Bitdefender®
TOTAL SECURITY

ΟΔΗΓΊΕΣ ΧΡΉΣΤΗ

iOS

Bitdefender Total Security
Οδηγίες χρήστη

Publication date 07/19/2020

Νομική σημείωση

Bitdefender

Πίνακας Περιεχομένων

Σχετικά με τον οδηγό

1. Σκοπός και κοινό στο οποίο απευθύνεται

Η συνδρομή σας του Bitdefender Total Security μπορεί να προστατεύσει έως και 10 διαφορετικά PC, Mac, iOS και Android smartphones και tablets. Η διαχείριση των προστατευόμενων συσκευών μπορεί να γίνει μέσω ενός Bitdefender λογαριασμού, η οποίος πρέπει να συνδέεται με μια ενεργή συνδρομή.

Αυτός ο οδηγός παρέχει βοήθεια για την εγκατάσταση και χρήση των προϊόντων που περιλαμβάνονται στο συνδρομή σας: Bitdefender Total Security (για Windows), Bitdefender Antivirus for Mac (για macOS), Bitdefender Mobile Security για Android συσκευές και Bitdefender Mobile Security for iOS.

Μπορείτε να μάθετε πώς να ρυθμίσετε το Bitdefender σε διαφορετικές συσκευές για να τις κρατήσει προστατευμένες από κάθε είδους απειλές.

2. Πώς να χρησιμοποιήσετε αυτό τον οδηγό

Αυτός ο οδηγός είναι οργανωμένος γύρω από τα τέσσερα προϊόντα που περιλαμβάνονται στο Bitdefender Total Security:

- “Total Security για PC” (p. 1)

  Μάθετε πώς μπορείτε να χρησιμοποιήσετε το προϊόν για υπολογιστές και φορητούς υπολογιστές που βασίζονται στα Windows.

- “Antivirus για Mac” (p. 226)

  Μάθετε πώς να χρησιμοποιείτε το προϊόν στον Mac σας.

- “Mobile Security για iOS” (p. 276)

  Μάθετε πώς μπορείτε να χρησιμοποιήσετε το προϊόν για τα iOS smartphones και tablets σας.

- “Mobile Security για Android” (p. 296)

  Μάθετε πώς μπορείτε να χρησιμοποιήσετε το προϊόν για τα Android smartphones και tablets σας.

- “Επικοινωνήστε μαζί μας” (p. 344)

  Μάθετε πού θα ψάξετε για βοήθεια αν κάτι αναπάντεχο προκύψει.

TOTAL SECURITY ΓΙΑ PC

1. ΕΓΚΑΤΆΣΤΑΣΗ

1.1. Προετοιμασία εγκατάστασης

Πριν από την εγκατάσταση του Bitdefender Total Security, παρακαλούμε να ολοκληρώσετε αυτά τα βήματα προετοιμασίας προκειμένου να υλοποιηθεί ομαλά η εγκατάσταση:

- Βεβαιωθείτε ότι η συσκευή στην οποία σκοπεύετε να εγκαταστήσετε το Bitdefender πληροί τις απαιτήσεις συστήματος. Εάν η συσκευή δεν πληροί όλες τις απαιτήσεις συστήματος, το Bitdefender δεν θα εγκατασταθεί ή, εάν εγκατασταθεί, δεν θα λειτουργήσει σωστά και θα προκαλέσει επιβράδυνση και αστάθεια του συστήματος. Για τον πλήρη κατάλογο απαιτήσεων συστήματος παρακαλούμε αναφερθείτε στο *"Απαιτήσεις συστήματος"* (p. 3).
- Συνδεθείτε στη συσκευή χρησιμοποιώντας λογαριασμό διαχειριστή.
- Αφαιρέστε οποιοδήποτε άλλο παρόμοιο λογισμικό από τη συσκευή. Εάν υπάρχει κάποιο ήδη εγκατεστημένο πρόγραμμα κατά την διάρκεια της Bitdefender εγκατάστασης, θα σας ζητηθεί να το απεγκαταστήσετε. Η παράλληλη λειτουργία δύο εφαρμογών ασφαλείας μπορεί να επηρεάσει την λειτουργία τους και να δημιουργήσει μείζονα προβλήματα στο σύστημα. Ο Windows Defender θα απενεργοποιηθεί κατά την διάρκεια της εγκατάστασης.
- Απενεργοποιήστε ή καταργήστε οποιοδήποτε πρόγραμμα τείχους προστασίας που ενδέχεται να εκτελείται στη συσκευή. Η παράλληλη λειτουργία δύο εφαρμογών ασφαλείας μπορεί να επηρεάσει την λειτουργία τους και να δημιουργήσει σημαντικά προβλήματα στο σύστημα. Το Windows Firewall θα απενεργοποιηθεί κατά την διάρκεια της εγκατάστασης.
- Συνιστάται η συσκευή σας να είναι συνδεδεμένη στο Διαδίκτυο κατά την εγκατάσταση, ακόμη και όταν γίνεται από CD / DVD. Εάν υπάρχουν νεώτερες εκδόσεις των αρχείων που βρίσκονται στο πακέτο εγκατάστασης, το Bitdefender θα τις μεταφορτώσει και εγκαταστήσει κατάλληλα.

1.2. Απαιτήσεις συστήματος

Μπορείτε να εγκαταστήσετε το Bitdefender Total Security μόνο σε συσκευές που εκτελούν τα ακόλουθα λειτουργικά συστήματα:

- Windows 7 με Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10

- 2.5 GB ελεύθερος χώρος στο σκληρό δίσκο (τουλάχιστον 800 MB στο δίσκο εκκίνησης του συστήματος)
- 2 GB μνήμης (RAM)

Σημαντικό
Η απόδοση του συστήματος μπορεί να επηρεαστεί σε συσκευές που διαθέτουν CPU παλαιάς γενιάς.

Σημείωση
Για να μάθετε το λειτουργικό σύστημα Windows που εκτελεί η συσκευή σας και πληροφορίες υλικού:

- Στα **Windows 7**, κάντε δεξί κλικ στο εικονίδιο **My Computer** στην επιφάνεια εργασίας, και επιλέξτε **Properties** από το μενού.
- Στην περίπτωση των **Windows 8**, από την οθόνη εκκίνησης των Windows, εντοπίστε το **Computer** (για παράδειγμα μπορείτε να αρχίσετε να πληκτρολογείτε "Computer" κατευθείαν στην οθόνη εκκίνησης των Windows) και κατόπιν να κάνετε δεξί κλικ στο εικονίδιο του. Στα **Windows 8.1**, εντοπίστε το **This PC**.

  Επιλέξτε **Ιδιότητες** στο κάτω μέρος του μενού επιλογών Ψάξτε στο **System** για να βρείτε πληροφορίες σχετικά με τον τύπο του συστήματός σας.
- Στα **Windows 10**, πληκτρολογήστε "**System**" στο πλαίσιο αναζήτησης από τη γραμμή εργασιών και κάντε κλικ στο εικονίδιο του. Ψάξτε στο **System** για να βρείτε πληροφορίες σχετικά με τον τύπο του συστήματός σας.

Απαιτήσεις λογισμικού

Για να μπορείτε να χρησιμοποιήσετε το Bitdefender και όλες τις δυνατότητές του, η συσκευή σας πρέπει να πληροί τις ακόλουθες απαιτήσεις λογισμικού:

- Microsoft Edge 40 και άνω
- Internet Explorer 10 και μεταγενέστερος
- Mozilla Firefox 51 ή μεταγενέστερος
- Google Chrome 34 ή μεταγενέστερο
- Microsoft Outlook εκδόσεις 2007, 2010, 2013 / 2016
- Mozilla Thunderbird 14 ή μεταγενέστερο

1.3. Εγκατάσταση του Bitdefender προιόντος σας

Μπορείτε να εγκαταστήσετε το Bitdefender από το δίσκο εγκατάστασης ή χρησιμοποιώντας το πρόγραμμα εγκατάστασης ιστού που έχετε λάβει στη συσκευή σας από το Bitdefender Central.

Εάν η αγορά σας καλύπτει περισσότερες από μία συσκευές, επαναλάβετε τη διαδικασία εγκατάστασης και ενεργοποιήστε το προϊόν σας με τον ίδιο λογαριασμό σε κάθε συσκευή. Ο λογαριασμός που πρέπει να χρησιμοποιήσετε είναι αυτός που περιέχει την ενεργή Bitdefender συνδρομή σας.

1.3.1. Εγκατάσταση από το Bitdefender Central

Από το Bitdefender Central μπορείτε να κατεβάσετε το κιτ εγκατάστασης που αντιστοιχεί στην συνδρομή που αγοράστηκε. Μόλις η διαδικασία εγκατάστασης ολοκληρωθεί, ενεργοποιείται το Bitdefender Total Security.

Για να κατεβάσετε το Bitdefender Total Security απο το Bitdefender Central:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το **Οι συσκευές μου** και στην συνέχεια κάντε κλικ **ΕΓΚΑΤΑΣΤΑΣΗ ΠΡΟΣΤΑΣΙΑΣ** .
3. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:
   - **Προστατέψτε αυτή τη συσκευή**
     a. Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.
     b. Αποθηκεύστε το αρχείο εγκατάστασης.
   - **Προστασία άλλων συσκευών**

a. Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.

b. Επιλέξτε **ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΛΗΨΗΣ**.

c. Πληκτρολογήστε μια διεύθυνση ηλεκτρονικού ταχυδρομείου στο αντίστοιχο πεδίο και κάντε κλικ στην επιλογή **ΑΠΟΣΤΟΛΗ EMAIL** .

   Λάβετε υπόψη ότι ο παραγόμενος σύνδεσμος λήψης ισχύει μόνο για τις επόμενες 24 ώρες. Εάν λήξει ο σύνδεσμος, θα πρέπει να δημιουργήσετε ένα νέο, ακολουθώντας τα ίδια βήματα.

d. Στην συσκευή που θέλετε να εγκαταστήσετε το Bitdefender προιόν, ελέγξτε το λογαριασμό ηλεκτρονικού ταχυδρομείου που πληκτρολογήσατε και στην συνέχεια κάντε κλικ στο αντίστοιχο κουμπί λήψης.

4. Περιμένετε να ολοκληρωθεί η λήψη, στη συνέχεια, εκτελέστε το πρόγραμμα εγκατάστασης.

Επικύρωση εγκατάστασης.

Το Bitdefender αρχικά ελέγχει το σύστημα σας για να επικυρώσει την εγκατάσταση.

Εάν το σύστημα σας δεν πληροί τις ελάχιστες απαιτήσεις εγκατάστασης του προιόντος Bitdefender, θα ενημερωθείτε για τα σημεία εκείνα που χρήζουν βελτίωσης πριν προχωρήσετε.

Εαν εντοπιστεί κάποιο ασύμβατο πρόγραμμα ασφαλείας ή κάποια παλιότερη έκδοση του Bitdefender, θα ερωτηθείτε για την αφαίρεσή του από το σύστημα σας. Παρακαλούμε ακολουθείστε τις οδηγίες για την απομακρυνση του λογισμικού από το σύστημα σας προκειμένου να αποφύγετε προβλήματα που θα εμφανιστούν αργότερα. Ίσως χρειαστεί να επανεκκινήσετε τη συσκευή σας για να ολοκληρώσετε την κατάργηση των εντοπισμένων λύσεων ασφαλείας.

Το πακέτο εγκατάστασης του Bitdefender Total Security επικαιροποιείται διαρκώς

Σημείωση

Η μεταφόρτωση των αρχείων εγκατάστασης μπορεί να διαρκέσει πολύ ώρα, ειδικά αν η σύνδεση στο Διαδίκτυο είναι αργή.

Αφού επικυρωθεί η εγκατάσταση, θα εμφανιστεί ο βοηθός εγκατάστασης. Ακολουθείστε τα βήματα για να εγκαταστήσετε το Bitdefender Total Security.

Βήμα 1 - Εγκατάσταση Bitdefender

Πριν προχωρήσετε στην εγκατάσταση, πρέπει να συμφωνήσετε με τη Συμφωνία Συνδρομής. Αφιερώστε λίγο χρόνο για να διαβάσετε τη Συμφωνία Συνδρομής επειδή περιέχει τους όρους και τις προϋποθέσεις κάτω από τις οποίες μπορείτε να χρησιμοποιήσετε το Bitdefender Total Security.

Εάν δεν συμφωνείτε με τους όρους αυτούς, κλείστε το παράθυρο αυτό. Η διαδικασία εγκατάστασης θα διακοπεί και η εγκατάσταση θα τερματιστεί.

Δύο επιπρόσθετες εργασίες μπορούν να υλοποιηθούν στο βήμα αυτό:

- Κρατήστε την επιλογή **Αποστολή αναφορών προϊόντος** ενεργοποιημένη. Επιτρέποντας την επιλογή αυτή, οι αναφορές περιέχουν πληροφορίες σχετικά με το πώς χρησιμοποιείτε αυτό το προϊόν αποστέλλεται στους Bitdefender servers. Οι πληροφορίες αυτές είναι απαραίτητες για την βελτίωση του προιόντος και θα βοηθήσουν να έχετε καλυτερη εμπειρία χρήσης στο μέλλον. Σημειώστε ότι οι αναφορές αυτές δεν περιέχουν εμπιστευτικά δεδομένα, όπως όνομα ή διεύθυνση IP και δεν πρόκειται να χρησιμοποιηθούν για εμπορικούς σκοπούς.
- Επιλέξτε τη γλώσσα που θέλετε να εγκαταστήσετε στο προϊόν σας.

Κάντε κλικ στο κουμπί **ΕΓΚΑΤΑΣΤΑΣΗ** για να ξεκινήσετε τη διαδικασία εγκατάστασης του προϊόντος Bitdefender.

Βήμα 2 - Εγκατάσταση σε εξέλιξη

Παρακαλούμε περιμένετε για την ολοκλήρωση της εγκατάστασης. Εμφανίζονται λεπτομερείς πληροφορίες για την πρόοδο της εγκατάστασης

Βήμα 3 - Η εγκατάσταση ολοκληρώθηκε

Το Bitdefender προϊόν σας έχει εγκατασταθεί με επιτυχία.

Εμφανίζεται σύνοψη της εγκατάστασης. Στην περίπτωση που κάποια ενεργά κακόβουλα προγράμματα (malware) εντοπίζονται και αφαιρούνται κατά την διάρκεια της εγκατάστασης, το σύστημα ίσως χρειαστεί επανεκκίνηση.

Βήμα 4 - Ανάλυση συσκευών

Θα ερωτηθείτε τώρα εάν θέλετε να πραγματοποιήσετε ανάλυση της συσκευής σας, για να βεβαιωθείτε ότι είναι ασφαλής. Κατά τη διάρκεια αυτού του βήματος, το Bitdefender θα σαρώσει κρίσιμες περιοχές συστήματος. Κάντε κλικ στο **Έναρξη ανάλυσης συσκευής** για να την ξεκινήσετε.

Μπορείτε να αποκρύψετε τη διεπαφή σάρωσης κάνοντας κλικ στο **Εκτέλεση σάρωσης στο παρασκήνιο** . Μετά από αυτό, επιλέξτε αν θέλετε να ενημερωθείτε όταν ολοκληρωθεί η σάρωση ή όχι.

Όταν ολοκληρωθεί η σάρωση, κάντε κλικ στο **Άνοιγμα διεπαφής Bitdefender** .

Σημείωση

Εναλλακτικά, εάν δεν θέλετε να εκτελέσετε τη σάρωση, μπορείτε απλώς να κάνετε κλικ στο **Παράλειψη** .

Βήμα 5 - Έναρξη

Στο παράθυρο **Έναρξη** μπορείτε να δείτε λεπτομέρειες για την ενεργή συνδρομή σας.

Κάντε κλικ στο **ΤΕΛΟΣ** για να αποκτήσετε πρόσβαση στο Bitdefender Total Security.

1.3.2. Εγκατάσταση από το δίσκο εγκατάστασης

Για να ξεκινήσει η εγκατάσταση του Bitdefender από τον δίσκο εγκατάστασης, εισάγετε τον δίσκο στον οπτικό αναγνώστη (optical drive).

Η οθόνη εγκατάστασης θα εμφανιστεί σε σύντομο χρονικό διάστημα. Ακολουθείστε τις οδηγίες στην οθόνη για την έναρξη της εγκατάστασης.

Στην περίπτωση που η οθόνη εγκατάστασης δεν εμφανιστεί, χρησιμοποιείστε τον Windows Explorer για να πλοηγηθείτε στον αρχικό φάκελο του δίσκου και κάντε διπλό κλικ στο αρχείο autorun.exe.

Αν η ταχύτητα σας στο Internet είναι αργή, ή το σύστημά σας δεν είναι συνδεδεμένο στο Internet, κάντε κλικ στο **Install from CD/DVD** κουμπί. Στην περίπτωση αυτή, το Bitdefender προϊόν διαθέσιμο στο δίσκο θα εγκατασταθεί και μια νεότερη έκδοση θα κατέβει από τους Bitdefender servers μέσω της ενημέρωσης προϊόντος.

Επικύρωση εγκατάστασης.

Το Bitdefender αρχικά ελέγχει το σύστημα σας για να επικυρώσει την εγκατάσταση.

Εάν το σύστημα σας δεν πληροί τις ελάχιστες απαιτήσεις εγκατάστασης του προιόντος Bitdefender, θα ενημερωθείτε για τα σημεία εκείνα που χρήζουν βελτίωσης πριν προχωρήσετε.

Εαν εντοπιστεί κάποιο ασύμβατο πρόγραμμα ασφαλείας ή κάποια παλιότερη έκδοση του Bitdefender, θα ερωτηθείτε για την αφαίρεσή του από το σύστημα σας. Παρακαλούμε ακολουθείστε τις οδηγίες για την απομακρυνση του λογισμικού από το σύστημα σας προκειμένου να αποφύγετε προβλήματα που θα εμφανιστούν αργότερα. Ίσως χρειαστεί να επανεκκινήσετε τη συσκευή σας για να ολοκληρώσετε την κατάργηση των εντοπισμένων λύσεων ασφαλείας.

Σημείωση

Η μεταφόρτωση των αρχείων εγκατάστασης μπορεί να διαρκέσει πολύ ώρα, ειδικά αν η σύνδεση στο Διαδίκτυο είναι αργή.

