός, καθώς μπορεί να εντοπίσει και να καταργήσει αποτελεσματικά οποιοδήποτε ενεργό επιβλαβές λογισμικό υπάρχει στον υπολογιστή σας.
Πλήρης σάρωση υπολογιστή	Ολόκληρος ο υπολογιστής σας (εσωτερικές και εξωτερικές μονάδες σκληρού δίσκου) για ιούς, κατασκοπευτικό λογισμικό και λογισμικό riskware	Όταν θέλετε να βεβαιωθείτε ότι δεν υπάρχει επιβλαβές λογισμικό ή λογισμικό riskware στον υπολογιστή. Αυτός ο τύπος σάρωσης χρειάζεται περισσότερη ώρα για να ολοκληρωθεί. Συνδυάζει τη γρήγορη σάρωση για επιβλαβές λογισμικό και τη σάρωση μονάδας σκληρού δίσκου. Επίσης ελέγχει για στοιχεία που ενδεχομένως κρύβονται από λογισμικό rootkit.
Επιλογή αντικειμένου σάρωσης	Ένα συγκεκριμένο φάκελο ή μονάδα δίσκου για ιούς, κατασκοπευτικό λογισμικό και λογισμικό riskware	Όταν υποψιάζεστε ότι μια συγκεκριμένη θέση στον υπολογιστή σας μπορεί να περιέχει επιβλαβές λογισμικό, π.χ. η θέση περιέχει στοιχεία λήψης πιθανώς επικίνδυνης προέλευσης, όπως ομότιμα δίκτυα κοινής χρήσης αρχείων. Η διάρκεια της σάρωσης εξαρτάται από το μέγεθος του προορισμού που σαρώνετε. Η σάρωση

Τύπος σάρωσης	Τι σαρώνεται	Πότε να χρησιμοποιήσετε αυτόν τον τύπο
		ολοκληρώνεται γρήγορα εάν, για παράδειγμα, σαρώνετε έναν φάκελο που περιέχει μόνο μερικά μικρά αρχεία.

Σάρωση στην Εξερεύνηση των Windows

Στην Εξερεύνηση των Windows, μπορείτε να πραγματοποιήσετε σάρωση σε δίσκους, φακέλους και αρχεία για *ιούς*, *κατασκοπευτικά προγράμματα* και *λογισμικό riskware*.

Για να πραγματοποιήσετε σάρωση σε ένα δίσκο, φάκελο ή αρχείο:

1. Τοποθετήστε το δείκτη του ποντικιού στο δίσκο, το φάκελο ή το αρχείο που θέλετε να σαρώσετε και κάντε δεξί κλικ.
2. Από το μενού που εμφανίζεται όταν κάνετε δεξί κλικ, επιλέξτε **Σάρωση φακέλων για ιούς**. (Το όνομα της επιλογής αλλάζει ανάλογα με το αν εκτελείτε σάρωση σε δίσκο, φάκελο ή αρχείο.)
   Ανοίγει το παράθυρο **Οδηγός σάρωσης** και ξεκινά η σάρωση.

Εάν βρεθεί *ιός* ή *κατασκοπευτικό πρόγραμμα*, ο **Οδηγός σάρωσης** σάς καθοδηγεί στα στάδια καθαρισμού.

Επιλογή αρχείων για σάρωση

Μπορείτε να επιλέξετε τους τύπους αρχείων που θέλετε να σαρωθούν για *ιούς* και *κατασκοπευτικό λογισμικό* σε μη αυτόματες και προγραμματισμένες σαρώσεις.

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **Μη αυτόματη σάρωση**.
3. Στην περιοχή **Επιλογές σάρωσης**, επιλέξτε από τις παρακάτω ρυθμίσεις:

Σάρωση μόνο γνωστών τύπων αρχείων
Για σάρωση μόνο των τύπων αρχείων που είναι περισσότερο ευπαθή, όπως για παράδειγμα, τα εκτελέσιμα αρχεία. Η ενεργοποίηση αυτής της επιλογής επιταχύνει επίσης τη διαδικασία σάρωσης. Πραγματοποιείται σάρωση των αρχείων με τις εξής επεκτάσεις: `ani, asp, ax, bat, bin, boo, chm, cmd, com, cpl, dll, doc, dot, drv, eml, exe, hlp, hta, htm, html, htt, inf, ini, job, js, jse, lnk, lsp, mdb, mht, mpp, mpt, msg, ocx, pdf, php, pif, pot, ppt, rtf, scr, shs, swf, sys, td0, vbe, vbs, vxd, wbk, wma, wmv, wmf, wsc, wsf, wsh, wri, xls, xlt, xml, zip, jar, arj, lzh, tar, tgz, gz, cab, rar, bz2, hqx`.

Σάρωση στα περιεχόμενα συμπιεσμένων αρχείων
Για σάρωση αρχείων και φακέλων αρχειοθηκών.

Χρήση προηγμένης ευρετικής
Για να χρησιμοποιήσετε όλη τη διαθέσιμη ευρετική στη διάρκεια της σάρωσης για καλύτερη εύρεση νέου ή άγνωστου επιβλαβούς λογισμικού.

Σημείωση: Εάν ενεργοποιήσετε αυτή την επιλογή, η σάρωση διαρκεί περισσότερο και μπορεί να εμφανίσει περισσότερες ψευδείς προειδοποιήσεις (ακίνδυνα αρχεία που αναφέρονται ως ύποπτα).

4. Κάντε κλικ στο κουμπί **OK**.

Σημείωση: Δεν γίνεται σάρωση των αποκλεισμένων αρχείων στη λίστα αποκλεισμένων αρχείων ακόμη κι αν τα επιλέξετε για σάρωση εδώ.