Αφού επικυρωθεί η εγκατάσταση, θα εμφανιστεί ο βοηθός εγκατάστασης. Ακολουθείστε τα βήματα για να εγκαταστήσετε το Bitdefender Total Security.

Βήμα 1 - Εγκατάσταση Bitdefender

Πριν προχωρήσετε στην εγκατάσταση, πρέπει να συμφωνήσετε με τη Συμφωνία Συνδρομής. Αφιερώστε λίγο χρόνο για να διαβάσετε τη Συμφωνία Συνδρομής επειδή περιέχει τους όρους και τις προϋποθέσεις κάτω από τις οποίες μπορείτε να χρησιμοποιήσετε το Bitdefender Total Security.

Εάν δεν συμφωνείτε με τους όρους αυτούς, κλείστε το παράθυρο αυτό. Η διαδικασία εγκατάστασης θα διακοπεί και η εγκατάσταση θα τερματιστεί.

Δύο επιπρόσθετες εργασίες μπορούν να υλοποιηθούν στο βήμα αυτό:

- Κρατήστε την επιλογή **Αποστολή αναφορών προϊόντος** ενεργοποιημένη. Επιτρέποντας την επιλογή αυτή, οι αναφορές περιέχουν πληροφορίες σχετικά με το πώς χρησιμοποιείτε αυτό το προϊόν αποστέλλεται στους Bitdefender servers. Οι πληροφορίες αυτές είναι απαραίτητες για την βελτίωση του προιόντος και θα βοηθήσουν να έχετε καλυτερη εμπειρία χρήσης στο μέλλον. Σημειώστε ότι οι αναφορές αυτές δεν περιέχουν

εμπιστευτικά δεδομένα, όπως όνομα ή διεύθυνση IP και δεν πρόκειται να χρησιμοποιηθούν για εμπορικούς σκοπούς.

- Επιλέξτε τη γλώσσα που θέλετε να εγκαταστήσετε στο προϊόν σας.

Κάντε κλικ στο κουμπί **ΕΓΚΑΤΑΣΤΑΣΗ** για να ξεκινήσετε τη διαδικασία εγκατάστασης του προϊόντος Bitdefender.

Βήμα 2 - Εγκατάσταση σε εξέλιξη

Παρακαλούμε περιμένετε για την ολοκλήρωση της εγκατάστασης. Εμφανίζονται λεπτομερείς πληροφορίες για την πρόοδο της εγκατάστασης

Βήμα 3 - Η εγκατάσταση ολοκληρώθηκε

Εμφανίζεται σύνοψη της εγκατάστασης. Στην περίπτωση που κάποια ενεργά κακόβουλα προγράμματα (malware) εντοπίζονται και αφαιρούνται κατά την διάρκεια της εγκατάστασης, το σύστημα ίσως χρειαστεί επανεκκίνηση.

Βήμα 4 - Ανάλυση συσκευών

Θα ερωτηθείτε τώρα εάν θέλετε να πραγματοποιήσετε ανάλυση της συσκευής σας, για να βεβαιωθείτε ότι είναι ασφαλής. Κατά τη διάρκεια αυτού του βήματος, το Bitdefender θα σαρώσει κρίσιμες περιοχές συστήματος. Κάντε κλικ στο **Έναρξη ανάλυσης συσκευής** για να την ξεκινήσετε.

Μπορείτε να αποκρύψετε τη διεπαφή σάρωσης κάνοντας κλικ στο **Εκτέλεση σάρωσης στο παρασκήνιο** . Μετά από αυτό, επιλέξτε αν θέλετε να ενημερωθείτε όταν ολοκληρωθεί η σάρωση ή όχι.

Όταν ολοκληρωθεί η σάρωση, κάντε κλικ στο **Συνέχεια με τη δημιουργία λογαριασμού** .

Σημείωση

Εναλλακτικά, εάν δεν θέλετε να εκτελέσετε τη σάρωση, μπορείτε απλώς να κάνετε κλικ στο **Παράλειψη** .

Βήμα 5 - Bitdefender λογαριασμός

Όταν ολοκληρώσετε την αρχική ρύθμιση, θα εμφανιστεί το παράθυρο του Bitdefender λογαριασμού. Ένας Bitdefender λογαριασμός απαιτείται προκειμένου να ενεργοποιήσετε το προϊόν και να χρησιμοποιήσετε τις

online δυνατότητές του. Για περισσότερες πληροφορίες, ανατρέξτε στην "*Bitdefender Central*" (p. 32).

Συνεχίστε ανάλογα την περίπτωσή σας

- **Θέλω να δημιουργήσω ένα λογαριασμό Bitdefender**

1. Πληκτρολογήστε τις απαιτούμενες πληροφορίες στα αντίστοιχα πεδία. Τα δεδομένα που εισαγάγατε εδώ παραμένουν εμπιστευτικά. Ο κωδικός πρόσβασης πρέπει να έχει μήκος τουλάχιστον 8 χαρακτήρων, να περιέχει τουλάχιστον έναν αριθμό ή σύμβολο και να περιλαμβάνει χαρακτήρες με μικρά ή κεφαλαία γράμματα.
2. Πριν προχωρήσετε περαιτέρω, πρέπει να συμφωνήσετε με τους Όρους Χρήσης. Αποκτήστε πρόσβαση στους Όρους Χρήσης και διαβάστε προσεκτικά, καθώς περιέχουν τους όρους και τις προϋποθέσεις υπό τις οποίες μπορείτε να χρησιμοποιήσετε Bitdefender.

   Επιπλέον, μπορείτε να έχετε πρόσβαση και να διαβάσετε την Πολιτική Απορρήτου.
3. Πατήστε στο **ΔΗΜΙΟΥΡΓΙΑ ΛΟΓΑΡΙΑΣΜΟΥ**.

Σημείωση

Μόλις δημιουργηθεί ο λογαριασμός, μπορείτε να χρησιμοποιήσετε το email και τον κωδικό πρόσβασης που δώσατε για να συνδεθείτε στο λογαριασμό σας στο https://central.bitdefender.com, ή στην εφαρμογή Bitdefender Central app, με την προϋπόθεση ότι είναι εγκατεστημένη σε μια από τις Android ή iOS συσκευές σας. Για να εγκαταστήσετε την εφαρμογή Bitdefender Central app στο Android, πρέπει να έχετε πρόσβαση στο Google Play, να πραγματοποιήσετε αναζήτηση σαν Bitdefender Central, και, στη συνέχεια, να επιλέξετε την αντίστοιχη επιλογή εγκατάστασης. Για να εγκαταστήσετε την εφαρμογή Bitdefender Central app στο iOS, πρέπει να έχετε πρόσβαση στο App Store, να πραγματοποιήσετε αναζήτηση σανBitdefender Central, και, στη συνέχεια, να επιλέξετε την αντίστοιχη επιλογή εγκατάστασης.

- **Έχω ήδη ένα λογαριασμό Bitdefender.**

1. Κάντε κλικ στην επιλογή **Σύνδεση** .
2. Πληκτρολογήστε την e-mail διεύθυνσή στο αντίστοιχο πεδίο και στη συνέχεια κάντε κλικ στο **ΕΠΟΜΕΝΟ**.

3. Εισάγετε τον κωδικό πρόσβασης και στη συνέχεια κάντε κλικ στο **ΣΥΝΔΕΣΗ**.

   Αν ξεχάσατε τον κωδικό πρόσβασης για το λογαριασμό σας ή απλά θέλετε να επαναφέρετε αυτόν που έχετε ήδη ορίσει:

   a. Κάντε κλικ στο κουμπί **Ξεχάσατε τον κωδικό;**.

   b. Εισάγετε τη διεύθυνση e-mail σας, και επιλέξτε **ΕΠΟΜΕΝΟ**.

   c. Ελέγξτε τον email λογαριασμό, πληκτρολογήστε τον κωδικό ασφαλείας που λάβατε και στη συνέχεια κάντε κλικ στο κουμπί **ΕΠΟΜΕΝΟ**.

      Εναλλακτικά, μπορείτε να κάνετε κλικ στο **Αλλαγή κωδικού πρόσβασης** στο email που σας στείλαμε.

   d. Πληκτρολογήστε τον νέο κωδικό πρόσβασης που θέλετε να ορίσετε και στη συνέχεια πληκτρολογήστε τον ξανά. Κάντε κλικ στο **SAVE**.

Σημείωση
Αν έχετε ήδη ένα λογαριασμό MyBitdefender, μπορείτε να το χρησιμοποιήσετε για να συνδεθείτε στο Bitdefender λογαρισμό. Εάν έχετε ξεχάσει τον κωδικό πρόσβασής σας, θα πρέπει πρώτα να πάτε στο https://my.bitdefender.com για να τον επαναφέρετε. Στη συνέχεια, χρησιμοποιήστε τα ενημερωμένα διαπιστευτήρια για να συνδεθείτε στο Bitdefender λογαρισμό.

- **Θέλω να συνδεθώ χρησιμοποιώντας το λογαριασμό μου Microsoft, Facebook ή Google.**

Για να συνδεθείτε μέσω του λογαριασμού Microsoft, Facebook ή Google:

1. Επιλέξτε την υπηρεσία που θέλετε να χρησιμοποιήσετε Θα μεταφερθείτε στην σελίδα σύνδεσης της υπηρεσίας που επιλέξατε
2. Ακολουθείστε τις οδηγίες που παρέχει η επιλεγείσα υπηρεσία για να συνδέσετε το λογαριασμό σας με το Bitdefender.

Σημείωση
Το Bitdefender δεν πρόκειται να αποκτήσει πρόσβαση σε οποιαδήποτε εμπιστευτική πληροφορία όπως τον κωδικό πρόσβασης του λογαριασμού που χρησιμοποιείτε για την σύνδεση ή τις προσωπικές πληροφορίες των φίλων σας και των επαφών σας.

Βήμα 6 - Ενεργοποιήστε το προϊόν σας!

Σημείωση
Αυτό το βήμα εμφανίζεται αν έχετε επιλέξει να δημιουργήσετε ένα νέο Bitdefender λογαριασμό κατά τη διάρκεια του προηγούμενου βήματος, ή αν είστε συνδεδεμένοι χρησιμοποιώντας ένα λογαριασμό με συνδρομή που έχει λήξει.

Για την ολοκλήρωση της ενεργοποίησης του προϊόντος σας απαιτείται ενεργή σύνδεση στο Internet.

Συνεχίστε ανάλογα την περίπτωσή σας

- Εχω έναν κωδικό ενεργοποίησης

  Σε αυτή την περίπτωση, ενεργοποιήστε το προϊόν σας ακολουθώντας αυτά τα βήματα:

  1. Πληκτρολογήστε τον κωδικό ενεργοποίησης στο πεδίο **Εχω έναν κωδικό ενεργοποίησης** και, στη συνέχεια, κάντε κλικ στο κουμπί **ΣΥΝΕΧΕΙΑ**.

     Σημείωση
     Για να βρείτε τον κωδικό ενεργοποίησης:
     - στην ετικέτα του CD/DVD
     - σχετικά με την κάρτα εγγραφής προϊόντος.
     - στο ηλεκτρονικό μήνυμα αγοράς από το Διαδίκτυο (online purchase e-mail.)

  2. **Θέλω να αξιολογήσω το Bitdefender.**

     Σε αυτή την περίπτωση μπορείτε να χρησιμοποιήσετε το προιόν για 30 ημέρες Για να ξεκινήσετε τη δοκιμαστική περίοδο, επιλέξτε **Δεν έχω συνδρομή, θα ήθελα να δοκιμάσω το προϊόν δωρεάν**, και στη συνέχεια κάντε κλικ στο κουμπί **ΣΥΝΕΧΕΙΑ**.

Βήμα 7 - Έναρξη

Στο παράθυρο **Έναρξη** μπορείτε να δείτε λεπτομέρειες για την ενεργή συνδρομή σας.

Κάντε κλικ στο **ΤΕΛΟΣ** για να αποκτήσετε πρόσβαση στο Bitdefender Total Security.

2. ΞΕΚΙΝΏΝΤΑΣ

2.1. Τα βασικά

Μόλις εγκαταστήσετε το Bitdefender Total Security, η συσκευή σας προστατεύεται από κάθε είδους απειλές (όπως κακόβουλο λογισμικό, spyware, ransomware, exploits, botnets και trojans) και απειλές στο Διαδίκτυο (όπως χάκερ, ηλεκτρονικό ψάρεμα και spam).

Η εφαρμογή χρησιμοποιεί την τεχνολογία Photon για να αυξήσει την ταχύτητα και απόδοση της διαδικασίας ανίχνευσης και αναχαίτισης απειλών. Λειτουργεί μαθαίνοντας το αποτύπωμα χρήσης των εφαρμογών του συστήματος σας ώστε να γνωρίζει τι και πότε να ανιχνεύσει, ελαχιστοποιώντας τις επιπτώσεις στην απόδοση του συστήματος

Η σύνδεση με δημόσια ασύρματα δίκτυα που ανήκουν σε αεροδρόμια, εμπορικά κέντρα, καφέ ή ξενοδοχεία χωρίς προστασία μπορεί να είναι επικίνδυνη για τη συσκευή και τα δεδομένα σας. Κυρίως επειδή οι απατεώνες μπορεί να παρακολουθούν τη δραστηριότητά σας και να βρουν την καλύτερη στιγμή για να κλέψουν προσωπικά δεδομένα, αλλά και επειδή όλοι μπορούν να δουν τη διεύθυνση IP σας, καθιστώντας έτσι τη μηχανή σας θύμα μελλοντικών cyberattacks. Για να αποφύγετε τέτοιες δυσάρεστες καταστάσεις, εγκαταστήστε και χρησιμοποιήστε την εφαρμογή “*VPN*” (p. 156).

Μπορείτε να παρακολουθείτε τους κωδικούς πρόσβασης και τους λογαριασμούς σας στο διαδίκτυο, αποθηκεύοντάς τα με “*Προστασία των κωδικών σας με το Διαχειριστή Κωδικών Ασφαλείας*” (p. 145) σε ένα wallet. Με ένα μοναδικό κύριο κωδικό πρόσβασης είστε σε θέση να προστατεύσετε το απόρρητό σας από εισβολείς που μπορεί να προσπαθήσουν να σας κλέψουν χρήματα.

“*ΠΡΟΣΤΑΣΙΑ ΓΙΑ Webcam*” (p. 138)Διατηρεί μακριά τις μη αξιόπιστες εφαρμογές από την πρόσβαση στην βιντεοκάμερα σας, αποφεύγοντας έτσι οποιαδήποτε προσπάθεια να παραβιαστεί. Με βάση την επιλογή των χρηστών του Bitdefender, η πρόσβαση σε δημοφιλείς εφαρμογές στην κάμερά σας θα επιτρέπεται ή θα εμποδίζεται.

Για να σας προστατέψουμε από πιθανές ενοχλήσεις και κατασκόπους όταν η συσκευή σας είναι συνδεδεμένη σε μη ασφαλές ασύρματο δίκτυο, το Bitdefender αναλύει το επίπεδο ασφαλείας του και, όταν είναι απαραίτητο, σας προτείνει τρόπους για την ενίσχυση της ασφάλειας των online

δραστηριοτήτων σας. Εάν θα θέλατε οδηγίες για το πως θα διατηρήσετε τα δεδομένα ασφαλή. μπορείτε να ανατρέξετε στο *"Wi-Fi Security Advisor"* (p. 134).

Τα κρυπτογραφημένα αρχεία με ransomware μπορούν τώρα να ανακτηθούν χωρίς να χρειαστεί να ξοδέψετε χρήματα για οποιοδήποτε ζητούμενο λύτρο. Για πληροφορίες σχετικά με τον τρόπο ανάκτησης κρυπτογραφημένων αρχείων, ανατρέξτε στο *"Αποκατάσταση από Ransomware"* (p. 143).

Ενώ εργάζετε, παίζετε παιχνίδια ή βλέπετε ταινίες, το Bitdefender μπορεί να σας προσφέρει μία αδιάλειπτη εμπειρία χρήστη αναβάλλοντας εργασίες συντήρησης, εξαφανίζοντας τις διακοπές και ρυθμίζοντας τα οπτικά εφφέ του συστήματος. Μπορείτε να επωφεληθείτε από όλα αυτά ενεργοποιώντας και προσαρμόζοντας τα *"Προφίλ"* (p. 183).

Το Bitdefender θα πάρει για λογαριασμό σας τις περισσότερες σχετιζόμενες με την ασφάλεια αποφάσεις και σπάνια θα σας δείξει pop-up για συναγερμό. Λεπτομέρειες για τις ενέργειες που εκτελέστηκαν και πληροφορίες για την λειτουργία εφαρμογών είναι διαθέσιμες στο παράθυρο Ειδοποιήσεων. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Ειδοποιήσεις"* (p. 15).

Από καιρό σε καιρό, θα πρέπει να ανοίγετε το Bitdefender και να διορθώσετε τυχόν υφιστάμενα προβλήματα. Ίσως χρειαστεί να διαμορφώσετε συγκεκριμένα στοιχεία του Bitdefender ή να λάβετε προληπτικά μέτρα για την προστασία της συσκευής και των δεδομένων σας.

Για να χρησιμοποιήσετε τα διαδικτυακά χαρακτηριστικά του Bitdefender Total Security και να διαχειριστείτε τις συνδρομές και τις συσκευές σας, μπείτε στον Bitdefender λογαριασμό σας. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Bitdefender Central"* (p. 32).

Το *"Πως μπορείτε να"* (p. 47) τμήμα είναι εκεί όπου θα βρείτε βήμα-βήμα οδηγίες για την εκτέλεση κοινών εργασιών. Εάν αντιμετωπίσετε προβλήματα κατά τη χρήση του Bitdefender, ελέγξτε το *"Επίλυση κοινών ζητημάτων"* (p. 193) τμήμα για πιθανές λύσεις των πλέον συνηθισμένων προβλημάτων.

Άνοιγμα παραθύρου του Bitdefender

Για πρόσβαση στην κύρια διεπαφή του Bitdefender Total Security, κάντε κλικ στο εικονίδιο στην επιφάνεια εργασίας σας.