Τι να κάνετε όταν εντοπίζονται επιβλαβή αρχεία

Επιλέξτε πώς θέλετε να χειρίζεστε τα επιβλαβή αρχεία όταν εντοπίζονται.

Για να επιλέξετε την ενέργεια που θα εκτελείται όταν εντοπίζεται επιβλαβές περιεχόμενο κατά τη διάρκεια της μη αυτόματης σάρωσης:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **Μη αυτόματη σάρωση**.
3. Στην ενότητα **Όταν εντοπιστεί ιός ή κατασκοπευτικό πρόγραμμα**, ενεργοποιήστε μία από τις παρακάτω επιλογές:

Επιλογή	Περιγραφή
Να γίνεται ερώτηση πάντα (προεπιλογή)	Μπορείτε να επιλέξετε την ενέργεια που θα εκτελείται για κάθε στοιχείο που εντοπίζεται κατά τη διάρκεια της μη αυτόματης σάρωσης.
Καθαρισμός των αρχείων	Το προϊόν προσπαθεί να καθαρίσει αυτόματα τα μολυσμένα αρχεία που εντοπίζονται κατά τη διάρκεια μη αυτόματης σάρωσης. **Σημείωση:** Εάν το προϊόν δεν μπορεί να καθαρίσει το μολυσμένο αρχείο, το αρχείο μπαίνει σε καραντίνα (εκτός κι αν βρίσκεται στο δίκτυο ή σε αφαιρούμενες μονάδες), για να μην προκαλέσει βλάβη στον υπολογιστή.
Μεταφορά των αρχείων σε καραντίνα	Το προϊόν μεταφέρει τα μολυσμένα αρχεία που εντοπίζονται κατά τη διάρκεια μιας μη αυτόματης σάρωσης στην καραντίνα, όπου δεν μπορούν να προκαλέσουν βλάβη στον υπολογιστή.
Αυτόματη διαγραφή	Το προϊόν διαγράφει τυχόν μολυσμένα αρχεία που εντοπίζονται κατά τη διάρκεια της μη αυτόματης σάρωσης.
Μόνο αναφορά	Το προϊόν αφήνει όπως είναι τυχόν επιβλαβή αρχεία που εντοπίζονται κατά τη διάρκεια της μη αυτόματης σάρωσης και καταγράφει τον εντοπισμό στην αναφορά σάρωσης. **Σημείωση:** Εάν η σάρωση σε πραγματικό χρόνο είναι απενεργοποιημένη, τυχόν κακόβουλο λογισμικό θα μπορεί και πάλι να βλάψει τον υπολογιστή εάν ενεργοποιήσετε αυτή την επιλογή.

Σημείωση: Όταν εντοπίζονται επιβλαβή αρχεία κατά τη διάρκεια προγραμματισμένης σάρωσης, καθαρίζονται αυτόματα.

Προγραμματισμός σάρωσης

Ρυθμίστε τον υπολογιστή σας να πραγματοποιεί σάρωση και να καταργεί ιούς και άλλες επιβλαβείς εφαρμογές αυτόματα όταν δεν τον χρησιμοποιείτε ή ορίστε την τακτική εκτέλεση της σάρωσης ώστε να διασφαλίσετε ότι ο υπολογιστής σας είναι καθαρός.

Για να προγραμματίσετε μια σάρωση:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **Προγραμματισμένη σάρωση**.
3. Ενεργοποιήστε την **Προγραμματισμένη σάρωση**.
4. Επιλέξτε πότε θα θέλατε να ξεκινήσει η σάρωση.

Επιλογή	Περιγραφή
Κάθε μέρα	Πραγματοποιείτε σάρωση του υπολογιστή σας κάθε μέρα.
Κάθε βδομάδα	Πραγματοποιείτε σάρωση του υπολογιστή σας σε επιλεγμένες ημέρες της εβδομάδας. Επιλέξτε τις ημέρες από τη λίστα.

Επιλογή	Περιγραφή
Κάθε μήνα	Πραγματοποιείτε σάρωση του υπολογιστή σας σε επιλεγμένες ημέρες του μήνα. Για να επιλέξετε τις ημέρες: **1.** Πραγματοποιήστε μια επιλογή από τη λίστα **Ημέρα**. **2.** Επιλέξτε την ημέρα του μήνα από τη λίστα δίπλα στην επιλεγμένη ημέρα.

5. Επιλέξτε πότε θέλετε να ξεκινήσει η σάρωση στις επιλεγμένες ημέρες.

Επιλογή	Περιγραφή
Ώρα έναρξης	Ξεκινήστε τη σάρωση την καθορισμένη ώρα.
Μετά από αδράνεια του υπολογιστή για	Ξεκινήστε τη σάρωση αφού δεν έχετε χρησιμοποιήσει τον υπολογιστή για το καθορισμένο χρονικό διάστημα.

Η Προγραμματισμένη σάρωση χρησιμοποιεί τις ρυθμίσεις της μη αυτόματης σάρωσης κατά τη σάρωση του υπολογιστή σας. Επιπλέον, εκτελεί σάρωση αρχειοθηκών κάθε φορά και αυτόματο καθαρισμό των επιβλαβών αρχείων.

Σημείωση: Οι προγραμματισμένες σαρώσεις διακόπτονται όταν ενεργοποιείται η *λειτουργία παιχνιδιών*. Όταν την απενεργοποιήσετε, η σάρωση που έχει ανασταλεί συνεχίζει αυτόματα.

4.2.3 Σάρωση ηλεκτρονικού ταχυδρομείου

Η Σάρωση ηλεκτρονικού ταχυδρομείου σας προστατεύει από τη λήψη επιβλαβών αρχείων σε μηνύματα ηλεκτρονικού ταχυδρομείου που λαμβάνετε.