Εάν είναι απαραίτητο, μπορείτε επίσης να ακολουθήσετε τα παρακάτω βήματα:

- Στα **Windows 7**:
  1. Κάντε κλικ στην **Έναρξη** και οδηγηθείτε στο **Όλα τα προγράμματα**.
  2. Κάντε κλικ στο **Bitdefender**.
  3. Κάντε κλικ στο **Bitdefender Total Security** ή, για πιο γρήγορα, κάντε διπλό κλικ στο εικονίδιο του Bitdefender στην περιοχή ειδοποιήσεων (system tray).
- Στα **Windows 8 και στα Windows 8.1**:

  Εντοπίστε το Bitdefender από το μενού έναρξης των Windows (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Bitdefender" απευθείας στο μενού Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του. Εναλλακτικά, ανοίξτε την εφαρμογή επιφάνειας εργασίας και στη συνέχεια κάντε διπλό κλικ στο εικονίδιο Bitdefender στο System Tray.
- Στα **Windows 10**:

  Πληκτρολογήστε "Bitdefender" στο πλαίσιο αναζήτησης από τη γραμμή εργασιών και στη συνέχεια κάντε κλικ στο εικονίδιο του. Εναλλακτικά, κάντε διπλό κλικ στο εικονίδιο Bitdefender στο δίσκο του συστήματος.

Για περισσότερες πληροφορίες σχετικά με το παράθυρο του Bitdefender και το εικονίδιο στην περιοχή ειδοποιήσεων, παρακαλώ ανατρέξτε στο *"Βασικό περιβάλλον του Bitdefender"* (p. 20).

2.1.1. Ειδοποιήσεις

Το Bitdefender διατηρεί ένα λεπτομερές αρχείο καταγραφής συμβάντων σχετικά με τη δραστηριότητά του στη συσκευή σας. Κάθε φορά που συμβαίνει κάτι σχετικό με την ασφάλεια του συστήματος ή των δεδομένων σας, ένα νέο μήνυμα προστίθεται στις Ενημερώσεις του Bitdefender με τον ιδιο τρόπο που ένα νέο μήνυμα ηλεκτρονικού ταχυδρομείου εμφανίζεται στα Εισερχόμενα σας.

Οι Ενημερωςεις αποτελούν ένα πολύ σημαντικό εργαλείο για την παρακολούθηση και τη διαχείριση της προστασίας του Bitdefender σας. Για παράδειγμα, μπορείτε εύκολα να ελέγξετε εάν η ενημέρωση πραγματοποιήθηκε με επιτυχία, εάν εντοπίστηκαν απειλές ή ευπάθειες στη συσκευή σας κ.λπ. Επιπλέον, μπορείτε να κάνετε περαιτέρω ενέργειες αν χρειαστεί ή να αλλάξετε ενέργειες που έχουν γίνει από το Bitdefender.

Για να αποκτήσετε πρόσβαση στο ιστορικό Ειδοποιήσεων, κάντε κλικ στο **Ειδοποιήσεις** στο μενού πλοήγησης στο Bitdefender interface. Κάθε φορά που συμβαίνει κάποιο σημαντικό γεγονός, ένας μετρητής μπορεί να παρατηρηθεί στο 2 εικονίδιο.

Ανάλογα με τον τύπο και τη σοβαρότητα, οι ειδοποιήσεις ομαδοποιούνται σε:

- **Critical** τα συμβάντα δείχνουν κρίσιμα θέματα. Θα πρέπει να τα ελέγξετε αμέσως.
- **Προσοχή** τα συμβάντα δείχνουν μη κρίσιμα θέματα Θα πρέπει να τα ελέγξετε και να τα διορθώσετε όταν έχετε το χρόνο.
- Οι **πληροφορίες** συμβάντων δείχνουν επιτυχείς εργασίες

Κάντε κλικ σε κάθε καρτέλα για να βρείτε περισσότερες λεπτομέρειες σχετικά με τα συμβάντα που δημιουργούνται. Τα συνοπτικά στοιχεία εμφανίζονται με ένα κλικ σε κάθε τίτλο συμβάντος, και συγκεκριμένα: μια σύντομη περιγραφή, η δράση που το Bitdefender πήρε όταν συνέβη, και την ημερομηνία και την ώρα, όταν αυτό συνέβη. Επιλογές μπορεί να παρέχονται για να ληφθεί περαιτέρω ενέργεια εάν χρειαστεί.

Για να σας βοηθήσει να διαχειριστείτε εύκολα τα καταγεγραμμένα συμβάντα, κάθε τμήμα του παραθύρου Ενημερώσεις παρέχει επιλογές για τη διαγραφή ή σήμανση ως αναγνωσμένου όλων των γεγονότων σε αυτό το τμήμα.

2.1.2. Προφίλ

Μερικές από τις δραστηριότητες του υπολογιστή, όπως διαδικτυακά παιχνίδια ή παρουσιάσεις βίντεο, απαιτούν αυξημένη ανταπόκριση του συστήματος, και υψηλή απόδοση χωρίς διακοπές. Όταν ο φορητός υπολογιστής σας λειτουργεί με μπαταρία, καλό είναι οι περιττές ενέργειες, οι οποίες καταναλώνουν επιπλέον ισχύ, να αναβληθουν μέχρι ο φορητός υπολογιστής σας συνδεθεί στο ρεύμα.

Τα Bitdefender Προφίλ αποδίδουν περισσότερους πόρους του συστήματος στις εφαρμογές που εκτελούνται με την προσωρινή τροποποίηση των ρυθμίσεων προστασίας και τη ρύθμιση παραμέτρων του συστήματος Κατά συνέπεια, οι επιπτώσεις του συστήματος στις δραστηριότητες σας ελαχιστοποιούνται.

Για την προσαρμογή σε διαφορετικές δραστηριότητες, το Bitdefender διαθέτει τα ακόλουθα προφίλ:

Προφίλ Εργασίας
Βελτιστοποιεί την απόδοση της εργασίας σας εντοπίζοντας και προσαρμόζοντας τις ρυθμίσεις του προϊόντος και του συστήματος.

Προφίλ Ταινιών
Ενισχύει τα οπτικά εφέ και εξαλείφει τις διακοπές, όταν παρακολουθείτε ταινίες.

Προφίλ Παιχνιδιών
Ενισχύει τα οπτικά εφέ και εξαλείφει τις διακοπές όταν παίζετε παιχνίδια.

Προφίλ Δημόσιο Wi-Fi
Εφαρμόζει ρυθμίσεις του προϊόντος για να επωφεληθείτε από την πλήρη προστασία, ενώ συνδέεστε με ένα μη ασφαλές ασύρματο δίκτυο.

Προφίλ Battery Mode
Εφαρμόζει ρυθμίσεις του προϊόντος και μειώνει τις παρασκηνιακές δραστηριότητας για να εξοικονομήσει τη ζωή της μπαταρίας.

Διαμορφώστε αυτόματη ενεργοποίηση των προφίλ

Για μια εύχρηστη εμπειρία, μπορείτε να διαμορφώσετε το Bitdefender ώστε να διαχειρίζεται το προφίλ εργασίας σας. Σε αυτήν την περίπτωση, το Bitdefender εντοπίζει αυτόματα τη δραστηριότητα που εκτελείτε και εφαρμόζει τις ρυθμίσεις βελτιστοποίησης του συστήματος και του προϊόντος.

Την πρώτη φορά που θα αποκτήσετε πρόσβαση στα **Προφίλ** θα σας ζητηθεί να ενεργοποιήσετε τα αυτόματα προφίλ. Για να το κάνετε αυτό, μπορείτε απλώς να κάνετε κλικ στο **ΕΝΕΡΓΟΠΟΙΗΣΗ** στο παράθυρο που εμφανίζεται.

Μπορείτε να κάνετε κλικ στο **ΟΧΙ ΤΩΡΑ** εάν θέλετε να ενεργοποιήσετε τη λειτουργία αργότερα.

Για να επιτρέψετε στο Bitdefender να ενεργοποιεί αυτόματα τα προφίλ:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **Προφίλ** , κάντε κλικ στο **Ρυθμίσεις** .

3. Επιλέξτε τον αντίστοιχο διακόπτη για να ενεργοποιήσετε την επιλογή **Ενεργοποιήσετε αυτόματα τα profiles**.

Εάν δεν θέλετε τα προφίλ να ενεργοποιείται αυτόματα, απενεργοποιήστε το διακόπτη.

Για να ενεργοποιήσετε χειροκίνητα ένα προφίλ, κάντε κλικ στον αντίστοιχο διακόπτη Από τα πρώτα τρία προφίλ, μόνο ένα μπορεί να ενεργοποιηθεί χειροκίνητα ταυτόχρονα.

Για περισσότερες πληροφορίες, παρακολούμε ανατρέξτε στο "*Προφίλ*" (p. 183)

2.1.3. Ρυθμίσεις προστασίας του Κωδικού πρόσβασης του Bitdefender

Εάν δεν είστε το μόνο άτομο με δικαιώματα διαχειριστή που χρησιμοποιεί αυτήν τη συσκευή, συνιστάται να προστατεύσετε τις ρυθμίσεις Bitdefender με κωδικό πρόσβασης.

Για να διαμορφώσετε την προστασία με κωδικό για τις ρυθμίσεις του Bitdefender:

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Γενικά** , ενεργοποιήστε το **Προστασία με κωδικό πρόσβασης**.
3. Εισάγετε τον κωδικό πρόσβασης στα δύο πεδία και στη συνέχεια κάντε κλικ στο **OK**. Ο κωδικός πρόσβασης πρέπει να αποτελείται από τουλάχιστον 8 χαρακτήρες.

Αφού έχετε ορίσετε έναν κωδικό πρόσβασης, ο καθένας που θα προσπαθήσει να αλλάξει τις ρυθμίσεις του Bitdefender θα πρέπει πρώτα να δώσει τον κωδικό πρόσβασης.

Σημαντικό

Βεβαιωθείτε ότι θυμάστε τον κωδικό πρόσβασής σας ή κρατήσετε ένα αρχείο σε ένα ασφαλές μέρος. Εάν ξεχάσετε τον κωδικό πρόσβασης, θα πρέπει να εγκαταστήσετε ξανά το πρόγραμμα ή να επικοινωνήσετε με το Bitdefender για την υποστήριξη.

Για να καταργήσετε την προστασία με password:

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.

2. Στο παράθυρο **Γενικά** , απενεργοποιήστε το **Προστασία με κωδικό πρόσβαση**.
3. Εισάγετε τον κωδικό πρόσβασης και στη συνέχεια κάντε κλικ στο **OK**.

Σημείωση
Για να τροποποιήσετε τον κωδικό πρόσβασης για το προϊόν σας, κάντε κλικ στο **Αλλαγή κωδικού**. Πληκτρολογήστε τον τρέχοντα κωδικό πρόσβασης και στη συνέχεια κάντε κλικ στο **OK**. Στο νέο παράθυρο που θα εμφανιστεί εισάγετε τον νέο κωδικό που θα χρησιμοποιείτε στο εξής για να αποτρέπετε την πρόσβαση στις ρυθμίσεις του Bitdefender σας.

2.1.4. Αναφορές προϊόντος

Οι αναφορές προϊόντων περιέχουν πληροφορίες σχετικά με τον τρόπο χρήσης του προϊόντος Bitdefender που έχετε εγκαταστήσει. Οι πληροφορίες αυτές είναι απαραίτητες για την βελτίωση του προιόντος και μπορούν να μας βοηθήσουν να σας προσφέρουμε μια καλύτερη εμπειρία χρήσης στο μέλλον.

Σημειώστε ότι οι αναφορές αυτές δεν περιέχουν εμπιστευτικά δεδομένα, όπως όνομα ή διεύθυνση IP και δεν πρόκειται να χρησιμοποιηθούν για εμπορικούς σκοπούς.

Εάν κατά τη διάρκεια της διαδικασίας εγκατάστασης έχετε επιλέξει να στείλετε τέτοιες αναφορές στους Bitdefender servers και τώρα θα θέλατε να διακόψετε τη διαδικασία:

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Επιλέξτε την καρτέλα **Advanced**.
3. Απενεργοποιήστε **Αναφορές προϊόντος**.

2.1.5. Ειδικές ειδοποιήσεις προσφορών

Όταν οι προσφορές είναι διαθέσιμες, το Bitdefender προϊόν έχει ρυθμιστεί να σας ειδοποιεί μέσω ενός αναδυόμενου παραθύρου. Αυτό σας δίνει την ευκαιρία να επωφεληθείτε από τις ευνοϊκές τιμές και να διατηρήσετε τις συσκευές προστατευμένες για μεγαλύτερο χρονικό διάστημα.

Για να ενεργοποιήσετε ή να απενεργοποιήσετε τις ειδοποιήσεις για ειδικές προσφορές:

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.

2. Στο παράθυρο **ΓΕΝΙΚΑ**, επιλέξτε τον αντίστοιχο ON/OFF διακόπτη.

Οι ειδικές προσφορές και οι κοινοποιήσεις του προϊόντος είναι ενεργοποιημένες από προεπιλογή.

2.2. Βασικό περιβάλλον του Bitdefender

Bitdefender Total Security ικανοποιεί τις ανάγκες τόσο των αρχάριων στους υπολογιστές όσο και των πολύ εξειδικευμένων τεχνικά . Το γραφικό περιβάλλον του χρήστη έχει σχεδιαστεί για να ταιριάζει σε κάθε κατηγορία χρηστών.

Για να εισέλθετε στο μενού του Bitdefender, στην επάνω αριστερή πλευρά, θα εμφανιστεί ένα εισαγωγικός οδηγός με οδηγίες χρήσης και ρύθμισης του προϊόντος. Επιλέξτε το αντίστοιχο σύμβολο για να συνεχίσετε την περιήγηση, ή **Παράλειψη περιήγησης** για να κλείσετε τον οδηγό.

Το Bitdefender system tray εικονίδιο είναι διαθέσιμο ανά πάσα στιγμή, ανεξάρτητα από το εάν θέλετε να ανοίξετε το κύριο παράθυρο, να εκτελέσετε μια ενημέρωση προϊόντος ή να προβάλετε πληροφορίες σχετικά με το εγκατεστημένη έκδοση.

Το κύριο παράθυρο σάς παρέχει πληροφορίες σχετικά με την κατάσταση ασφαλείας σας. Με βάση τη χρήση και τις ανάγκες της συσκευής σας, το Autopilot εμφανίζει εδώ διαφορετικούς τύπους συστάσεων που θα σας βοηθήσουν να βελτιώσετε την ασφάλεια και την απόδοση της συσκευής σας. Επιπλέον, μπορείτε να προσθέσετε γρήγορες ενέργειες που χρησιμοποιείτε περισσότερο, ώστε να μπορείτε να τις έχετε πάντα στη διάθεσή σας όποτε χρειάζεστε.

Από το μενού πλοήγησης στην αριστερή πλευρά μπορείτε να αποκτήσετε πρόσβαση στην περιοχή ρυθμίσεων, στις ειδοποιήσεις και στις Bitdefender ενότητες για λεπτομερή διαμόρφωση και προχωρημένες εργασίες διαχείρισης.

Από το επάνω μέρος της κύριας διεπαφής, μπορείτε να αποκτήσετε πρόσβαση στον Bitdefender λογαριασμό σας . Επίσης, μπορείτε να επικοινωνήσετε μαζί μας για υποστήριξη σε περίπτωση που έχετε ερωτήσεις ή κάτι απροσδόκητο εμφανιστεί.

2.2.1. Εικονίδιο περιοχής ειδοποιήσεων

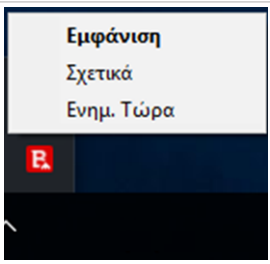
Για να διαχειριστείτε ολόκληρο το προϊόν πιο γρήγορα, μπορείτε να χρησιμοποιήσετε το εικονίδιο του Bitdefender στην περιοχή ειδοποιήσεων.

Σημείωση

Το εικονίδιο του Bitdefender μπορεί να μην είναι πάντα ορατό. Για να κάνετε το εικονίδιο να εμφανίζεται μόνιμα:

- Στα **Windows 7, Windows 8 και στα Windows 8.1**:
  1. Κάντε κλικ στο βελάκι στην κάτω δεξιά γωνία της οθόνης.
  2. Κάντε κλικ στο **Προσαρμογή...** Για να ανοίξετε το παράθυρο εικονιδίων περιοχής ειδοποιήσεων .
  3. Επιλέξτε **Εικονίδια και ειδοποιήσεις** για το εικονίδιο του **Bitdefender Agent** .
- Στα **Windows 10**:
  1. Κάντε δεξί κλικ στη γραμμή εργασιών και επιλέξτε **Ιδιότητες** .
  2. Κάντε κύλιση προς τα κάτω και κάντε κλικ στο σύνδεσμο **Επιλέξτε ποια εικονίδια εμφανίζονται στη γραμμή εργασιών** στη σελίδα **Περιοχή ειδοποιήσεων**.
  3. Ενεργοποιήστε το διακόπτη δίπλα στο **Bitdefender Agent**.

Εάν κάντε διπλό κλικ σε αυτό το εικονίδιο, το Bitdefender θα ανοίξει. Επίσης, κάνοντας δεξί κλικ στο εικονίδιο, ένα αναδυόμενο μενού θα σας επιτρέψει να διαχειριστείτε γρήγορα το Bitdefender προϊόν.



Tray Icon

- **Εμφάνιση** - ανοίγει το κύριο παράθυρο του Bitdefender.
- **Σχετικά με** - ανοίγει ένα παράθυρο όπου μπορείτε να δείτε πληροφορίες σχετικά με το Bitdefender, από όπου μπορείτε να αναζητήσετε βοήθεια σε περίπτωση που εμφανιστεί κάτι απρόσμενο, από όπου μπορείτε να ανατρέξετε στη Συμφωνία Συνδρομής, και να δείτε 3rd Party Components και Πολιτική Απορρήτου.
- **Ενημέρωση Τώρα** - ξεκινά μια άμεση ενημέρωση. Μπορείτε να παρακολουθείτε την κατάσταση ενημέρωσης στον πίνακα Ενημέρωση στο βασικό παράθυρο Bitdefender.