Η Σάρωση για ιούς και κατασκοπευτικά προγράμματα θα πρέπει να είναι ενεργοποιημένη για να πραγματοποιηθεί σάρωση του ηλεκτρονικού ταχυδρομείου για ιούς.

Για ενεργοποίηση της σάρωσης ηλεκτρονικού ταχυδρομείου:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **Προστασία από ιούς**.
3. Επιλέξτε **Κατάργηση επιβλαβών συνημμένων ηλεκτρονικού ταχυδρομείου**.
4. Κάντε κλικ στο κουμπί **OK**.

Πότε σαρώνονται τα μηνύματα και τα συνημμένα του ηλεκτρονικού ταχυδρομείου;

Η Προστασία από ιούς μπορεί να καταργήσει επιβλαβές περιεχόμενο από email που λαμβάνετε.

Η Προστασία από ιούς καταργεί τα επιβλαβή μηνύματα email που λαμβάνονται από προγράμματα email, όπως είναι το Microsoft Outlook και το Outlook Express, το Microsoft Mail ή το Mozilla Thunderbird. Πραγματοποιεί σάρωση μη κρυπτογραφημένων μηνυμάτων email και συνημμένων κάθε φορά που το πρόγραμμα email που χρησιμοποιείτε τα λαμβάνει από διακομιστή αλληλογραφίας μέσω πρωτοκόλλου POP3.

Η Προστασία από ιούς δεν μπορεί να σαρώσει μηνύματα email σε webmail, τα οποία περιλαμβάνουν εφαρμογές email που εκτελούνται στο πρόγραμμα περιήγησης web, όπως το Hotmail, το Yahoo! mail ή το Gmail. Εξακολουθείτε να είστε προστατευμένοι από *ιούς* ακόμη κι αν δεν καταργήσετε επιβλαβή συνημμένα ή ακόμη κι αν χρησιμοποιείτε webmail. Όταν ανοίγετε συνημμένα email, η Σάρωση σε πραγματικό χρόνο καταργεί τυχόν επιβλαβή συνημμένα προτού προκαλέσουν βλάβη.

Σημείωση: Η Σάρωση σε πραγματικό χρόνο προστατεύει μόνο τον υπολογιστή σας αλλά όχι και τους φίλους σας. Η Σάρωση σε πραγματικό χρόνο δεν σαρώνει συνημμένα αρχεία εκτός κι αν ανοίξετε το συνημμένο. Αυτό σημαίνει ότι εάν χρησιμοποιείτε ηλεκτρονικό ταχυδρομείο μέσω web και προωθήσετε ένα μήνυμα πριν ανοίξετε το συνημμένο του, μπορεί να προωθήσετε ένα μολυσμένο μήνυμα ηλεκτρονικού ταχυδρομείου στους φίλους σας.

4.2.4 Προβολή των αποτελεσμάτων σάρωσης

Το Ιστορικό ιών και λογισμικού κατασκοπίας εμφανίζει όλα τα επιβλαβή αρχεία που εντόπισε το προϊόν.

Μερικές φορές, το προϊόν δεν μπορεί να εκτελέσει την ενέργεια που έχετε επιλέξει όταν εντοπιστεί κάποιο επιβλαβές στοιχείο. Για παράδειγμα, εάν επιλέξετε τον καθαρισμό αρχείων και κάποιο αρχείο δεν μπορεί να καθαριστεί, το προϊόν το μετακινεί στην καραντίνα. Μπορείτε να προβάλλετε τις πληροφορίες αυτές στο Ιστορικό ιών και λογισμικού κατασκοπίας.

Για να δείτε το ιστορικό:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **Προστασία από ιούς**.
3. Επιλέξτε **Προβολή ιστορικού κατάργησης**.

Το Ιστορικό ιών και λογισμικού κατασκοπίας εμφανίζει τις παρακάτω πληροφορίες:

- ημερομηνία και ώρα εντοπισμού του επιβλαβούς αρχείου,
- το όνομα του επιβλαβούς λογισμικού και η θέση του στον υπολογιστή σας και
- η ενέργεια που εκτελέστηκε.

4.3 Πώς να εξαιρέσετε αρχεία από τη σάρωση

Μερικές φορές μπορεί να θέλετε να εξαιρέσετε κάποια αρχεία ή εφαρμογές από τη σάρωση. Τα εξαιρούμενα αρχεία δεν σαρώνονται εκτός κι αν τα καταργήσετε από τη λίστα εξαιρούμενων στοιχείων.

Σημείωση: Οι λίστες αποκλεισμού είναι διαφορετικές για τη σάρωση σε πραγματικό χρόνο και τη μη αυτόματη σάρωση. Για παράδειγμα, εάν εξαιρέσετε ένα αρχείο από τη σάρωση σε πραγματικό χρόνο, σαρώνεται κατά τη μη αυτόματη σάρωση εκτός και αν το εξαιρέσετε και από αυτή τη διαδικασία.

4.3.1 Εξαίρεση τύπων αρχείων

Όταν εξαιρέσετε αρχεία βάσει του τύπου τους, δεν εκτελείται σάρωση για επιβλαβές περιεχόμενο στα αρχεία με τις καθορισμένες επεκτάσεις.

Για να προσθέσετε ή να καταργήσετε τύπο αρχείου που θέλετε να εξαιρέσετε:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε εάν θέλετε να εξαιρέσετε τον τύπο αρχείου από τη σάρωση σε πραγματικό χρόνο ή τη μη αυτόματη σάρωση:
   - Επιλέξτε **Προστασία από ιούς** για να εξαιρέσετε τον τύπο αρχείου από τη σάρωση σε πραγματικό χρόνο.
   - Επιλέξτε **Μη αυτόματη σάρωση** για να εξαιρέσετε τον τύπο αρχείου από τη μη αυτόματη σάρωση.
3. Επιλέξτε **Εξαίρεση αρχείων από τη σάρωση**.
4. Για να εξαιρέσετε έναν τύπο αρχείου:
   a) Επιλέξτε την καρτέλα **Τύποι αρχείων**.
   b) Επιλέξτε **Εξαίρεση αρχείων με τις εξής επεκτάσεις**.
   c) Πληκτρολογήστε μια επέκταση αρχείου που αποτελεί τον τύπο αρχείων που θέλετε να εξαιρέσετε, στο πεδίο δίπλα στο κουμπί **Προσθήκη**.