Το εικονίδιο δίσκου συστήματος Bitdefender σας ενημερώνει πότε ζητήματα επηρεάζουν τη συσκευή σας ή πώς λειτουργεί το προϊόν, εμφανίζοντας ένα ειδικό σύμβολο, ως εξής:

Κανένα πρόβλημα δεν επηρεάζει την ασφάλεια του συστήματός σας.
Κρίσιμα ζητήματα επηρεάζουν την ασφάλεια του συστήματός σας. Απαιτείται η άμεση προσοχή σας και πρέπει να διορθωθούν το συντομότερο δυνατόν.

Εάν το Bitdefender δεν λειτουργεί, το εικονίδιο στην περιοχή ειδοποιήσεων εμφανίζεται σε γκρίζο φόντο: . Αυτό συμβαίνει συνήθως όταν λήξει η συνδρομή. Μπορεί επίσης να προκύψει όταν οι υπηρεσίες του Bitdefender δεν ανταποκρίνονται ή όταν άλλα σφάλματα επηρεάζουν την ομαλή λειτουργία του Bitdefender.

2.2.2. Μενού πλοήγησης

Στην αριστερή πλευρά της διεπαφής Bitdefender βρίσκεται το μενού πλοήγησης, το οποίο σας επιτρέπει να αποκτήσετε γρήγορα πρόσβαση στις λειτουργίες και τα εργαλεία Bitdefender που χρειάζεστε για να χειριστείτε το προϊόν σας. Οι διαθέσιμες καρτέλες σε αυτήν την περιοχή είναι:

- **Dashboard**. Από εδώ, μπορείτε να διορθώσετε γρήγορα θέματα ασφάλειας, να προβάλετε συστάσεις σύμφωνα με τις ανάγκες του συστήματος και τα πρότυπα χρήσης, να πραγματοποιήσετε γρήγορες ενέργειες και να εγκαταστήσετε το Bitdefender σε άλλες συσκευές.

- **Protection**. Από εδώ, μπορείτε να ξεκινήσετε και να διαμορφώσετε σαρώσεις προστασίας από ιούς, να αποκτήσετε πρόσβαση στις ρυθμίσεις του Τείχους προστασίας, να ανακτήσετε δεδομένα σε περίπτωση που κρυπτογραφηθεί από ένα ransowmware και να διαμορφώσετε την προστασία ενώ περιηγείστε στο Διαδίκτυο.

- **Απόρρητο**. Από εδώ μπορείτε να δημιουργήσετε password managers πρόσβασης για τους λογαριασμούς σας στο διαδίκτυο, να προστατεύσετε την πρόσβαση στην κάμερά σας από ανεπιθύμητα μάτια, να πραγματοποιήσετε ηλεκτρονικές πληρωμές σε ασφαλές περιβάλλον, να ανοίξετε την εφαρμογή VPN και να προστατέψετε τα παιδιά σας προβάλλοντας και περιορίζοντας online δραστηριότητα.

- **Βοηθητικά προγράμματα**. Από εδώ, μπορείτε να βελτιώσετε την ταχύτητα του συστήματος και να διαμορφώσετε τη λειτουργία Anti-theft για τις συσκευές σας.
- **Ειδοποιήσεις**. Από εδώ, έχετε πρόσβαση στις παραγώμενες ειδοποιήσεις.
- **Ρυθμίσεις**. Από εδω έχετε πρόσβαση στις γενικές ρυθμίσεις.

Στην επάνω πλευρά της κύριας διεπαφής, θα βρείτε τις δυνατότητες **Ο λογαριασμός μου** και **Υποστήριξη** .

- **Υποστήριξη**. Από εδώ, κάθε φορά που χρειάζεστε βοήθεια για την επίλυση μιας κατάστασης με το Bitdefender Total Security, μπορείτε να επικοινωνήσετε με το Τμήμα Τεχνικής Υποστήριξης της Bitdefender.
- **Ο λογαριασμός μου**. Αποκτήστε πρόσβαση στον Bitdefender λογαριασμό σας για να επαληθεύσετε τις συνδρομές σας και την εκτέλεση των εργασιών ασφαλείας στις συσκευές που διαχειρίζεστε. Λεπτομέρειες σχετικά με το Bitdefender λογαριασμό και τη συνδρομή που χρησιμοποιείτε είναι διαθέσιμες.

2.2.3. Ταμπλό

Το κύριο παράθυρο σας επιτρέπει να εκτελείτε κοινές εργασίες, να διορθώνετε γρήγορα τα ζητήματα ασφάλειας, να βλέπετε πληροφορίες σχετικά με τη λειτουργία του προϊόντος και να έχετε πρόσβαση στις καρτέλες όπου διαμορφώνετε τις ρυθμίσεις του προϊόντος.

Τα πάντα είναι μόλις μερικά κλικ μακριά.

Το παράθυρο είναι οργανωμένο σε τρεις βασικούς τομείς:

Security status area

Εδώ μπορείτε να ελέγξετε την κατάσταση ασφαλείας της συσκευής σας.

Autopilot

Εδώ μπορείτε να ελέγξετε τις συστάσεις του Autopilot για να διασφαλίσετε την καλή λειτουργία του συστήματος.

Γρήγορες ενέργειες

Εδώ μπορείτε να εκτελέσετε διάφορες εργασίες για να διατηρήσετε προστατευμένο το σύστημά σας και για να λειτουργεί σε βέλτιστη

ταχύτητα. Μπορείτε επίσης να εγκαταστήσετε το Bitdefender σε άλλες συσκευές, με την προϋπόθεση ότι η συνδρομή σας παρέχει τον ικανό αριθμό συσκευών.

Security status area

Το Bitdefender χρησιμοποιεί ένα σύστημα παρακολούθησης προβλημάτων για να εντοπίσει και να σας ενημερώσει σχετικά με ζητήματα που ενδέχεται να επηρεάσουν την ασφάλεια της συσκευής και των δεδομένων σας. Κάποια εντοπισμένα ζητήματα περιλαμβάνουν σημαντικές ρυθμίσεις προστασίας που είναι απενεργοποιημένες και άλλες καταστάσεις που μπορεί να αποτελέσουν κίνδυνο για την ασφάλεια.

Όποτε ζητήματα επηρεάζουν την ασφάλεια της συσκευής σας, η κατάσταση που εμφανίζεται στην επάνω πλευρά της διεπαφής Bitdefender γίνεται κόκκινη. Η εμφανιζόμενη κατάσταση υποδεικνύει τη φύση των ζητημάτων που επηρεάζουν το σύστημά σας. Επίσης, το εικονίδιο του system tray αλλάζει σε και εάν μετακινείτε το δείκτη του ποντικιού πάνω από το εικονίδιο, ένα αναδυόμενο παράθυρο θα επιβεβαιώσει την ύπαρξη εκκρεμών ζητημάτων.

Καθώς τα εντοπισμένα ζητήματα ενδέχεται να εμποδίσουν το Bitdefender να σας προστατεύσει από απειλές ή να αποτελέσει σοβαρό κίνδυνο για την ασφάλεια, σας συνιστούμε να δώσετε προσοχή και να τα διορθώσετε το συντομότερο δυνατό. Για να διορθώσετε ένα πρόβλημα, κάντε κλικ στο κουμπί δίπλα στο πρόβλημα που εντοπίστηκε.

Autopilot

Για να σας προσφέρουμε αποτελεσματική λειτουργία και αυξημένη προστασία κατά την εκτέλεση διαφορετικών δραστηριοτήτων, το Bitdefender Autopilot θα ενεργήσει ως προσωπικός σας σύμβουλος ασφάλειας. Ανάλογα με τη δραστηριότητα που εκτελείτε, είτε εργάζεστε, πραγματοποιείτε ηλεκτρονικές πληρωμές, παρακολουθείτε ταινίες ή παίζετε παιχνίδια το Bitdefender Autopilot θα παρουσιάσει συνημμένες συστάσεις βάσει της χρήσης και των αναγκών της συσκευής σας. Οι προτεινόμενες συστάσεις μπορεί επίσης να σχετίζονται με ενέργειες που πρέπει να εκτελέσετε για να διατηρήσετε το προϊόν σας σε πλήρη λειτουργία.

Για να αρχίσετε να χρησιμοποιείτε μια προτεινόμενη λειτουργία ή να κάνετε βελτιώσεις στο προϊόν σας, κάντε κλικ στο αντίστοιχο κουμπί.

Απενεργοποίηση ειδοποιήσεων αυτόματου πιλότου

Για να επιστήσετε την προσοχή σας στις συστάσεις Autopilot, το προϊόν του Bitdefender έχει ρυθμιστεί για να σας ειδοποιεί μέσω ενός αναδυόμενου παραθύρου.

Για να απενεργοποιήσετε τις ειδοποιήσεις του Autopilot :

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Γενικά** , απενεργοποιήστε το **Ειδοποιήσεις συστάσεων**.

Γρήγορες ενέργειες

Χρησιμοποιώντας τις γρήγορες ενέργειες, μπορείτε να ξεκινήσετε γρήγορα εργασίες που θεωρείτε σημαντικές για την προστασία του συστήματος σας και τη λειτουργία του με τη βέλτιστη ταχύτητα.

Από προεπιλογή, το Bitdefender έρχεται με μερικές γρήγορες ενέργειες που μπορούν να αντικατασταθούν με εκείνες που γνωρίζετε ότι χρησιμοποιείτε κυρίως. Για να αντικαταστήσετε μια γρήγορη ενέργεια:

1. Κάντε κλικ στο εικονίδιο στην επάνω δεξιά γωνία της κάρτας που θέλετε να καταργήσετε.
2. Δείξτε την εργασία που θέλετε να προσθέσετε στο interface και, στη συνέχεια, κάντε κλικ στο κουμπί **ADD**.

Οι εργασίες που μπορείτε να προσθέσετε στο κύριο interface είναι:

- **Γρήγορη Σάρωση**. Εκτελέστε μια γρήγορη σάρωση για να εντοπίσετε αμέσως τις πιθανές απειλές που ενδέχεται να υπάρχουν στη συσκευή σας.
- **Σάρωση Συστήματος**. Εκτελέστε σάρωση συστήματος για να βεβαιωθείτε ότι η συσκευή σας είναι καθαρή από απειλές.
- **Σάρωση για ευπάθειες**. Σαρώστε τη συσκευή σας για ευπάθειες για να βεβαιωθείτε ότι όλες οι εγκατεστημένες εφαρμογές, μαζί με το λειτουργικό σύστημα, είναι ενημερωμένες και λειτουργούν σωστά.
- **Σύμβουλος ασφάλειας Wi-Fi** . Ανοίξτε το παράθυρο Wi-Fi Security Advisor μέσα στη μονάδα ευπάθειας.
- **Wallets**. Προβάλετε και διαχειριστείτε τα wallets σας.
- **Άνοιγμα Safepay**. Ανοίξτε το Bitdefender Safepay™ για την προστασία των ευαίσθητων δεδομένων σας, ενώ πραγματοποιείτε διαδικτυακές συναλλαγές.

- **Άνοιγμα VPN**. Ανοίξτε το Bitdefender VPN για να προσθέσετε ένα επιπλέον επίπεδο προστασίας ενώ είστε συνδεδεμένοι στο διαδίκτυο.
- **Καταστροφέας Αρχείων**. Εκκινήστε το εργαλείο File Shredder για να αφαιρέσετε ίχνη ευαίσθητων δεδομένων από τη συσκευή σας.
- **Άνοιγμα του OneClick Optimizer**. Ελευθερώστε χώρο στο δίσκο, διορθώσετε τα σφάλματα μητρώου και προστατεύστε τα προσωπικά σας δεδομένα διαγράφοντας τα αρχεία που δεν μπορούν πλέον να είναι χρήσιμα με ένα μόνο κλικ.

Για να αρχίσετε να προστατεύετε επιπλέον συσκευές με το Bitdefender:

1. Πατήστε **Εγκατάσταση σε άλλη συσκευή**.

   Εμφανίζεται ένα νέο παράθυρο στην οθόνη σας.

2. Επιλέξτε **ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΕΓΚΑΤΑΣΤΑΣΗΣ**.

3. Ακολουθήστε τα βήματα της οθόνης για να εγκαταστήσετε το Bitdefender.

Ανάλογα την επιλογή σας, τα ακόλουθα Bitdefender προϊόντα θα εγκατασταθούν:

- Bitdefender Total Security σε windows συσκευές.
- Bitdefender Antivirus για Mac σε OS X συσκευές.
- Bitdefender Mobile Security για Android συσκευές.
- Bitdefender Mobile Security για iOS συσκευές.

2.2.4. Τα τμήματα του Bitdefender

Το Bitdefender προϊόν έρχεται με τρία τμήματα τα οποία χωρίζονται σε χρήσιμες ενότητες για να σας βοηθήσει να μείνετε προστατευμένοι ενώ εργάζεστε, να περιηγείστε στο διαδίκτυο ή να εκτελείτε τις online πληρωμές, να βελτιώσει την ταχύτητα του συστήματός σας και πολλά άλλα.

Κάθε φορά που θέλετε να αποκτήσετε πρόσβαση στις ενότητες για ένα συγκεκριμένο τμήμα ή για να ξεκινήσετε τη διαμόρφωση του προϊόντος σας, χρησιμοποιείστε τα εικονίδια που βρίσκονται στο μενού πλοήγησης του Bitdefender interface:

- Προστασία
- Ιδιωτικότητα

- Εργαλεία

Προστασία

Στην ενότητα Προστασία μπορείτε να διαμορφώσετε τις προηγμένες ρυθμίσεις ασφαλείας, να διαχειριστείτε φίλους και spammers, να προβάλετε και να επεξεργαστείτε τις ρυθμίσεις σύνδεσης δικτύου, να ρυθμίσετε τις δυνατότητες Πρόληψης απειλών στο διαδίκτυο, να ελέγξετε και να διορθώσετε πιθανές ευπάθειες του συστήματος και να αξιολογήσετε την ασφάλεια των ασύρματων δικτύων στα οποία συνδέεστε .

Οι ενότητες που μπορείτε να διαχειριστείτε στο τμήμα Προστασίας είναι:

ANTIVIRUS

Η προστασία από ιούς είναι τα θεμέλια της ασφάλειας σας. Το Bitdefender σας προστατεύει σε πραγματικό χρόνο και κατ' επιλογή από κάθε είδους απειλές, όπως οι malware, trojans, spyware, adware, κλπ.

Από την ενότητα Antivirus μπορείτε εύκολα να έχετε πρόσβαση στις ακόλουθες εργασίες σάρωσης:

- Γρηγορη Σαρωση
- Σάρωση Συστήματος
- Διαχείριση Σαρώσεων
- Περιβάλλον διάσωσης

Για περισσότερες πληροφορίες σχετικά με τις εργασίες σάρωσης και το πως να ρυθμίσετε την προστασία από ιούς, ανατρέξτε στο "*Antivirus Προστασία*" (p. 86).

ONLINE ΠΡΟΛΗΨΗ ΑΠΕΙΛΩΝ

Η Online Threat Prevention βοηθά να μένετε προστατευμένοι από επιθέσεις phishing, απόπειρες απάτης και του διαρροές προσωπικών δεδομένων, ενώ σερφάρετε στο Διαδίκτυο.

Για περισσότερες πληροφορίες σχετικά με τη ρύθμιση του Bitdefender για την προστασία της δραστηριότητάς σας στο διαδίκτυο, παρακαλούμε ανατρέξτε στο "*ONLINE ΠΡΟΛΗΨΗ ΑΠΕΙΛΩΝ*" (p. 110).

FIREWALL

Το τείχος προστασίας σας προστατεύει, ενώ είστε συνδεδεμένοι με τα δίκτυα και το Διαδίκτυο φιλτράροντας όλες τις προσπάθειες σύνδεσης.

Για περισσότερες πληροφορίες σχετικά με τη διαμόρφωση του τείχου προστασίας σας, παρακαλούμε ανατρέξτε στο *"Firewall"* (p. 123).

ADVANCED THREAT DEFENSE

Το Advanced Threat Defense προστατεύει ενεργά το σύστημά σας από απειλές, όπως ransomware, spyware και trojans, αναλύοντας τη συμπεριφορά όλων των εγκατεστημένων εφαρμογών. Οι ύποπτες διεργασίες εντοπίζονται και, όταν είναι απαραίτητο, αποκλείονται.

Για περισσότερες πληροφορίες σχετικά με τον τρόπο προστασίας του συστήματός σας από απειλές, ανατρέξτε στο *"Advanced Threat Defense"* (p. 108).

ΠΡΟΣΤΑΣΙΑ ΑΠΟ SPAM

Η ενότητα antispam του Bitdefender εξασφαλίζει ότι τα Εισερχόμενα σας απαλλάσσονται των ανεπιθύμητων e-mails από το φιλτράρισμα της POP3 κυκλοφορίας ηλεκτρονικού ταχυδρομείου.

Για περισσότερες πληροφορίες σχετικά με την προστασία antispam, παρακαλούμε ανατρέξτε στο *"Antispam"* (p. 113).

ΕΥΠΑΘΕΙΕΣ

Η ενότητα ευπάθειας σάς βοηθά να διατηρείτε ενημερωμένο το λειτουργικό σύστημα και τις εφαρμογές που χρησιμοποιείτε τακτικά και να εντοπίζετε τα ανασφαλή ασύρματα δίκτυα στα οποία συνδέεστε. Κάντε κλικ στο **Άνοιγμα** στη μονάδα ευπάθειας για πρόσβαση στις δυνατότητές της.

Η δυνατότητα **Vulnerability Scan** σάς επιτρέπει να αναγνωρίζετε κρίσιμες ενημερώσεις των Windows, ενημερώσεις εφαρμογών, αδύναμους κωδικούς πρόσβασης που ανήκουν σε λογαριασμούς Windows και ασύρματα δίκτυα που δεν είναι ασφαλή. Κάντε κλικ στο **Έναρξη σάρωσης** για να πραγματοποιήσετε σάρωση στη συσκευή σας.

Κάντε κλικ στο **Wi-Fi Security Advisor** για να δείτε τη λίστα των ασύρματων δικτύων στα οποία συνδέεστε, μαζί με την αξιολόγηση της φήμης μας για καθένα από αυτά και τις ενέργειες που μπορείτε να κάνετε για να παραμείνετε ασφαλείς από πιθανές κατασκοπίες.