      Για να εντοπίσετε τα αρχεία που δεν έχουν επέκταση, πληκτρολογήστε '.'. Μπορείτε να χρησιμοποιήσετε τον χαρακτήρα μπαλαντέρ '?' για να απεικονίσετε έναν μεμονωμένο χαρακτήρα ή το '*' για να απεικονίσετε οποιονδήποτε αριθμό χαρακτήρων.

      Για παράδειγμα, για να εξαιρέσετε εκτελέσιμα αρχεία, πληκτρολογήστε `exe` στο πεδίο.

   d) Κάντε κλικ στην επιλογή **Προσθήκη**.

5. Επαναλάβετε το προηγούμενο βήμα για οποιαδήποτε άλλη επέκταση που θέλετε να εξαιρεθεί από τη σάρωση για ιούς.
6. Κάντε κλικ στο **OK** για να κλείσετε το παράθυρο διαλόγου **Εξαίρεση από τη σάρωση**.
7. Κάντε κλικ στο **OK** για να εφαρμόσετε τις νέες ρυθμίσεις.

Οι επιλεγμένοι τύποι αρχείων εξαιρούνται από τις μελλοντικές σαρώσεις.

4.3.2 Εξαίρεση αρχείων βάσει θέσης

Όταν εξαιρείτε αρχεία βάσει θέσης, δεν εκτελείται σάρωση για επιβλαβές περιεχόμενο στα αρχεία στις καθορισμένες μονάδες ή φακέλους.

Για να προσθέσετε ή να καταργήσετε θέσεις αρχείων που θέλετε να εξαιρέσετε:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε εάν θέλετε να εξαιρέσετε τη θέση από τη σάρωση σε πραγματικό χρόνο ή τη μη αυτόματη σάρωση:
   - Επιλέξτε **Προστασία από ιούς** για να εξαιρέσετε τη θέση από τη σάρωση σε πραγματικό χρόνο.
   - Επιλέξτε **Μη αυτόματη σάρωση** για να εξαιρέσετε τη θέση από τη μη αυτόματη σάρωση.
3. Επιλέξτε **Εξαίρεση αρχείων από τη σάρωση**.
4. Για να εξαιρέσετε ένα αρχείο, μονάδα δίσκου ή φάκελο:
   a) Επιλέξτε την καρτέλα **Αντικείμενα**.
   b) Επιλέξτε **Εξαιρούμενα αντικείμενα (αρχεία, φάκελοι, ...)**.
   c) Κάντε κλικ στην επιλογή **Προσθήκη**.
   d) Επιλέξτε το αρχείο, τη μονάδα δίσκου ή τον φάκελο που θέλετε να εξαιρέσετε από τη σάρωση για ιούς.

      Σημείωση: Κάποιες μονάδες δίσκου μπορεί να είναι αποσπώμενες, όπως οι μονάδες δίσκου CD, DVD ή δικτύου. Οι μονάδες δίσκου δικτύου και οι κενές αποσπώμενες μονάδες δίσκου δεν μπορούν να εξαιρεθούν.

   e) Κάντε κλικ στο κουμπί **OK**.
5. Επαναλάβετε το προηγούμενο βήμα για να εξαιρέσετε άλλα αρχεία, μονάδες δίσκου ή φακέλους από τη σάρωση για ιούς.
6. Κάντε κλικ στο **OK** για να κλείσετε τον διάλογο **Εξαίρεση από τη σάρωση**.
7. Κάντε κλικ στο **OK** για να ισχύσουν οι νέες ρυθμίσεις.

Τα επιλεγμένα αρχεία, μονάδες ή φάκελοι εξαιρούνται από τις μελλοντικές σαρώσεις.

4.3.3 Προβολή εξαιρούμενων εφαρμογών

Μπορείτε να προβάλλετε τις εφαρμογές που έχετε εξαιρέσει από τη σάρωση και να τις καταργήσετε από τη λίστα εξαιρούμενων στοιχείων εάν θέλετε να εκτελείται σάρωσή τους στο μέλλον.

Εάν η σάρωση σε πραγματικό χρόνο ή η μη αυτόματη σάρωση εντοπίζει μια εφαρμογή που συμπεριφέρεται σαν λογισμικό κατασκοπίας ή λογισμικό riskware αλλά γνωρίζετε ότι είναι ασφαλές, μπορείτε να το εξαιρέσετε από τη σάρωση ώστε να μην λαμβάνετε πλέον σχετικές ειδοποιήσεις από το προϊόν.

Σημείωση: Εάν η εφαρμογή συμπεριφέρεται σαν ιός ή άλλο κακόβουλο λογισμικό, δεν μπορεί να εξαιρεθεί.

Δεν μπορείτε να εξαιρέσετε άμεσα εφαρμογές. Οι νέες εφαρμογές εμφανίζονται στη λίστα αποκλεισμού μόνο εάν τις εξαιρέσετε κατά τη διάρκεια της σάρωσης.