Για περισσότερες πληροφορίες σχετικά με τη ρύθμιση της προστασίας των ευπαθειών, ανατρέξτε στο *"ΕΥΠΑΘΕΙΑ"* (p. 129).

ΑΠΟΚΑΤΑΣΤΑΣΗ RANSOMWARE

Η δυνατότητα αποκατάστασης Ransomware σας βοηθά να ανακτήσετε αρχεία σε περίπτωση που κρυπτογραφηθούν απο ransomware.

Για περισσότερες πληροφορίες σχετικά με τον τρόπο ανάκτησης κρυπτογραφημένων αρχείων, ανατρέξτε στο *"Αποκατάσταση από Ransomware"* (p. 143).

Ιδιωτικότητα

Στην ενότητα Απόρρητο μπορείτε να ανοίξετε την εφαρμογή Bitdefender VPN, να κρυπτογραφήσετε τα προσωπικά σας δεδομένα, να προστατεύσετε τις ηλεκτρονικές σας συναλλαγές, να διατηρήσετε την κάμερα web και την εμπειρία περιήγησης ασφαλή και να προστατέψετε τα παιδιά σας με την προβολή και τον περιορισμό των online δραστηριοτήτων τους.

Τα χαρακτηριστικά που μπορείτε να διαχειριστείτε στην ενότητα Προστασία προσωπικών δεδομένων είναι:

VPN

Το VPN εξασφαλίζει την ηλεκτρονική σας δραστηριότητα και αποκρύπτει τη διεύθυνση IP κάθε φορά που συνδέεστε σε ασύρματα ασύρματα δίκτυα, ενώ βρίσκεστε σε αεροδρόμια, εμπορικά κέντρα, καφέ ή ξενοδοχεία. Επιπλέον, μπορείτε να αποκτήσετε πρόσβαση σε περιεχόμενο που κανονικά είναι περιορισμένο σε ορισμένες περιοχές.

Για περισσότερες πληροφορίες σχετικά με αυτή τη λειτουργία, παρακαλούμε ανατρέξτε στο *"VPN"* (p. 156).

ΒΙΝΤΕΟ & ΠΡΟΣΤΑΣΙΑ ΗΧΟΥ

Η προστασία βίντεο & ήχου κρατά την κάμερά σας εκτός κινδύνου αποκλείοντας την πρόσβαση των μη αξιόπιστων εφαρμογών και σας ειδοποιεί πότε οι εφαρμογές θα προσπαθήσουν να αποκτήσουν πρόσβαση στο μικρόφωνό σας.

Για περισσότερες πληροφορίες σχετικά με τον τρόπο προστασίας της κάμεράς σας από ανεπιθύμητη πρόσβαση και τον τρόπο ρύθμισης του Bitdefender για να σας ειδοποιήσει για τη δραστηριότητα του μικροφώνου σας, ανατρέξτε στο *"ΒΙΝΤΕΟ & ΠΡΟΣΤΑΣΙΑ ΗΧΟΥ"* (p. 138).

PASSWORD MANAGER

Ο Bitdefender Διαχειριστής Κωδικών Ασφαλείας σας βοηθά να παρακολουθείτε τους κωδικούς πρόσβασής σας, προστατεύει την ιδιωτικότητα σας και παρέχει μια ασφαλή εμπειρία περιήγησης.

Για περισσότερες πληροφορίες σχετικά με τη διαμόρφωση του Γονικού Συμβούλου, παρακαλούμε ανατρέξτε στο *"Προστασία των κωδικών σας με το Διαχειριστή Κωδικών Ασφαλείας"* (p. 145).

SAFEPAY

Το πρόγραμμα περιήγησης Bitdefender Safepay™ σας βοηθά να κρατήσετε απόρρητες και ασφαλείς τις ηλεκτρονικές τραπεζικές συναλλαγές σας, τις ηλεκτρονικές αγορές, καθώς και κάθε άλλου είδους ηλεκτρονική συναλλαγή.

Για περισσότερες πληροφορίες σχετικά με το Bitdefender Safepay™, παρακαλούμε ανατρέξτε στο "*Ασφάλεια Safepay για online συναλλαγές*" (p. 159).

ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ

Bitdefender Ο Γονικός έλεγχος σάς επιτρέπει να παρακολουθείτε τι κάνουν τα παιδιά σας στη συσκευή τους. Σε περίπτωση ακατάλληλου περιεχομένου, μπορείτε να αποφασίσετε να περιορίσετε την πρόσβαση του στο Διαδίκτυο ή σε συγκεκριμένες εφαρμογές.

Κάντε κλικ στο **Διαμόρφωση** στην μονάδα Γονικού Συμβούλου για να ξεκινήσετε τη ρύθμιση των συσκευών των παιδιών σας και να παρακολουθείτε τη δραστηριότητά τους όπου κι αν βρίσκεστε.

Για περισσότερες πληροφορίες σχετικά με τη ρύθμιση του γονικού ελέγχου, ανατρέξτε στο "*Γονικός Έλεγχος*" (p. 165).

ANTI-TRACKER

Η λειτουργία Anti-tracker σας βοηθά να αποφύγετε την παρακολούθηση, έτσι ώστε τα δεδομένα σας να παραμένουν ιδιωτικά κατά την περιήγησή σας στο διαδίκτυο, μειώνοντας ταυτόχρονα τον χρόνο που απαιτείται για τη φόρτωση των ιστότοπων.

Για περισσότερες πληροφορίες σχετικά με τη λειτουργία Anti-tracker, ανατρέξτε στο "*Anti-tracker*" (p. 153).

Εργαλεία

Στα ενότητα Βοηθητικά προγράμματα μπορείτε να βελτιώσετε την ταχύτητα του συστήματος »και να διαχειριστείτε τις συσκευές σας.

OneClick Optimizer

Το Bitdefender Total Security προσφέρει όχι μόνο ασφάλεια, αλλά σας βοηθά επίσης να διατηρήσετε την απόδοση της συσκευής σας σε φόρμα.

Το OneClick Optimizer θα σας βοηθήσει να βρείτε και να καταργήσετε περιττά αρχεία από τη συσκευή σας σε ένα εύκολο βήμα.

Για περισσότερες πληροφορίες σχετικά με αυτό, ανατρέξτε στο *"OneClick Optimizer"* (p. 190).

Anti-Theft

Bitdefender Η αντικλεπτική προστασία προστατεύει τη συσκευή και τα δεδομένα σας από κλοπή ή απώλεια. Σε περίπτωση τέτοιου συμβάντος, αυτό σας επιτρέπει να εντοπίσετε ή να κλειδώσετε τη συσκευή σας από απόσταση. Μπορείτε επίσης να εξαφανίσετε όλα τα δεδομένα που βρίσκονται στο σύστημά σας.

Το Bitdefender Anti-Theft προσφέρει τις ακόλουθες λειτουργίες:

- Απομακρυσμένος εντοπισμός
- Απομακρυσμένο Κλείδωμα
- Απομακρυσμένη Διαγραφή
- Απομακρυσμένη ειδοποίηση

Για περισσότερες πληροφορίες σχετικά με το πώς μπορείτε να διατηρήσετε το σύστημά σας μακριά από τα λάθος χέρια, παρακαλούμε ανατρέξτε στο *"Κατά της κλοπής συσκευής (Anti-Theft)"* (p. 178).

ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Το Bitdefender File Shredder σας βοηθά να διαγράψετε οριστικά τα δεδομένα αφαιρώντας τα από το σκληρό σας δίσκο.

Για περισσότερες πληροφορίες σχετικά με αυτό, ανατρέξτε στο *"ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ"* (p. 191).

Προφίλ

Οι καθημερινές δραστηριότητες εργασίας, όπως παρακολουθώντας ταινίες ή παίζοντας παιχνίδια μπορεί να προκαλέσουν επιβράδυνση του συστήματος, ειδικά αν εκτελούνται ταυτόχρονα με τις διαδικασίες ενημέρωσης των Windows και τις εργασίες συντήρησης.

Με το Bitdefender, μπορείτε τώρα να επιλέξετε και να εφαρμόσετε το προτιμώμενο προφίλ σας, το οποίο κάνει προσαρμογές του συστήματος που είναι κατάλληλες για την αύξηση της απόδοσης των συγκεκριμένων εγκατεστημένων εφαρμογών.

Για περισσότερες πληροφορίες σχετικά με αυτή τη λειτουργία, παρακαλούμε ανατρέξτε στο *"Προφίλ"* (p. 183).

2.2.5. Αλλάξτε τη γλώσσα του προϊόντος

Το περιβάλλον του Bitdefender είναι διαθέσιμο σε πολλές γλώσσες και μπορεί να αλλάξει ακολουθώντας τα παρακάτω βήματα:

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Γενικά**, κάντε κλικ στην επιλογή **Αλλαγή γλώσσας**.
3. Επιλέξτε τη γλώσσα που θέλετε από τη λίστα και στη συνέχεια, κάντε κλικ στο κουμπί **ΑΠΟΘΗΚΕΥΣΗ**.
4. Περιμένετε για να εφαρμοστούν οι νέες ρυθμίσεις.

2.3. Bitdefender Central

Bitdefender Central είναι η πλατφόρμα όπου έχετε πρόσβαση στις λειτουργίες και τις υπηρεσίες του προϊόντος στο διαδίκτυο και μπορείτε να εκτελείτε εξ αποστάσεως σημαντικές εργασίες στις συσκευές Bitdefender που είναι εγκατεστημένες. Μπορείτε να συνδεθείτε στον λογαριασμό σας Bitdefender από οποιαδήποτε συσκευή που είναι συνδεδεμένη στο διαδίκτυο μεταβαίνοντας στο https://central.bitdefender.com ή απευθείας από την εφαρμογή Bitdefender Central σε συσκευές Android και iOS.

Για να εγκαταστήσετε την Bitdefender Centralεφαρμογή στις συσκευές σας:

- **Σε Android** - αναζητήστε Bitdefender Central στο Google Play και στη συνέχεια κατεβάστε και εγκαταστήστε την εφαρμογή. Ακολουθήστε τα απαιτούμενα βήματα για να ολοκληρώσετε την εγκατάσταση.
- **Σε iOS** - αναζητήστε Bitdefender Central στο App Store και στη συνέχεια κάντε λήψη και εγκατάσταση της εφαρμογής. Ακολουθήστε τα απαιτούμενα βήματα για να ολοκληρώσετε την εγκατάσταση.

Μόλις έχετε πρόσβαση, μπορείτε να αρχίσετε να κάνετε τα εξής:

- Λήψη και εγκατάσταση του Bitdefender σε Windows, macOS, iOS και σε Android λειτουργικά συστήματα. Τα προϊόντα που διατίθενται για λήψη είναι:
  - Bitdefender Total Security
  - Bitdefender Antivirus για Mac
  - Bitdefender Mobile Security για Android
  - Bitdefender Mobile Security για iOS
  - Bitdefender Γονικός Έλεγχος
- Διαχειριστείτε και ανανεώστε τις Bitdefender συνδρομές σας.

- Προσθέστε νέες συσκευές στο δίκτυό σας και διαχειριστείτε τις από όπου κι αν βρίσκεστε.
- Προστατέψτε τις συσκευές δικτύου και τα δεδομένα τους από κλοπή ή απώλεια με το Anti-Theft.
- Διαμορφώστε τις ρυθμίσεις του Γονικού Ελέγχου για τις συσκευές των παιδιών σας για να ελέγχετε τη δραστηριότητά τους από όπου κι αν βρίσκεστε.

Πρόσβαση στο Bitdefender Central

Υπάρχουν διάφοροι τρόποι για να αποκτήσετε πρόσβαση στο Bitdefender Central:

- Από τη κεντρική διεπαφή του Bitdefender:
  1. Επιλέξτε**Ο λογαριασμός μου** στο μενού πλοήγησης του Bitdefender περιβάλλοντος.
  2. Κάντε κλικ στο **Μεταβείτε στο Bitdefender Central** .
  3. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
- Από τον πλοηγό σας:
  1. Ανοίξτε ένα πρόγραμμα περιήγησης σε οποιαδήποτε συσκευή με πρόσβαση στο Διαδίκτυο.
  2. Μετάβαση σε: https://central.bitdefender.com.
  3. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
- Από την Android ή iOS συσκευή σας:

  Ανοίξτε την Bitdefender Central εφαρμογή που έχετε εγκαταστήσει.

Σημείωση
Σε αυτό το υλικό παρέχονται οι επιλογές και οι οδηγίες που διατίθενται στην πλατφόρμα web.

2.3.1. 2-Factor Authentication

Η μέθοδος 2-Factor Authentication προσθέτει ένα πρόσθετο επίπεδο ασφαλείας στον Bitdefenderλογαριασμό σας, απαιτώντας έναν κωδικό επαλήθευσης εκτός από τα διαπιστευτήριά σας σύνδεσης. Έτσι θα

αποτρέψετε την υποκλοπή του λογαριασμού σας και θα προστατευτείτε από επιθέσεις.

Ενεργοποίηση 2-Factor Authentication

Ενεργοποιώντας το 2-Factor Authentication, ο Bitdefender λογαριασμός σας θα είναι πολύ πιο ασφαλής. Η ταυτότητά σας θα επαληθεύεται κάθε φορά που θα συνδεθείτε από διαφορετικές συσκευές,για να εγκαταστήσετε ένα από τα Bitdefender προϊόντα, να ελέγξτε την κατάσταση της συνδρομής σας ή να εκτελέστε απομακρυσμένα εργασίες στις συσκευές σας.

Για να ενεργοποιήσετε το 2-Factor Authentication:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο εικονίδιο στην επάνω δεξιά πλευρά της οθόνης.
3. Κάντε κλικ στο **Bitdefender Λογαριασμός** στο μενού.
4. Επιλέξτε την καρτέλα **Κωδικός και ασφάλεια**
5. Επιλέξτε **2-Factor Authentication**.
6. Κάντε κλικ στο κουμπί **ΕΝΑΡΞΗ ΤΩΡΑ**.

   Επιλέξτε μία από τις ακόλουθες μεθόδους:

   - **Εφαρμογή Authenticator** - χρησιμοποιήστε μια εφαρμογή ελέγχου ταυτότητας για να δημιουργήσετε έναν κωδικό κάθε φορά που θέλετε να συνδεθείτε στον Bitdefender λογαριασμό σας.

     Εάν θέλετε να χρησιμοποιήσετε μια εφαρμογή ελέγχου ταυτότητας, αλλά δεν είστε σίγουροι για το τι θα επιλέξετε, υπάρχει διαθέσιμη μια λίστα με τις εφαρμογές ελέγχου ταυτότητας που συστήνουμε.

     a. Κάντε κλικ στο κουμπί **ΧΡΗΣΙΜΟΠΟΙΗΣΤΕ ΤΗΝ ΕΦΑΡΜΟΓΗ AUTHENTICATOR** για να ξεκινήσετε.

     b. Για να συνδεθείτε σε μια συσκευή Android ή iOS, χρησιμοποιήστε τη συσκευή σας για να σαρώσετε τον QR κωδικό .

        Για να συνδεθείτε σε φορητό υπολογιστή ή επιτραπέζιο υπολογιστή, μπορείτε να προσθέσετε μη αυτόματα τον εμφανιζόμενο κώδικα.

        Κάντε κλικ στο **CONTINUE**.

     c. Εισαγάγετε τον κωδικό που παρέχεται από την εφαρμογή ή αυτόν που εμφανίζεται στο προηγούμενο βήμα και στη συνέχεια κάντε κλικ στο κουμπί **ΕΝΕΡΓΟΠΟΙΗΣΗ**.

- **E-mail** - κάθε φορά που συνδέεστε στο Bitdefender λογαριασμό σας, θα σταλεί στο εισερχόμενό σας email ένας κωδικός επαλήθευσης. στη συνέχεια πληκτρολογήστε τον κωδικό που λάβατε.

  a. Κάντε κλικ στο κουμπί **ΧΡΗΣΗ EMAIL** για να ξεκινήσετε.

  b. Ελέγξτε το email και πληκτρολογήστε τον παρεχόμενο κωδικό.

     Σημειώστε ότι έχετε πέντε λεπτά για να ελέγξετε τον email λογαριασμό και να πληκτρολογήσετε τον παραγόμενο κώδικα. Εάν λήξει ο χρόνος, θα πρέπει να δημιουργήσετε έναν νέο κωδικό ακολουθώντας τα ίδια βήματα.

  c. Κάντε κλικ στο κουμπί **ΕΝΕΡΓΟΠΟΙΗΣΗ**.

  d. Σας παρέχονται δέκα κωδικοί ενεργοποίησης. Μπορείτε να τους αντιγράψετε, να τους κατεβάσετε ή να εκτυπώσετε τη λίστα και να την χρησιμοποιήσετε σε περίπτωση που χάσετε το email ή δεν θα μπορείτε να συνδεθείτε. Κάθε κωδικός μπορεί να χρησιμοποιηθεί μόνο μία φορά.

  e. Κάντε κλικ στο κουμπί **ΟΛΟΚΛΗΡΩΣΗ**.

Σε περίπτωση που θέλετε να σταματήσετε να χρησιμοποιείτε το 2-Factor Authentication:

1. Κάντε κλικ στο κουμπί **ΑΠΕΝΕΡΓΟΠΟΙΗΣΗ 2-FACTOR AUTHENTICATION**
2. Ελέγξτε την εφαρμογή ή το email σας και πληκτρολογήστε τον κωδικό που λάβατε.

   Σημειώστε ότι έχετε πέντε λεπτά για να ελέγξετε τον email λογαριασμό σας και πληκτρολογήσετε τον παραγόμενο κώδικα. Εάν λήξει ο χρόνος, θα πρέπει να δημιουργήσετε έναν νέο κωδικό ακολουθώντας τα ίδια βήματα.
3. Επιβεβαιώστε την επιλογή σας.

Προσθήκη έμπιστης συσκευής

Για να βεβαιωθείτε ότι μόνο εσείς μπορείτε να αποκτήσετε πρόσβαση στο Bitdefender λογαριασμό σας, ίσως χρειαστεί πρώτα έναν κωδικό ασφαλείας. Εάν θέλετε να παραλείψετε αυτό το βήμα κάθε φορά που συνδέεστε από την ίδια συσκευή, σας συνιστούμε να την ορίσετε ως αξιόπιστη συσκευή.