Για να δείτε τις εφαρμογές που έχουν εξαιρεθεί από τη σάρωση:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε εάν θέλετε να προβάλλετε τις εφαρμογές που έχουν εξαιρεθεί από τη σάρωση σε πραγματικό χρόνο ή τη μη αυτόματη σάρωση:
   - Επιλέξτε **Προστασία από ιούς** για να προβάλλετε εφαρμογές που έχουν αποκλειστεί από τη σάρωση σε πραγματικό χρόνο.
   - Επιλέξτε **Μη αυτόματη σάρωση** για να προβάλλετε εφαρμογές που έχουν αποκλειστεί από τη μη αυτόματη σάρωση.
3. Επιλέξτε **Εξαίρεση αρχείων από τη σάρωση**.
4. Επιλέξτε την καρτέλα **Εφαρμογές**.

   Σημείωση: Μόνο οι εφαρμογές κατασκοπευτικού λογισμικού και λογισμικού riskware μπορούν να εξαιρεθούν, όχι οι ιοί.

5. Εάν θέλετε να εκτελέσετε ξανά σάρωση της εξαιρούμενης εφαρμογής:
   a) Επιλέξτε την εφαρμογή που θέλετε να συμπεριλάβετε στη σάρωση.
   b) Πατήστε **Αφαίρεση**.
6. Κάντε κλικ στο **OK** για να κλείσετε τον διάλογο **Εξαίρεση από τη σάρωση**.
7. Κάντε κλικ στο **OK** για έξοδο.

4.4 Πώς μπορώ να χρησιμοποιήσω την καραντίνα;

Η καραντίνα είναι ένας αποθηκευτικός χώρος για αρχεία που μπορεί να είναι επιβλαβή.

Τα αρχεία σε καραντίνα δεν είναι δυνατό να επεκταθούν ή να προκαλέσουν οποιαδήποτε βλάβη στον υπολογιστή σας.

Μπορείτε να θέσετε σε καραντίνα στοιχεία *επιβλαβούς λογισμικού*, *κατασκοπευτικού προγράμματος* και *λογισμικού riskware* για να είναι ακίνδυνα. Μπορείτε να επαναφέρετε εφαρμογές ή αρχεία από την καραντίνα, αν τα χρειαστείτε.

Αν δεν χρειάζεστε ένα στοιχείο που είναι σε καραντίνα, μπορείτε να το διαγράψετε. Με τη διαγραφή ενός στοιχείου που βρίσκεται σε καραντίνα, το στοιχείο διαγράφεται οριστικά από τον υπολογιστή.

- Γενικά, μπορείτε να διαγράψετε *επιβλαβές λογισμικό* που βρίσκεται σε καραντίνα.
- Στις περισσότερες περιπτώσεις, μπορείτε να διαγράψετε *κατασκοπευτικό πρόγραμμα* που βρίσκεται σε καραντίνα. Το *κατασκοπευτικό πρόγραμμα* που βρίσκεται σε καραντίνα μπορεί να αποτελεί τμήμα ενός εγκεκριμένου προγράμματος λογισμικού και με την κατάργησή του να διακόπτεται η σωστή λειτουργία του προγράμματος αυτού. Εάν θέλετε να διατηρήσετε το πρόγραμμα στον υπολογιστή σας, μπορείτε να επαναφέρετε το *κατασκοπευτικό πρόγραμμα* που βρίσκεται σε καραντίνα.
- Το *λογισμικό riskware* που βρίσκεται σε καραντίνα μπορεί να είναι ένα εγκεκριμένο πρόγραμμα. Εάν έχετε εγκαταστήσει και ρυθμίσει το πρόγραμμα μόνοι σας, μπορείτε να το επαναφέρετε από την καραντίνα. Εάν η εγκατάσταση του *λογισμικού riskware* έχει γίνει χωρίς να το γνωρίζετε, είναι πολύ πιθανό να έχει εγκατασταθεί με κακόβουλο σκοπό και πρέπει να το διαγράψετε.

4.4.1 Προβολή στοιχείων σε καραντίνα

Μπορείτε να προβάλετε περισσότερες πληροφορίες σχετικά με τα στοιχεία που βρίσκονται σε καραντίνα.

Για να δείτε αναλυτικές πληροφορίες σχετικά με τα στοιχεία σε καραντίνα:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **Προστασία από ιούς**.
3. Επιλέξτε **Προβολή καραντίνας**.
   Η σελίδα **Καραντίνα** εμφανίζει το συνολικό αριθμό των στοιχείων που είναι σε καραντίνα.
4. Για προβολή λεπτομερών πληροφοριών σχετικά με ένα επιλεγμένο στοιχείο σε καραντίνα, κάντε κλικ στο κουμπί **Λεπτομέρειες**.

5. Για προβολή περισσότερων πληροφοριών σχετικά με τον λόγο για τον οποίο ένα στοιχείο είναι σε καραντίνα, κάντε κλικ στο εικονίδιο δίπλα στο στοιχείο.

4.4.2 Επαναφορά στοιχείων από καραντίνα

Μπορείτε να επαναφέρετε απαραίτητα στοιχεία από καραντίνα.

Μπορείτε να επαναφέρετε εφαρμογές ή αρχεία από την καραντίνα, αν τα χρειάζεστε. Μην επαναφέρετε στοιχεία από την καραντίνα εκτός εάν είστε σίγουροι ότι τα στοιχεία δεν αποτελούν απειλή. Τα στοιχεία που επαναφέρετε επανέρχονται στην αρχική τους θέση στον υπολογιστή.

Επαναφορά στοιχείων από καραντίνα

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **Προστασία από ιούς**.
3. Επιλέξτε **Προβολή καραντίνας**.
4. Επιλέξτε τα στοιχεία σε καραντίνα που θέλετε να επαναφέρετε.
5. Πατήστε **Επαναφορά**.

Τι είναι το DeepGuard;

Θέματα:

Το DeepGuard παρακολουθεί τις εφαρμογές για να εντοπίσει πιθανές επιβλαβείς αλλαγές στο σύστημα.

Το DeepGuard φροντίζει να χρησιμοποιείτε μόνο ασφαλείς εφαρμογές. Η ασφάλεια μιας εφαρμογής επαληθεύεται από την υπηρεσία ασφαλούς νέφους. Εάν η ασφάλεια μιας εφαρμογής δεν μπορεί να επαληθευτεί, το DeepGuard ξεκινά να παρακολουθεί τη συμπεριφορά της εφαρμογής.

Το DeepGuard αποκλείει νέους ιούς τύπου *δούρειου ίππου* και *worm*, *προγράμματα εκμετάλλευσης ευπαθειών* και άλλες επιβλαβείς εφαρμογές που δεν έχουν ανακαλυφθεί και προσπαθούν να κάνουν αλλαγές στον υπολογιστή σας και αποτρέπει την πρόσβαση ύποπτων εφαρμογών στο Internet.

Στις πιθανώς επιβλαβείς αλλαγές του συστήματος που εντοπίζονται από το DeepGuard περιλαμβάνονται οι εξής:

- αλλαγές στις ρυθμίσεις του συστήματος (μητρώο των Windows),
- απόπειρες για απενεργοποίηση σημαντικών προγραμμάτων του συστήματος, π.χ. προγράμματα ασφάλειας όπως αυτό το προϊόν, και
- απόπειρες για επεξεργασία σημαντικών αρχείων του συστήματος.

5.1 Επιλέξτε τι παρακολουθεί το DeepGuard

Το DeepGuard παρακολουθεί σημαντικές ρυθμίσεις και αρχεία του συστήματος και τυχόν προσπάθειες απενεργοποίησης σημαντικών εφαρμογών, συμπεριλαμβανομένου του συγκεκριμένου προϊόντος ασφαλείας.

Για να επιλέξετε τι παρακολουθεί το DeepGuard:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **DeepGuard**.
3. Βεβαιωθείτε ότι το **DeepGuard** είναι ενεργοποιημένο.
4. Επιλέξτε τις ρυθμίσεις για το DeepGuard:

Να προειδοποιούμαι για ύποπτη συμπεριφορά	Διατηρείτε τη ρύθμιση αυτή ενεργοποιημένη για να λαμβάνετε ειδοποιήσεις σχετικά με ύποπτη συμπεριφορά εφαρμογών. Εάν την απενεργοποιήσετε, το DeepGuard σταματά να παρακολουθεί την ύποπτη συμπεριφορά, γεγονός που μειώνει το επίπεδο ασφαλείας.
Να ειδοποιούμαι σχετικά με προγράμματα εκμετάλλευσης ευπαθειών εφαρμογών	Διατηρείτε τη ρύθμιση αυτή ενεργοποιημένη για να λαμβάνετε ειδοποιήσεις σχετικά με πιθανές απόπειρες προγραμμάτων εκμετάλλευσης ευπαθειών. Εάν την απενεργοποιήσετε, επιβλαβείς σελίδες web και έγγραφα μπορεί να εκμεταλλευτούν τις εφαρμογές σας, γεγονός που μειώνει το επίπεδο ασφαλείας. Συνιστάται η απενεργοποίησή της.
Να ζητείται η άδειά μου για σύνδεση στο Internet	Διατηρείτε τη ρύθμιση αυτή ενεργοποιημένη εάν θέλετε το DeepGuard να σας ειδοποιεί όταν μια άγνωστη εφαρμογή δοκιμάζει να συνδεθεί στο Internet.
Χρήση λειτουργίας συμβατότητας (μειώνει το επίπεδο ασφάλειας).	Για μέγιστη προστασία, το DeepGuard τροποποιεί προσωρινά τα προγράμματα που εκτελούνται. Ορισμένα προγράμματα ελέγχουν ότι δεν έχουν καταστραφεί ή τροποποιηθεί και ενδέχεται να μην είναι συμβατά με αυτή τη λειτουργία. Για παράδειγμα, τα online παιχνίδια με αντικλεπτικά συστήματα ελέγχουν ότι δεν έχουν τροποποιηθεί με οποιονδήποτε τρόπο κατά την εκτέλεσή τους. Στις περιπτώσεις αυτές, μπορείτε να ενεργοποιήσετε τη λειτουργία συμβατότητας.

5. Κάντε κλικ στο κουμπί **OK**.

5.1.1 Επιτρέψτε τις εφαρμογές που έχουν αποκλειστεί από το DeepGuard

Μπορείτε να ελέγχετε ποιες εφαρμογές επιτρέπει και ποιες αποκλείει το DeepGuard.

Μερικές φορές το DeepGuard μπορεί να αποκλείσει την εκτέλεση μιας ασφαλούς εφαρμογής, ακόμη κι αν εσείς θέλετε να χρησιμοποιήσετε την εφαρμογή και γνωρίζετε ότι είναι ασφαλής. Αυτό συμβαίνει επειδή η εφαρμογή προσπαθεί να πραγματοποιήσει αλλαγές στο σύστημα που ενδέχεται να είναι επιβλαβείς. Ενδέχεται επίσης να έχετε ακούσια αποκλείσει την εφαρμογή όταν εμφανίστηκε ένα αναδυόμενο παράθυρο DeepGuard.

Για να επιτρέψετε την εφαρμογή που έχει αποκλειστεί από το DeepGuard:

1. Στη σελίδα "Κατάσταση", κάντε κλικ στην επιλογή **Ρυθμίσεις**.

   Σημείωση: Χρειάζεστε δικαιώματα διαχειριστή για να αλλάξετε τις ρυθμίσεις.

2. Επιλέξτε **DeepGuard**.
3. Επιλέξτε **Αλλαγή αδειών εφαρμογής**.
   Εμφανίζεται η λίστα **Παρακολουθούμενες εφαρμογές**.
4. Βρείτε την εφαρμογή που θέλετε να επιτρέψετε και κάντε κλικ στην επιλογή **Λεπτομέρειες**.