Για να δηλώσετε συσκευές ως αξιόπιστες:

1. Πρόσβαση στο Bitdefender Central.

2. Κάντε κλικ στο εικονίδιο 👤 στην επάνω δεξιά πλευρά της οθόνης.
3. Κάντε κλικ στο **Bitdefender Λογαριασμός** στο μενού.
4. Επιλέξτε την καρτέλα **Κωδικός και ασφάλεια**
5. Κάντε κλικ στην επιλογή **Έμπιστες Συσκευές**.
6. Εμφανίζεται η λίστα με τις συσκευές όπου το Bitdefender που είναι εγκατεστημένο. Κάντε κλικ στην επιθυμητή συσκευή.

Μπορείτε να προσθέσετε όσες συσκευές επιθυμείτε, υπό την προϋπόθεση ότι έχει εγκατασταθεί το Bitdefender και η συνδρομή σας είναι έγκυρη.

2.3.2. Οι Συνδρομές μου

Η Bitdefender Central πλατφόρμα σας δίνει τη δυνατότητα να διαχειριστείτε εύκολα τις συνδρομές που έχετε για όλες τις συσκευές σας.

Ελέγξτε τις διαθέσιμες συνδρομές

Για να ελέγξετε τις διαθέσιμες συνδρομές σας:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε τον πίνακα **Οι συνδρομές μου**.

Εδώ έχετε πληροφορίες σχετικά με τη διαθεσιμότητα των συνδρομών που έχετε στην κατοχή σας και τον αριθμό των συσκευών που χρησιμοποιούν κάθε μία από αυτές.

Μπορείτε να προσθέσετε μια νέα συσκευή σε μια συνδρομή ή να την ανανεώσετε, επιλέγοντας μια κάρτα συνδρομής.

Σημείωση
Μπορείτε να έχετε μία ή περισσότερες συνδρομές στο λογαριασμό σας, υπό την προϋπόθεση ότι πρόκειται για διαφορετικές πλατφόρμες (Windows, Mac OS X, iOS ή Android).

Προσθέστε μια νέα συσκευή

Εάν η συνδρομή σας καλύπτει περισσότερες από μία συσκευή, μπορείτε να προσθέσετε μια νέα συσκευή και να εγκαταστήσετε το Bitdefender Total Security σε αυτή, με τον ακόλουθο τρόπο:

1. Πρόσβαση στο Bitdefender Central.

2. Επιλέξτε το **Οι συσκευές μου** και στην συνέχεια κάντε κλικ **ΕΓΚΑΤΑΣΤΑΣΗ ΠΡΟΣΤΑΣΙΑΣ** .
3. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:
   - **Προστατέψτε αυτή τη συσκευή**

     Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.
   - **Προστασία άλλων συσκευών**

     Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.

     Επιλέξτε **ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΛΗΨΗΣ**. Πληκτρολογήστε μια διεύθυνση ηλεκτρονικού ταχυδρομείου στο αντίστοιχο πεδίο και κάντε κλικ στην επιλογή **ΑΠΟΣΤΟΛΗ EMAIL** . Λάβετε υπόψη ότι ο παραγόμενος σύνδεσμος λήψης ισχύει μόνο για τις επόμενες 24 ώρες. Εάν λήξει ο σύνδεσμος, θα πρέπει να δημιουργήσετε ένα νέο, ακολουθώντας τα ίδια βήματα.

     Στην συσκευή που θέλετε να εγκαταστήσετε το Bitdefender προιόν, ελέγξτε το λογαριασμό ηλεκτρονικού ταχυδρομείου που πληκτρολογήσατε και στην συνέχεια κάντε κλικ στο αντίστοιχο κουμπί λήψης.
4. Περιμένετε να ολοκληρωθεί η λήψη, στη συνέχεια, εκτελέστε το πρόγραμμα εγκατάστασης.

Παράταση συνδρομής

Εάν δεν έχετε επιλέξει την αυτόματη ανανέωση της συνδρομής Bitdefender, μπορείτε να την ανανεώσετε χειροκίνητα, ακολουθώντας τα παρακάτω βήματα:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε τον πίνακα **Οι συνδρομές μου**.
3. Επιλέξτε την επιθυμητή κάρτα συνδρομής.
4. Κάντε κλικ στο **Ανανέωση** για να συνεχίσετε.

Μια ιστοσελίδα ανοίγει στο πρόγραμμα πλοήγησης σας, όπου μπορείτε να ανανεώσετε τη Bitdefender συνδρομή σας.

Ενεργοποίηση συνδρομής

Μια συνδρομή μπορεί να ενεργοποιηθεί κατά τη διάρκεια της διαδικασίας εγκατάστασης χρησιμοποιώντας τον λογαριασμό σας Bitdefender. Μαζί με την διαδικασία ενεργοποίησης, αρχίζει και η αντίστροφη μέτρηση της διάρκειας ισχύος.

Αν έχετε αγοράσει ένα κωδικό ενεργοποίησης από έναν από τους μεταπωλητές μας ή σας τον έκαναν δώρο, τότε μπορείτε να προσθέσετε τη διάρκεια της συνδρομής στην δική σας Bitdefender συνδρομή , με την προϋπόθεση ότι και οι δυο είναι για το ίδιο προϊόν.

Για να ενεργοποιήσετε μια συνδρομή χρησιμοποιώντας έναν κωδικό ενεργοποίησης:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε τον πίνακα **Οι συνδρομές μου**.
3. Κάντε κλικ στο κουμπί **ΚΩΔΙΚΟΣ ΕΝΕΡΓΟΠΟΙΗΣΗΣ**, στη συνέχεια, πληκτρολογήστε τον κωδικό στο αντίστοιχο πεδίο.
4. Κάντε κλικ στο **ΕΝΕΡΓΟΠΟΙΗΣΗ** για να συνεχίσετε.

Η συνδρομή ενεργοποιήθηκε. Μεταβείτε στο **Οι Συσκευές μου** και επιλέξτε **ΕΓΚΑΤΑΣΤΑΣΗ ΠΡΟΣΤΑΣΙΑΣ** για να εγκαταστήσετε το προϊόν σε μία από τις συσκευές σας.

2.3.3. Οι συσκευές μου

Η περιοχή **Οι συσκευές μου** στο Bitdefender Central σας δίνει τη δυνατότητα να εγκαταστήσετε, να διαχειριστείτε και να ολοκληρώσετε ενέργειες εξ αποστάσεως στο Bitdefender σε οποιαδήποτε συσκευή, υπό την προϋπόθεση ότι είναι ενεργοποιημένη και συνδεδεμένη στο Internet. Οι κάρτες συσκευής εμφανίζουν το όνομα της συσκευής, την κατάσταση προστασίας και αν υπάρχουν κίνδυνοι ασφαλείας που επηρεάζουν την προστασία των συσκευών σας.

Για να δείτε μια λίστα με τις συσκευές σας ταξινομημένες ανάλογα με την κατάστασή τους ή τους χρήστες τους, κάντε κλικ στο βέλος που βρίσκεται στην επάνω δεξιά γωνία της οθόνης.

Για να εντοπίσετε εύκολα τις συσκευές σας, μπορείτε να προσαρμόσετε το όνομα της συσκευής:

1. Πρόσβαση στο Bitdefender Central.

2. Επιλέξτε το **Οι συσκευές μου**.
3. Πατήστε την επιθυμητή κάρτα συσκευής και, στη συνέχεια, το εικονίδιο ⋮ στην επάνω δεξιά γωνία της οθόνης.
4. Επιλέξτε **Ρυθμίσεις**.
5. Πληκτρολογήστε ένα νέο όνομα στο πεδίο **Όνομα συσκευής** και, στη συνέχεια, επιλέξτε **ΑΠΟΘΗΚΕΥΣΗ**.

Μπορείτε να δημιουργήσετε και να ορίσετε έναν ιδιοκτήτη σε κάθε μία από τις συσκευές σας για καλύτερη διαχείριση:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το **Οι συσκευές μου**.
3. Πατήστε την επιθυμητή κάρτα συσκευής και, στη συνέχεια, το εικονίδιο ⋮ στην επάνω δεξιά γωνία της οθόνης.
4. Επιλέξτε **Προφίλ**.
5. Επιλέξτε **Προσθήκη κατόχου** και στη συνέχεια συμπληρώστε τα αντίστοιχα πεδία. Προσαρμόστε το προφίλ προσθέτοντας μια φωτογραφία και επιλέγοντας μια ημερομηνία γέννησης.
6. Κάντε κλικ στο **ΠΡΟΣΘΗΚΗ** για να αποθηκεύσετε ένα προφίλ.
7. Επλέξτε τον επιθυμητό ιδιοκτήτη από τη λίστα **Ιδιοκτήτης συσκευής** και στη συνέχεια κάντε κλικ στο **ΑΝΤΙΣΤΟΙΧΙΣΗ**.

Για να ενημερώσετε από απόσταση το Bitdefender σε μια συσκευή των Windows:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το **Οι συσκευές μου**.
3. Πατήστε την επιθυμητή κάρτα συσκευής και, στη συνέχεια, το εικονίδιο ⋮ στην επάνω δεξιά γωνία της οθόνης.
4. Επιλέξτε **Αναβάθμιση**.

Για περισσότερες ενέργειες εξ αποστάσεως και πληροφορίες σχετικά με το Bitdefender προϊόν σας σε μια συγκεκριμένη συσκευή, κάντε κλικ στην επιθυμητή κάρτα συσκευής.

Μόλις κάνετε κλικ σε μια κάρτα συσκευής, οι ακόλουθες καρτέλες είναι διαθέσιμες:

- **Ταμπλώ**. Σε αυτό το παράθυρο μπορείτε να δείτε λεπτομέρειες σχετικά με την επιλεγμένη συσκευή, να ελέγξετε την κατάσταση προστασίας, την κατάσταση του Bitdefender VPN και πόσες απειλές έχουν αποκλειστεί τις τελευταίες επτά ημέρες. Η κατάσταση προστασίας μπορεί να είναι πράσινη, όταν δεν υπάρχει κανένα πρόβλημα που να επηρεάζει τη συσκευή σας, κίτρινη όταν η συσκευή σας χρειαστεί την προσοχή σας ή κόκκινη όταν η συσκευή κινδυνεύει. Όταν υπάρχουν ζητήματα που επηρεάζουν τη συσκευή σας, κάντε κλικ στο αναπτυσσόμενο βέλος στην επάνω περιοχή κατάστασης για να μάθετε περισσότερες λεπτομέρειες. Από εδώ μπορείτε να διορθώσετε χειροκίνητα ζητήματα που επηρεάζουν την ασφάλεια των συσκευών σας.
- **ΠΡΟΣΤΑΣΙΑ**. Από αυτό το παράθυρο μπορείτε να εκτελέσετε μια Γρήγορη ή μια Απομακρυσμένη Σάρωση Συστήματος στις συσκευές σας. Κάντε κλικ στο κουμπί **ΣΑΡΩΣΗ** για να ξεκινήσει η διαδικασία. Μπορείτε επίσης να ελέγξετε πότε πραγματοποιήθηκε η τελευταία σάρωση στη συσκευή καθώς και μία διαθέσιμη αναφορά της τελευταίας σάρωσης με τις πιο σημαντικές πληροφορίες.Για περισσότερες πληροφορίες σχετικά με αυτές τις δύο διεργασίες, παρακαλούμε ανατρέξτε στο “*Εκτέλεση Σάρωσης Συστήματος*” και στο "*Εκτέλεση γρήγορης σάρωσης*" (p. 93).
- **Optimizer**. Εδώ μπορείτε να βελτιώσετε εξ αποστάσεως τις επιδόσεις μιας συσκευής με μια γρήγορη σάρωση, ανίχνευση και καθαρισμό άχρηστων αρχείων. Κάντε κλικ στο κουμπί **ΕΚΚΙΝΗΣΗ**, και στη συνέχεια επιλέξτε τις περιοχές που θέλετε να βελτιστοποιήσετε. Κάντε κλικ ξανά στο κουμπί **ΕΝΑΡΞΗ** για να ξεκινήσει η διαδικασία βελτιστοποίησης. Κάντε κλικ στο **More details** για να αποκτήσετε πρόσβαση σε μια λεπτομερή έκθεση σχετικά με τα θέματα που βρέθηκαν.
- **Anti-theft**. Σε περίπτωση προσωρινής απώλειας, κλοπής ή απώλειας, με τη λειτουργία Anti-Theft μπορείτε να εντοπίσετε τη συσκευή σας και να προβείτε σε εξ αποστάσεως ενέργειες. Κάντε κλικ στο **ΕΝΤΟΠΙΣΜΟΣ** για να μάθετε τη θέση της συσκευής. Η τελευταία γνωστή θέση θα εμφανιστεί, μαζί με την ώρα και την ημερομηνία. Για περισσότερες λεπτομέρειες σχετικά με αυτή τη δυνατότητα, ανατρέξτε στο "*Κατά της κλοπής συσκευής (Anti-Theft)*" (p. 178).
- **Ευπάθεια**. Για να ελέγξετε μια συσκευή για ευπάθειες όπως για ενημερώσεις Windows που λείπουν, παρωχημένες εφαρμογές, ή

αδύναμους κωδικούς πρόσβασης, κάντε κλικ στο κουμπί **ΣΑΡΩΣΗ** στην καρτέλα Ευπάθεια. Οι Ευπάθειες δεν μπορούν να διορθωθούν εξ αποστάσεως. Σε περίπτωση που βρεθεί κάποια ευπάθεια, θα πρέπει να εκτελέσετε μια νέα σάρωση στη συσκευή και στη συνέχεια να λάβετε τις προτεινόμενες ενέργειες. Κάντε κλικ **More details** για να αποκτήσετε πρόσβαση σε μια λεπτομερή έκθεση σχετικά με τα θέματα που βρέθηκαν. Για περισσότερες λεπτομέρειες σχετικά με αυτή τη δυνατότητα, ανατρέξτε στο "*ΕΥΠΑΘΕΙΑ*" (p. 129).

2.3.4. Δραστηριότητα

Στην περιοχή Δραστηριότητα έχετε πρόσβαση στις πληροφορίες σχετικά με τις συσκευές που έχουν εγκαταστήσει το Bitdefender.

Μόλις αποκτήσετε πρόσβαση στο παραθύρο **Δραστηριότητα**, θα είναι διαθέσιμες οι ακόλουθες κάρτες :

- **Οι συσκευές μου**. Εδώ μπορείτε να δείτε τον αριθμό των συνδεδεμένων συσκευών μαζί με την κατάσταση προστασίας τους. Για να διορθώσετε τα ζητήματα εξ αποστάσεως στις συσκευές που εντοπίστηκαν, κάντε κλικ στο κουμπί **Επίλυση προβλημάτων** και, στη συνέχεια, κάντε κλικ στο κουμπί **Σάρωση και επίλυση προβλημάτων**.

  Για να δείτε λεπτομέρειες σχετικά με τα εντοπισμένα προβλήματα, κάντε κλικ στο **Προβολή προβλημάτων** .

  Δεν είναι δυνατή η ανάκτηση πληροφοριών σχετικά με τις απειλές που ανιχνεύθηκαν σε iOS συσκευές.

- **Αποκλεισμένες απειλές**. Εδώ μπορείτε να δείτε ένα γράφημα που παρουσιάζει ένα συνολικό στατιστικό στοιχείο, συμπεριλαμβανομένων των πληροφοριών για τις απειλές που αποκλείστηκαν κατά τις τελευταίες 24 ώρες και επτά ημέρες. Οι πληροφορίες που εμφανίζονται ανακτώνται ανάλογα με την κακόβουλη συμπεριφορά που εντοπίζεται στα αρχεία, τις εφαρμογές και τις διευθύνσεις URL που αποκτήθηκε πρόσβαση.

- **Οι κορυφαίοι χρήστες με αποκλεισμένες απειλές**. Εδώ μπορείτε να δείτε τους χρήστες όπου βρέθηκαν οι περισσότερες απειλές.

- **Οι κορυφαίες συσκευές με αποκλεισμένες απειλές**. Εδώ μπορείτε να δείτε τις συσκευές όπου βρέθηκαν οι περισσότερες απειλές.

2.3.5. Ειδοποιήσεις

Για να σας να είστε ενήμεροι για το τι συμβαίνει στις ενεργοποιημένες συσκευές σας, υπάρχει το 🔔 εικονίδιο. Μόλις το επιλέξετε θα εμφανιστεί μία οθόνη με πληροφορίες σχετικά με την δραστηριότητα των Bitdefender προϊόντων που είναι εγκατεστημηνένα στις συσκευές σας.

2.4. Διατηρώντας το Bitdefender ενημερωμένο με τις πιο πρόσφατες ενημερώσεις

Νέες απειλές ανιχνεύεται και προσδιορίζονται κάθε μέρα. Αυτός είναι ο λόγος για τον οποίο είναι πολύ σημαντικό να ενημερώνεται το Bitdefender με την τελευταία βάση δεδομένων πληροφοριών απειλών.

Αν είστε συνδεδεμένοι στο Internet μέσω ευρυζωνικής ή DSL σύνδεσης, το Bitdefender φροντίζει το ίδιο τον εαυτό του. Από προεπιλογή, ελέγχει για ενημερώσεις όταν ενεργοποιείτε τη συσκευή σας και κάθε **ώρα** μετά από αυτήν. Εάν εντοπιστεί μια ενημέρωση, πραγματοποιείται αυτόματη λήψη και εγκατάσταση στη συσκευή σας.

Η διαδικασία ενημέρωσης εκτελείται on the fly (εν πτήσει), πράγμα που σημαίνει ότι τα αρχεία προς ενημέρωση αντικαθίστανται σταδιακά. Με τον τρόπο αυτό, η διαδικασία ενημέρωσης δεν θα επηρεάσει τη λειτουργία του προϊόντος και, ταυτόχρονα, οποιαδήποτε ευπάθεια θα αποκλείεται.