> **Σημείωση:** Μπορείτε να κάνετε κλικ στις κεφαλίδες της στήλης για να ταξινομήσετε τη λίστα. Για παράδειγμα, κάντε κλικ στη στήλη **Δικαίωμα** για να ταξινομήσετε τη λίστα σε ομάδες επιτρεπόμενων και αποκλεισμένων προγραμμάτων.

5. Επιλέξτε **Να επιτρέπεται**.
6. Κάντε κλικ στο κουμπί **OK**.
7. Κάντε κλικ στο κουμπί **Κλείσιμο**.

Το DeepGuard επιτρέπει στην εφαρμογή να πραγματοποιήσει ξανά αλλαγές στο σύστημα.

5.2 Τι να κάνετε σε περίπτωση προειδοποιήσεων ύποπτης συμπεριφοράς

Το DeepGuard αποκλείει τις εφαρμογές που παρακολουθεί όταν συμπεριφέρονται ύποπτα ή κάνουν απόπειρα σύνδεσης στο Internet.

Μπορείτε να αποφασίσετε εάν θέλετε να επιτρέψετε στην εφαρμογή να συνεχίσει ή όχι βάσει όσων συνέβησαν.

5.2.1 Το DeepGuard αποκλείει μια επιβλαβή εφαρμογή

Το DeepGuard σας ειδοποιεί όταν εντοπίσει και αποκλείσει μια επιβλαβή εφαρμογή.

Όταν ανοίγει η ειδοποίηση:

Επιλέξτε **Λεπτομέρειες** για να προβάλλετε περισσότερες πληροφορίες σχετικά με την εφαρμογή. Οι λεπτομέρειες σας δείχνουν:

- η θέση της εφαρμογής,
- η φήμη της εφαρμογής στο Νέφος ασφαλείας,
- πόσο συνηθισμένη είναι η εφαρμογή και
- το όνομα του επιβλαβούς λογισμικού που εντοπίστηκε.

Μπορείτε να υποβάλλετε ένα δείγμα της εφαρμογής για ανάλυση.

5.2.2 Το DeepGuard αποκλείει μια ύποπτη εφαρμογή

Όταν είναι ενεργοποιημένη η επιλογή **Να προειδοποιούμαι για ύποπτη συμπεριφορά** στις ρυθμίσεις του DeepGuard, το DeepGuard σας ειδοποιεί όταν εντοπίσει μια εφαρμογή που συμπεριφέρεται ύποπτα. Εάν εμπιστεύεστε την εφαρμογή, μπορείτε να της επιτρέψετε να συνεχίσει.

Για να αποφασίσετε τι θέλετε να κάνετε με την εφαρμογή που έχει αποκλειστεί από το DeepGuard:

1. Επιλέξτε **Λεπτομέρειες** για να προβάλλετε περισσότερες πληροφορίες σχετικά με την εφαρμογή. Στην ενότητα των λεπτομερειών εμφανίζεται:
   - η θέση της εφαρμογής,
   - η φήμη της εφαρμογής στο Νέφος ασφαλείας,
   - πόσο συνηθισμένη είναι η εφαρμογή και
   - το όνομα του επιβλαβούς λογισμικού.
2. Αποφασίστε εάν εμπιστεύεστε την εφαρμογή που έχει αποκλειστεί από το DeepGuard:
   - Επιλέξτε **Θεωρώ την εφαρμογή αξιόπιστη. Να συνεχιστεί.** εάν δεν θέλετε να αποκλείσετε την εφαρμογή.

     Η εφαρμογή είναι πιθανώς ασφαλής εάν:
     - Το DeepGuard απέκλεισε την εφαρμογή ως αποτέλεσμα κάποιας δικής σας ενέργειας,
     - αναγνωρίζετε την εφαρμογή, ή
     - λάβατε την εφαρμογή από αξιόπιστη πηγή.
   - Επιλέξτε **Δεν θεωρώ αξιόπιστη την εφαρμογή. Να αποκλειστεί.** εάν θέλετε να διατηρήσετε αποκλεισμένη την εφαρμογή.

     Η εφαρμογή δεν είναι πιθανώς ασφαλής εάν:

- η εφαρμογή δεν είναι συνηθισμένη,
- η φήμη της εφαρμογής είναι άγνωστη, ή
- δεν γνωρίζετε την εφαρμογή.

Μπορείτε να υποβάλλετε ένα δείγμα της ύποπτης εφαρμογής για ανάλυση.

5.2.3 Μια άγνωστη εφαρμογή δοκιμάζει να συνδεθεί στο Internet

Όταν είναι ενεργοποιημένη η επιλογή **Να ζητείται η άδειά μου για σύνδεση στο Internet** στις ρυθμίσεις DeepGuard, το DeepGuard σάς ειδοποιεί όταν μια άγνωστη εφαρμογή δοκιμάζει να συνδεθεί στο Internet. Εάν εμπιστεύεστε την εφαρμογή, μπορείτε να της επιτρέψετε να συνεχίσει.

Για να αποφασίσετε τι θέλετε να κάνετε με την εφαρμογή που έχει αποκλειστεί από το DeepGuard:

1. Επιλέξτε **Λεπτομέρειες** για να προβάλλετε περισσότερες πληροφορίες σχετικά με την εφαρμογή. Στην ενότητα των λεπτομερειών εμφανίζεται:
   - η θέση της εφαρμογής,
   - η φήμη της εφαρμογής στο Νέφος ασφαλείας,
   - πόσο συνηθισμένη είναι η εφαρμογή.
   - τι προσπάθησε να κάνει η εφαρμογή και
   - πού προσπάθησε να συνδεθεί η εφαρμογή.
2. Αποφασίστε εάν εμπιστεύεστε την εφαρμογή που έχει αποκλειστεί από το DeepGuard:
   - Επιλέξτε **Θεωρώ την εφαρμογή αξιόπιστη. Να συνεχιστεί.** εάν δεν θέλετε να αποκλείσετε την εφαρμογή.

     Η εφαρμογή είναι πιθανώς ασφαλής εάν:

     - Το DeepGuard απέκλεισε την εφαρμογή ως αποτέλεσμα κάποιας δικής σας ενέργειας,
     - αναγνωρίζετε την εφαρμογή, ή
     - λάβατε την εφαρμογή από αξιόπιστη πηγή.
   - Επιλέξτε **Δεν θεωρώ αξιόπιστη την εφαρμογή. Να αποκλειστεί μόνιμα.** εάν θέλετε να παραμείνει αποκλεισμένη η εφαρμογή.

     Η εφαρμογή δεν είναι πιθανώς ασφαλής εάν:

     - η εφαρμογή δεν είναι συνηθισμένη,
     - η φήμη της εφαρμογής είναι άγνωστη, ή
     - δεν γνωρίζετε την εφαρμογή.

Όταν είναι ενεργοποιημένη η *λειτουργία παιχνιδιών*, το DeepGuard επιτρέπει σε οποιαδήποτε άγνωστη εφαρμογή να συνδέεται στο Internet. Να θυμάστε ότι εξακολουθεί να αποκλείει όλες τις επιβλαβείς εφαρμογές που δοκιμάζουν να συνδεθούν στο Internet όταν είναι ενεργοποιημένη η *λειτουργία παιχνιδιών*.

Μπορείτε να υποβάλλετε ένα δείγμα της ύποπτης εφαρμογής για ανάλυση.

5.2.4 Το DeepGuard εντοπίζει πιθανό πρόγραμμα εκμετάλλευσης ευπαθειών

Όταν είναι ενεργοποιημένη η επιλογή **Να ειδοποιούμαι σχετικά με προγράμματα εκμετάλλευσης ευπαθειών εφαρμογών** στις ρυθμίσεις του DeepGuard, το DeepGuard ειδοποιεί εάν εντοπίσει ύποπτη συμπεριφορά από μια εφαρμογή αφού ανοίξετε μια επιβλαβή σελίδα web ή ένα έγγραφο.

Για να αποφασίσετε τι θέλετε να κάνετε με την εφαρμογή που έχει αποκλειστεί από το DeepGuard:

1. Επιλέξτε **Λεπτομέρειες** για να προβάλλετε περισσότερες πληροφορίες σχετικά με την εφαρμογή. Στην ενότητα των λεπτομερειών εμφανίζεται:
   - το όνομα του επιβλαβούς λογισμικού και
   - η προέλευση του προγράμματος εκμετάλλευσης ευπαθειών (μια επιβλαβής σελίδα web ή ένα έγγραφο), εάν είναι γνωστή.

2. Αποφασίστε εάν εμπιστεύεστε την εφαρμογή που έχει αποκλειστεί από το DeepGuard:
   - Επιλέξτε **Διατήρηση της εφαρμογής ανοικτής (ενδέχεται να θέσει σε κίνδυνο τη συσκευή σας)** εάν δεν θέλετε να κλείσει η εφαρμογή.

     Ενδέχεται να θέλετε να κρατήσετε ανοικτή την εφαρμογή εάν το κλείσιμο της εφαρμογής χωρίς αποθήκευση των δεδομένων σας δεν είναι αποδεκτό αυτή τη στιγμή.
   - Επιλέξτε **Κλείσιμο της εφαρμογής για αποτροπή του προγράμματος εκμετάλλευσης ευπαθειών** εάν θέλετε να κλείσετε την εφαρμογή και να βεβαιωθείτε ότι δεν θέτετε τη συσκευή σας σε κίνδυνο.

     Συνιστάται το κλείσιμο της εφαρμογής ώστε να μην θέσετε τη συσκευή σας σε κίνδυνο.

Μπορείτε να υποβάλλετε ένα δείγμα για ανάλυση εάν εντοπίστηκε η προέλευση του προγράμματος εκμετάλλευσης ευπαθειών.

5.3 Υποβολή ύποπτων εφαρμογών για ανάλυση

Μπορείτε να μας βοηθήσετε να βελτιώσουμε την προστασία υποβάλλοντας ύποπτες εφαρμογές για ανάλυση.

Όταν το DeepGuard αποκλείσει μια εφαρμογή, για παράδειγμα επειδή αποτελεί πιθανό κίνδυνο ασφαλείας για τον υπολογιστή σας ή η εφαρμογή δοκίμασε να εκτελέσει μια πιθανώς επιβλαβή ενέργεια, μπορείτε να στείλετε ένα δείγμα της εφαρμογής για λόγους διερεύνησης της ασφάλειας.

Αυτό μπορείτε να το κάνετε εάν γνωρίζετε ότι η εφαρμογή που αποκλείστηκε από το DeepGuard είναι ασφαλής ή εάν υποπτεύεστε ότι η εφαρμογή μπορεί να είναι επιβλαβής.

Για να υποβάλλετε ένα δείγμα για ανάλυση:

1. Όταν το DeepGuard αποκλείει μια εφαρμογή, επιλέξτε εάν θέλετε να αποκλείσετε την εφαρμογή ή να την αφήσετε να συνεχίσει.
2. Το DeepGuard μπορεί να ρωτήσει εάν θέλετε να υποβάλλετε την εφαρμογή για ανάλυση. Κάντε κλικ στο κουμπί **Υποβολή** για να υποβάλλετε το δείγμα.

   Σημείωση: Το DeepGuard δεν ζητάει πάντα την υποβολή δείγματος, για παράδειγμα όταν υπάρχουν ήδη πληροφορίες σχετικά με την αποκλεισμένη εφαρμογή.