Σημαντικό
Για να προστατεύεστε από τις πιο πρόσφατες απειλές αφήστε ενεργή την επιλογή Automatic Update (Αυτόματη ενημέρωση)

Σε ορισμένες ειδικές περιπτώσεις, η παρέμβασή σας είναι απαραίτητη προκειμένου να διατηρηθεί η Bitdefender προστασία επικαιροποιημένη:

- Εάν η συσκευή σας συνδέεται στο Διαδίκτυο μέσω διακομιστή μεσολάβησης, πρέπει να διαμορφώσετε τις ρυθμίσεις διακομιστή μεσολάβησης όπως περιγράφεται στο *"Πώς μπορώ να ρυθμίσω το Bitdefender να χρησιμοποιήσει μια σύνδεση διακομιστή μεσολάβησης (proxy) του Internet;"* (p. 79).
- Αν είστε συνδεδεμένοι στο Internet μέσω μιας dial up σύνδεσης, τότε συνιστάται να ενημερώνετε τακτικά το Bitdefender με αίτημα του χρήστη. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Εκτελώντας ενημέρωση"* (p. 43).

2.4.1. Έλεγχος αν το Bitdefender είναι επικαιροποιημένο με τις τελευταίες ενημερώσεις

Για να ελέγξετε την ώρα της τελευταίας ενημέρωσης του Bitdefender:

1. Πατήστε **Ειδοποιήσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **All**, επιλέξτε την ειδοποίηση που αφορά την τελευταία ενημέρωση.

Μπορείτε να μάθετε πότε ξεκίνησαν οι ενημερώσεις καθώς και πληροφορίες σχετικά με αυτές (αν ήταν επιτυχημένη ή όχι η ενημέρωση, αν απαιτείται επανεκκίνηση για την ολοκλήρωση της εγκατάστασης). Εάν είναι απαραίτητο, κάντε επανεκκίνηση του συστήματος σας όσο το δυνατόν συντομότερα.

2.4.2. Εκτελώντας ενημέρωση

Προκειμένου να γίνουν ενημερώσεις, μια σύνδεση στο Internet είναι απαραίτητη.

Για να ξεκινήσετε μια ενημέρωση, κάντε δεξί κλικ στο εικονίδιο τουBitdefender στο system tray, και μετά επιλέξτε**Ενημέρωση τώρα**.

Η λειτουργία "Ενημέρωση" θα συνδεθεί στον Bitdefender update server και θα ελέγξει για ενημερώσεις. Αν μια ενημερωμένη έκδοση έχει εντοπιστεί, θα σας ζητηθεί να επιβεβαιώσετε τη λήψη ή η ενημέρωση θα γίνεται αυτόματα, ανάλογα με τις ρυθμίσεις ενημέρωσης .

Σημαντικό
Ίσως χρειαστεί να κάνετε επανεκκίνηση της συσκευής όταν ολοκληρώσετε την ενημέρωση. Σας συνιστούμε να γίνει το συντομότερο δυνατόν.

Μπορείτε επίσης να πραγματοποιήσετε ενημερώσεις εξ αποστάσεως, στις συσκευές σας, με την προϋπόθεση ότι είναι ενεργοποιημένες και συνδεδεμένες στο internet.

Για να ενημερώσετε από απόσταση το Bitdefender σε μια συσκευή των Windows:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το **Οι συσκευές μου**.

3. Πατήστε την επιθυμητή κάρτα συσκευής και, στη συνέχεια, το εικονίδιο ⋮ στην επάνω δεξιά γωνία της οθόνης.
4. Επιλέξτε **Αναβάθμιση**.

2.4.3. Ενεργοποίηση ή απενεργοποίηση αυτόματης ενημέρωσης

Για να ενεργοποιήσετε ή απενεργοποιήσετε την αυτόματη ενημέρωση:

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Επιλέξτε την καρτέλα **Update**.
3. Ενεργοποιήστε ή απενεργοποιήστε τον αντίστοιχο διακόπτη.
4. Ένα παράθυρο προειδοποίησης εμφανίζεται. Θα πρέπει να επιβεβαιώσετε την επιλογή σας επιλέγοντας από το μενού το χρόνο απενεργοποίησης της αυτόματης ενημέρωσης. Μπορείτε να απενεργοποιήσετε την αυτόματη ενημέρωση για 5, 15 ή 30 λεπτά, για μια ώρα ή μέχρι να γίνει επανεκκίνηση του συστήματος.

Προειδοποίηση

Αυτό είναι ένα κρίσιμο ζήτημα ασφάλειας. Σας συνιστούμε να απενεργοποιήσετε την αυτόματη ενημέρωση για τον ελάχιστο δυνατό χρόνο, εφόσον είναι αναγκαία η απενεργοποίηση. Εάν το Bitdefender δεν ενημερώνεται τακτικά, δεν θα είναι σε θέση να σας προστατεύσει από τις πιο πρόσφατες απειλές.

2.4.4. Προσαρμογή των ρυθμίσεων ενημέρωσης / επικαιροποίησης

Οι ενημερώσεις μπορούν να εκτελεστούν από το τοπικό δίκτυο, μέσω του Διαδικτύου, απευθείας ή μέσω ενός διακομιστή μεσολάβησης. Από προεπιλογή, το Bitdefender θα ελέγχει για ενημερώσεις κάθε ώρα, μέσω του Διαδικτύου, και θα εγκαθιστά τις διαθέσιμες ενημερώσεις χωρίς προειδοποίηση σας.

Οι προεπιλεγμένες ρυθμίσεις ενημέρωσης είναι κατάλληλη για τους περισσότερους χρήστες και κανονικά δεν θα χρειαστεί να τις αλλάξετε.

Για να προσαρμόσετε τις ρυθμίσεις ενημέρωσης:

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.

2. Επιλέξτε την καρτέλα **Update** και προσαρμόστε τις ρυθμίσεις σύμφωνα με τις προτιμήσεις σας.

Συχνότητα Ενημερώσεων

Το Bitdefender έχει ρυθμιστεί να ελέγχει για ενημερώσεις κάθε ώρα. Για να αλλάξετε τη συχνότητα ενημέρωσης, σύρετε το ρυθμιστικό(slider) κατά μήκος της γραμμής κλίμακας για να ορίσετε το επιθυμητό χρονικό διάστημα που θα πρέπει να γίνεται η ενημέρωση.

Κανόνες διαδικασίας ενημέρωσης

Κάθε φορά που είναι διαθέσιμη μια ενημέρωση, το Bitdefender θα πραγματοποιήσει αυτόματη λήψη και εφαρμογή της ενημέρωσης χωρίς να εμφανίζει ειδοποιήσεις. Απενεργοποιήστε την επιλογή **Silent update** εάν θέλετε να ενημερώνεστε κάθε φορά που είναι διαθέσιμη μια νέα ενημέρωση.

Ορισμένες ενημερώσεις απαιτούν επανεκκίνηση για να ολοκληρωθεί η εγκατάσταση.

Από προεπιλογή, εάν μια ενημέρωση απαιτεί επανεκκίνηση, το Bitdefender θα συνεχίσει να λειτουργεί με τα παλιά αρχεία έως ότου ο χρήστης επανεκκινήσει οικειοθελώς τη συσκευή. Η πρόνοια αυτή έχει ληφθεί για να αποφευχθεί η εμπλοκή της διαδικασίας ενημέρωσης του Bitdefender με την εργασία του χρήστη.

Εάν θέλετε να σας ζητηθεί όταν μια ενημέρωση απαιτεί επανεκκίνηση, ενεργοποιήστε το **Επανεκκίνηση ειδοποίησης**.

2.4.5. Συνεχείς ενημερώσεις

Για να βεβαιωθείτε ότι χρησιμοποιείτε την πιο πρόσφατη έκδοση, το Bitdefender ελέγχει αυτόματα για product updates. Αυτές οι ενημερώσεις ενδέχεται να φέρνουν νέες λειτουργίες και βελτιώσεις, να διορθώνουν προβλήματα προϊόντων ή να σας αναβαθμίζουν αυτόματα σε μια νέα έκδοση. Όταν η νέα έκδοση Bitdefender έρχεται μέσω ενημέρωσης, αποθηκεύονται προσαρμοσμένες ρυθμίσεις και παραλείπεται η διαδικασία απεγκατάστασης και επανεγκατάστασης.

Αυτές οι ενημερώσεις απαιτούν επανεκκίνηση του συστήματος, προκειμένου να ξεκινήσει η εγκατάσταση των νέων αρχείων. Όταν η ενημέρωση έκδοση του προϊόντος ολοκληρωθεί, ένα παράθυρο θα σας

ενημερώσει για την επανεκκίνηση του συστήματος. Εάν παραλείψετε αυτήν την ειδοποίηση, μπορείτε είτε να κάνετε κλικ στο **ΕΠΑΝΕΚΚΙΝΗΣΗ ΤΩΡΑ** στο παράθυρο Ειδοποιήσεις όπου αναφέρεται η πιο πρόσφατη ενημέρωση, ή να επανεκινήσετε χειροκίνητα το σύστημα.

Σημείωση

Οι ενημερώσεις, συμπεριλαμβανομένων των νέων λειτουργιών και βελτιώσεων, θα παραδίδονται μόνο σε χρήστες που έχουν εγκαταστήσει το Bitdefender 2020.

3. ΠΩΣ ΜΠΟΡΕΊΤΕ ΝΑ

3.1. Εγκατάσταση

3.1.1. Πώς μπορώ να εγκαταστήσω το Bitdefender σε μια δεύτερη συσκευή;

Εάν η συνδρομή που έχετε αγοράσει καλύπτει περισσότερες από μία συσκευές, μπορείτε να χρησιμοποιήσετε τον λογαριασμό σας Bitdefender για να ενεργοποιήσετε μία δεύτερη συσκευή.

Για να εγκαταστήσετε το Bitdefender σε μια δεύτερη συσκευή:

1. Επιλέξτε **Εγκατάσταση σε άλλη συσκευή** στην κάτω αριστερή γωνία του Bitdefender περιβάλλοντος.

   Εμφανίζεται ένα νέο παράθυρο στην οθόνη σας.

2. Επιλέξτε **ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΕΓΚΑΤΑΣΤΑΣΗΣ**.
3. Ακολουθήστε τα βήματα της οθόνης για να εγκαταστήσετε το Bitdefender.

Η νέα συσκευή στην οποία έχετε εγκαταστήσει το Bitdefender προϊόν θα εμφανιστεί στο Bitdefender Central ταμπλό.

3.1.2. Πώς μπορώ να επανεγκαταστήσω το Bitdefender;

Τυπικές περιπτώσεις εκ νέου εγκατάστασης του Bitdefender περιλαμβάνουν τα ακόλουθα:

- Επανεγκατάσταση του λειτουργικού συστήματος.
- Θέλετε να διορθώσετε ζητήματα που μπορεί να έχουν προκαλέσει επιβράδυνση και διακοπές.
- Το Bitdefender προϊόν σας δεν ξεκινά ή δεν λειτουργεί σωστά.

Σε περίπτωση που μία από τις αναφερόμενες καταστάσεις είναι η περίπτωσή σας, ακολουθήστε τα εξής βήματα:

- Στα **Windows 7**:

  1. Κάντε κλικ στην **Έναρξη** και οδηγηθείτε στο **Όλα τα προγράμματα**.
  2. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.

3. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ** στο παράθυρο που εμφανίζεται.
4. Πρέπει να κάνετε επανεκκίνηση της συσκευής για να ολοκληρώσετε τη διαδικασία.

- Στα **Windows 8 και στα Windows 8.1**:

1. Από την οθόνη Έναρξης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Πίνακας Ελέγχου" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του.
2. Κάντε κλικ στο **Κατάργηση εγκατάστασης προγράμματος** ή στο **Προγράμματα και δυνατότητες** .
3. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
4. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ** στο παράθυρο που εμφανίζεται.
5. Πρέπει να κάνετε επανεκκίνηση της συσκευής για να ολοκληρώσετε τη διαδικασία.

- Στα **Windows 10**:

1. Κάντε κλικ στο **Εκκίνηση**και στη συνέχεια, κάντε κλικ στην επιλογή Ρυθμίσεις.
2. Κάντε κλικ στο εικονίδιο **Σύστημα** στην περιοχή Ρυθμίσεις, στη συνέχεια, επιλέξτε **Χαρακτηριστικά εφαρμογών**.
3. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
4. Κάντε κλικ στο **Απεγκατάσταση** ξανά για να επιβεβαιώσετε την επιλογή σας.
5. Κάντε κλικ στο **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ**.
6. Πρέπει να κάνετε επανεκκίνηση της συσκευής για να ολοκληρώσετε τη διαδικασία.

Σημείωση

Ακολουθώντας αυτήν τη διαδικασία επανεγκατάστασης, οι προσαρμοσμένες ρυθμίσεις αποθηκεύονται και διατίθενται στο νέο εγκατεστημένο προϊόν.

Άλλες ρυθμίσεις μπορεί να επανέλθουν στην προεπιλεγμένη διαμόρφωσή τους.

3.1.3. Από πού μπορώ να μεταφορτώσω το Bitdefender προϊόν μου;

Μπορείτε να εγκαταστήσετε το Bitdefender από το δίσκο εγκατάστασης ή χρησιμοποιώντας το πρόγραμμα εγκατάστασης ιστού που μπορείτε να κατεβάσετε στη συσκευή σας από την πλατφόρμα Bitdefender Central.

Σημείωση

Πριν από την εκτέλεση του κιτ εγκατάστασης, συνιστάται να αφαιρέσετε οποιαδήποτε λύση ασφαλείας είναι εγκατεστημένη στο σύστημά σας. Όταν χρησιμοποιείτε περισσότερες από μία λύσεις ασφαλείας στην ίδια συσκευή, το σύστημα γίνεται ασταθές.

Για να εγκαταστήσετε το Bitdefender απο το Bitdefender Central:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το **Οι συσκευές μου** και στην συνέχεια κάντε κλικ **ΕΓΚΑΤΑΣΤΑΣΗ ΠΡΟΣΤΑΣΙΑΣ** .
3. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:

   - **Προστατέψτε αυτή τη συσκευή**

     Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.

   - **Προστασία άλλων συσκευών**

     Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.

     Επιλέξτε **ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΛΗΨΗΣ**. Πληκτρολογήστε μια διεύθυνση ηλεκτρονικού ταχυδρομείου στο αντίστοιχο πεδίο και κάντε κλικ στην επιλογή **ΑΠΟΣΤΟΛΗ EMAIL** . Λάβετε υπόψη ότι ο παραγόμενος σύνδεσμος λήψης ισχύει μόνο για τις επόμενες 24 ώρες. Εάν λήξει ο σύνδεσμος, θα πρέπει να δημιουργήσετε ένα νέο, ακολουθώντας τα ίδια βήματα.

     Στην συσκευή που θέλετε να εγκαταστήσετε το Bitdefender προιόν, ελέγξτε το λογαριασμό ηλεκτρονικού ταχυδρομείου που

πληκτρολογήσατε και στην συνέχεια κάντε κλικ στο αντίστοιχο κουμπί λήψης.

4. Εκτελέστε το Bitdefender προϊόν που έχετε κατεβάσει.

3.1.4. Πώς μπορώ να αλλάξω τη γλώσσα του Bitdefender;

Το περιβάλλον του Bitdefender είναι διαθέσιμο σε πολλές γλώσσες και μπορεί να αλλάξει ακολουθώντας τα παρακάτω βήματα:

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Γενικά**, κάντε κλικ στην επιλογή **Αλλαγή γλώσσας**.
3. Επιλέξτε τη γλώσσα που θέλετε από τη λίστα και στη συνέχεια, κάντε κλικ στο κουμπί **ΑΠΟΘΗΚΕΥΣΗ**.
4. Περιμένετε για να εφαρμοστούν οι νέες ρυθμίσεις.

3.1.5. Πώς μπορώ να χρησιμοποιήσω την συνδρομή Bitdefender μετά από μια αναβάθμιση των Windows;

Αυτή η κατάσταση εμφανίζεται όταν αναβαθμίζετε το λειτουργικό σας σύστημα και θέλετε να συνεχίσετε να χρησιμοποιείτε τη συνδρομή Bitdefender.

Εάν χρησιμοποιείτε μια προηγούμενη έκδοση του Bitdefender μπορείτε να αναβαθμίσετε, χωρίς χρέωση, στην τελευταία έκδοση του Bitdefender , ως εξής:

- Από προηγούμενη Bitdefender Antivirus έκδοση στην τελευταία διαθέσιμη Bitdefender Antivirus.
- Από προηγούμενη Bitdefender Internet Security έκδοση στην τελευταία διαθέσιμη Bitdefender Internet Security.
- Από προηγούμενη Bitdefender Total Security έκδοση στην τελευταία διαθέσιμη Bitdefender Total Security .

Υπάρχουν δύο περιπτώσεις όπου μπορεί να εμφανισθεί:

- Έχετε αναβαθμίσει το λειτουργικό σύστημα χρησιμοποιώντας την λειτουργία ενημέρωσης των Windows και παρατηρείτε ότι το Bitdefender δεν λειτουργεί.

  Σε αυτή την περίπτωση, θα χρειαστεί να επανεγκαταστήσετε το προιόν σας ακολουθώντας τα παρακάτω βήματα:

- Στα **Windows 7**:
  1. Κάντε κλικ στο **Εναρξη**, πηγαίνετε στο **Πίνακας Ελέγχου** και κάντε διπλό κλικ στο **Προγράμματα και Δυνατότητες** .
  2. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
  3. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ** στο παράθυρο που εμφανίζεται.
  4. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

     Ανοίξτε το interface του νέου σας εγκατεστημένου Bitdefender προϊόντος σας για να έχετε πρόσβαση στα χαρακτηριστικά του.
- Στα **Windows 8 και στα Windows 8.1**:
  1. Από την οθόνη Έναρξης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Πίνακας Ελέγχου" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του.
  2. Κάντε κλικ στο **Κατάργηση εγκατάστασης προγράμματος** ή στο **Προγράμματα και δυνατότητες** .
  3. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
  4. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ** στο παράθυρο που εμφανίζεται.
  5. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

     Ανοίξτε το interface του νέου σας εγκατεστημένου Bitdefender προϊόντος σας για να έχετε πρόσβαση στα χαρακτηριστικά του.
- Στα **Windows 10**:
  1. Κάντε κλικ στο **Εκκίνηση**και στη συνέχεια, κάντε κλικ στην επιλογή Ρυθμίσεις.
  2. Κάντε κλικ στο εικονίδιο **Σύστημα** στην περιοχή Ρυθμίσεις και στη συνέχεια επιλέξτε **Εφαρμογές**.

3. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
4. Κάντε κλικ στο **Απεγκατάσταση** ξανά για να επιβεβαιώσετε την επιλογή σας.
5. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ** στο παράθυρο που εμφανίζεται.
6. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

   Ανοίξτε το interface του νέου σας εγκατεστημένου Bitdefender προϊόντος σας για να έχετε πρόσβαση στα χαρακτηριστικά του.

Σημείωση

Ακολουθώντας αυτήν τη διαδικασία επανεγκατάστασης, οι προσαρμοσμένες ρυθμίσεις αποθηκεύονται και διατίθενται στο νέο εγκατεστημένο προϊόν. Άλλες ρυθμίσεις μπορεί να επανέλθουν στην προεπιλεγμένη διαμόρφωσή τους.

- Αλλάξατε το σύστημά σας και θέλετε να συνεχίσετε να χρησιμοποιείτε την προστασία Bitdefender. Ως εκ τούτου, θα πρέπει να εγκαταστήσετε ξανά το προϊόν χρησιμοποιώντας την πιο πρόσφατη διαθέσιμη έκδοση.

  Για την επίλυση αυτής της κατάστασης:

  1. Κατεβάστε το αρχείο εγκατάστασης:
     a. Πρόσβαση στο Bitdefender Central.
     b. Επιλέξτε το **Οι συσκευές μου** και στην συνέχεια κάντε κλικ **ΕΓΚΑΤΑΣΤΑΣΗ ΠΡΟΣΤΑΣΙΑΣ** .
     c. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:
        - **Προστατέψτε αυτή τη συσκευή**

          Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.
        - **Προστασία άλλων συσκευών**

Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.

Επιλέξτε **ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΛΗΨΗΣ**. Πληκτρολογήστε μια διεύθυνση ηλεκτρονικού ταχυδρομείου στο αντίστοιχο πεδίο και κάντε κλικ στην επιλογή **ΑΠΟΣΤΟΛΗ EMAIL** . Λάβετε υπόψη ότι ο παραγόμενος σύνδεσμος λήψης ισχύει μόνο για τις επόμενες 24 ώρες. Εάν λήξει ο σύνδεσμος, θα πρέπει να δημιουργήσετε ένα νέο, ακολουθώντας τα ίδια βήματα.

Στην συσκευή που θέλετε να εγκαταστήσετε το Bitdefender προιόν, ελέγξτε το λογαριασμό ηλεκτρονικού ταχυδρομείου που πληκτρολογήσατε και στην συνέχεια κάντε κλικ στο αντίστοιχο κουμπί λήψης.

2. Εκτελέστε το Bitdefender προϊόν που έχετε κατεβάσει.

Για περισσότερες πληροφορίες σχετικά με τη διαδικασία εγκατάστασης του Bitdefender, ανατρέξτε στο *"Εγκατάσταση του Bitdefender προιόντος σας"* (p. 4).

3.1.6. Πώς μπορώ να αναβαθμίσω στην πιο πρόσφατη Bitdefender έκδοση;

Από τώρα και στο εξής, είναι δυνατή η αναβάθμιση στην πιο πρόσφατη έκδοση χωρίς να ακολουθήσετε τη διαδικασία χειροκίνητης απεγκατάστασης και επανεγκατάστασης. Πιο συγκεκριμένα, το νέο προϊόν, συμπεριλαμβανομένων των νέων δυνατοτήτων και των σημαντικών βελτιώσεων του προϊόντος, παρέχεται μέσω της ενημέρωσης του προϊόντος και εάν έχετε ήδη μια ενεργή Bitdefender συνδρομή, το προϊόν ενεργοποιείται αυτόματα.

Εάν χρησιμοποιείτε την έκδοση 2020, μπορείτε να κάνετε αναβάθμιση στην πιο πρόσφατη έκδοση ακολουθώντας τα εξής βήματα:

1. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΚΙΝΗΣΗ ΤΩΡΑ** στην ειδοποίηση που λαμβάνετε με τις πληροφορίες αναβάθμισης. Εάν το χάσετε, μεταβείτε στο παράθυρο Ειδοποιήσεις, επιλέξτε την πιο πρόσφατη ενημέρωση κα, στη συνέχεια, κάντε κλικ στο κουμπί **ΕΠΑΝΕΚΙΝΗΣΗ ΤΩΡΑ**. Περιμένετε να γίνει επανεκκίνηση της συσκευής.

   Εμφανίζεται το παράθυρο **Τι νέο υπάρχει** με πληροφορίες σχετικά με τις βελτιωμένες και νέες λειτουργίες.

2. Κάντε κλικ στις συνδέσεις **Διαβάστε περισσότερα** για να ανακατευθυνθείτε στην ειδική σελίδα μας με περισσότερες λεπτομέρειες και χρήσιμα άρθρα.
3. Κλείστε το παράθυρο **Τι νέο υπάρχει** για να αποκτήσετε πρόσβαση στο interface της νέας εγκατεστημένης έκδοσης.

Οι χρήστες που επιθυμούν δωρεάν αναβάθμιση από το Bitdefender 2016 ή χαμηλότερη έκδοση στην πιο πρόσφατη έκδοση Bitdefender, πρέπει να αφαιρέσουν την τρέχουσα έκδοση τους από τον Πίνακα Ελέγχου και στη συνέχεια να πραγματοποιήσουν λήψη του πιο πρόσφατου αρχείου εγκατάστασης από το Bitdefender website στη παρακάτω διεύθυνση:https://www.bitdefender.com/Downloads/. Η ενεργοποίηση είναι δυνατή μόνο με έγκυρη συνδρομή.

3.2. Bitdefender Central

3.2.1. Πώς μπορώ να συνδεθώ στο Bitdefender λογαριασμό με άλλο λογαριασμό;

Έχετε δημιουργήσει ένα νέο Bitdefender λογαριασμό και θέλετε να το χρησιμοποιείτε από τώρα και στο εξής.

Για να συνδεθείτε επιτυχώς με έναν άλλο Bitdefender λογαριασμό:

1. Κάντε κλικ στο όνομα του λογαριασμού σας στο επάνω μέρος της διεπαφής Bitdefender.
2. Κάντε κλικ στο **Εναλλαγή λογαριασμού** στην επάνω δεξιά γωνία της οθόνης για να αλλάξετε τον λογαριασμό που είναι συνδεδεμένος στη συσκευή.
3. Πληκτρολογήστε την e-mail διεύθυνσή στο αντίστοιχο πεδίο και στη συνέχεια κάντε κλικ στο **ΕΠΟΜΕΝΟ**.
4. Εισάγετε τον κωδικό πρόσβασης και στη συνέχεια κάντε κλικ στο **ΣΥΝΔΕΣΗ**.

Σημείωση

Το Bitdefender προϊόν από τη συσκευή σας αλλάζει αυτόματα ανάλογα με τη συνδρομή που σχετίζεται με το νέο Bitdefender λογαριασμό.
Εάν δεν υπάρχει διαθέσιμη συνδρομή που σχετίζεται με το νέο Bitdefender λογαριασμό, ή αν επιθυμείτε να τη μεταφέρετε από τον προηγούμενο

λογαριασμό, μπορείτε να επικοινωνήσετε με τηνBitdefender για υποστήριξη, όπως περιγράφεται στην ενότητα *"Ζητήσετε βοήθεια"* (p. 345) .

3.2.2. Πώς μπορώ να απενεργοποιήσω τα μηνύματα βοήθειας του Bitdefender Central;

Για να σας βοηθήσουμε να καταλάβετε κάθε επιλογή του Bitdefender Central που σας είναι χρήσιμη, βοηθητικά μηνύματα εμφανίζονται στο ταμπλό.

Αν επιθυμείτε να σταματήσετε να βλέπετε αυτό το είδος των μηνυμάτων:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο εικονίδιο στην επάνω δεξιά πλευρά της οθόνης.
3. Κάντε κλικ στο **ο λογαριασμός μου** στο μενού.
4. Κάντε κλικ στο κουμπί **Ρυθμίσεις** στο μενού.
5. Απενεργοποιήστε την επιλογή **Turn on/off help messages**.

3.2.3. Ξέχασα τον κωδικό που έχω ορίσει για το Bitdefender λογαρισμό. Πώς μπορώ να το επαναφέρω;

Υπάρχουν δύο τρόποι για να αλλάξετε τον κωδικό του Bitdefender λογαριασμού:

- Από τη διεπαφή Bitdefender:
  1. Επιλέξτε**Ο λογαριασμός μου** στο μενού πλοήγησης του Bitdefender περιβάλλοντος.
  2. Κάντε κλικ **Αλλαγή λογαριασμού** στην επάνω δεξιά γωνία της οθόνης.

     Εμφανίζεται ένα νέο παράθυρο.
  3. Πληκτρολογήστε τη διεύθυνση email σας και κάντε κλικ στο **ΕΠΟΜΕΝΟ** .

     Εμφανίζεται ένα νέο παράθυρο.
  4. Κάντε κλικ στο κουμπί **Ξεχάσατε τον κωδικό;**.
  5. Κάντε κλικ στο κουμπί **Επόμενο**.
  6. Ελέγξτε τον email λογαριασμό, πληκτρολογήστε τον κωδικό ασφαλείας που λάβατε και στη συνέχεια κάντε κλικ στο κουμπί **ΕΠΟΜΕΝΟ**.

Εναλλακτικά, μπορείτε να κάνετε κλικ στο **Αλλαγή κωδικού πρόσβασης** στο email που σας στείλαμε.

7. Πληκτρολογήστε τον νέο κωδικό πρόσβασης που θέλετε να ορίσετε και στη συνέχεια πληκτρολογήστε τον ξανά. Κάντε κλικ στο **SAVE**.

- Από τον πλοηγό σας:

1. Μετάβαση σε: https://central.bitdefender.com.
2. Κάντε κλικ στην επιλογή **ΣΥΝΔΕΣΗ**.
3. Εισάγετε τη διεύθυνση e-mail σας, και επιλέξτε **ΕΠΟΜΕΝΟ**.
4. Κάντε κλικ στο κουμπί **Ξεχάσατε τον κωδικό;**.
5. Κάντε κλικ στο κουμπί **Επόμενο**.
6. Ελέγξτε το λογαριασμό e-mail σας και ακολουθήστε τις οδηγίες που παρέχονται για να ορίσετε έναν νέο κωδικό πρόσβασης για το Bitdefender λογαριασμό.

Για να αποκτήσετε πρόσβαση στο Bitdefender λογαριασμό σας από τώρα και στο εξής, πληκτρολογήστε την e-mail διεύθυνση σας και το νέο κωδικό πρόσβασης που μόλις δημιουργήσατε.

3.2.4. Πώς μπορώ να χειριστώ τις συνεδρίες σύνδεσης που σχετίζονται με τον Bitdefender λογαριασμό μου;

Στον Bitdefender λογαριαμσό έχετε την δυνατότητα να δείτε όλες τις πρόσφατες μη ενεργές και ενεργές συνεδρίες σύνδεσης που σχετίζονται με τις ενεργοποιημένες συσκευές σας. Επιπλέον, μπορείτε να αποσυνδεθείτε απομακρυσμένα με τα ακόλουθα βήματα:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο εικονίδιο 👤 στην επάνω δεξιά πλευρά της οθόνης.
3. Κάντε κλικ στο **Περίοδοι σύνδεσης** στο μενού διαφανειών.
4. Στην περιοχή **Ενεργές συνδέσεις**, επιλέξτε **ΑΠΟΣΥΝΔΕΣΗ** στην επιλογή δίπλα στη συσκευή που θέλετε να τερματίσετε την σύνδεση.

3.3. Έλεγχος με το Bitdefender

3.3.1. Πώς μπορώ να ελέγξω ένα αρχείο ή ένα φάκελο;

Ο ευκολότερος τρόπος για να ελέγξετε ένα αρχείο ή φάκελο είναι να κάντε δεξί κλικ στο αντικείμενο που θέλετε να ελέγξετε , να δείξτε στο Bitdefender και επιλέξτε **έλεγχος με Bitdefender** από το μενού.

Για να ολοκληρώσετε τον έλεγχο, ακολουθήστε τον οδηγό για ανίχνευση ιών. Το Bitdefender θα αναλάβει αυτόματα τις προτεινόμενες ενέργειες στα αρχεία που ανιχνεύτηκαν.

Εάν υπάρχουν παραμένουσες μη εξουδετερωμένες απειλές, θα σας ζητηθεί να επιλέξετε τις ενέργειες που πρέπει να εφαρμοστούν σε αυτές.

Τυπικές καταστάσεις που μπορεί να χρησιμοποιήσετε αυτή τη μέθοδο σάρωσης περιλαμβάνουν τις εξής:

- Υποπτεύεστε ότι ένα συγκεκριμένο αρχείο ή φάκελο είναι μολυσμένα.
- Κάθε φορά που θα κατεβάζετε αρχεία από το Internet τα οποία νομίζετε ότι μπορεί να είναι επικίνδυνα.
- Σαρώστε ένα κοινόχρηστο στοιχείο δικτύου πριν αντιγράψετε αρχεία στη συσκευή σας.

3.3.2. Πώς μπορώ να ελέγξω το σύστημά μου;

Για να εκτελέσετε μια πλήρη σάρωση του συστήματος:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Κάντε κλικ στο κουμπί **Εκτέλεση σάρωσης** δίπλα στο **Σάρωση συστήματος** .
4. Ακολουθείστε τον Οδηγό Σάρωσης Συστήματος για να ολοκληρωθεί η σάρωση. Το Bitdefender θα αναλάβει αυτόματα τις προτεινόμενες ενέργειες στα αρχεία που ανιχνεύτηκαν.

   Εάν υπάρχουν παραμένουσες μη εξουδετερωμένες απειλές, θα σας ζητηθεί να επιλέξετε τις ενέργειες που πρέπει να εφαρμοστούν σε αυτές. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Οδηγός σαρωτή Antivirus "* (p. 98).

3.3.3. Πώς μπορώ να προγραμματίσω μια σάρωση;

Μπορείτε να ρυθμίσετε το προϊόν Bitdefender για να ξεκινήσει η σάρωση σημαντικών τοποθεσιών συστήματος όταν δεν βρίσκεστε μπροστά της συσκευής.

Για να προγραμματίσετε μια σάρωση:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Κάντε κλικ στο ••• δίπλα στον τύπο σάρωσης που θέλετε να προγραμματίσετε, Σάρωση συστήματος ή Γρήγορη σάρωση, στο κάτω μέρος της διεπαφής και, στη συνέχεια, επιλέξτε **Επεξεργασία** .

   Εναλλακτικά, μπορείτε να δημιουργήσετε έναν τύπο σάρωσης που να ταιριάζει στις ανάγκες σας κάνοντας κλικ στο **+ Δημιουργία σάρωσης** δίπλα στο **Διαχείριση σάρωσης** .
4. Προσαρμόστε τη σάρωση σύμφωνα με τις ανάγκες σας και, στη συνέχεια, κάντε κλικ στο **Επόμενο** .
5. Επιλέξτε το πλαίσιο δίπλα στο **Επιλέξτε πότε θα προγραμματίσετε αυτήν την εργασία** .

   Επιλέξτε μία από τις αντίστοιχες επιλογές για να θέσετε ένα χρονοδιάγραμμα:

   - Κατά την εκκίνηση του συστήματος
   - Καθημερινά
   - Εβδομαδιαία
   - Μηνιαία

   Αν επιλέξετε Καθημερινά, Μηνιαία ή Εβδομαδιαία, σύρετε την μπάρα κατά μήκος της κλίμακας για να ορίσετε την επιθυμητή χρονική περίοδο κατά την έναρξη της προγραμματισμένης σάρωσης.

Εάν επιλέξετε να δημιουργήσετε μια νέα προσαρμοσμένη σάρωση, εμφανίζεται το παράθυρο **Σάρωση**. Από εδώ μπορείτε να επιλέξετε τις θέσεις που θέλετε να σαρωθούν.

3.3.4. Πώς μπορώ να δημιουργήσω μία εργασία προσαρμοσμένης σάρωσης;

Εάν θέλετε να σαρώσετε συγκεκριμένες τοποθεσίες στη συσκευή σας ή να διαμορφώσετε τις επιλογές σάρωσης, διαμορφώστε και εκτελέστε μια προσαρμοσμένη εργασία σάρωσης.

Για να δημιουργήσετε μια προσαρμοσμένη εργασία σάρωσης, ακολουθήστε την εξής διαδικασία:

1. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
2. Κάντε κλικ στο **+ Δημιουργία σάρωσης** δίπλα στο **Διαχείριση σαρώσεων** .
3. Στο πεδίο όνομα εργασίας, πληκτρολογήστε ένα όνομα για τη σάρωση, επιλέξτε τις τοποθεσίες που θέλετε να σαρώσετε και, στη συνέχεια, κάντε κλικ στο **ΕΠΟΜΕΝΟ** .
4. Διαμορφώστε αυτές τις γενικές επιλογές:
   - **Σάρωση εφαρμογών μόνο**. Μπορείτε να ορίσετε το Bitdefender για να σαρώσετε μόνο τις εφαρμογές που έχουν πρόσβαση.
   - **Προτεραιότητα στόχου σάρωσης**. Μπορείτε να επιλέξετε τον αντίκτυπο που θα πρέπει να έχει μια διαδικασία σάρωσης στην απόδοση του συστήματός σας.
     - Αυτόματα - Η προτεραιότητα της διαδικασίας σάρωσης θα εξαρτηθεί από τη δραστηριότητα του συστήματος. Για να βεβαιωθείτε ότι η διαδικασία σάρωσης δεν επηρεάζει τη δραστηριότητα του συστήματος, το Bitdefender θα αποφασίσει αν η διαδικασία σάρωσης θα πρέπει να εκτελείται με υψηλή ή χαμηλή προτεραιότητα.
     - Υψηλή - Η προτεραιότητα της διαδικασίας σάρωσης θα είναι υψηλή. Επιλέγοντας αυτή την επιλογή, θα επιτρέψετε σε άλλα προγράμματα να τρέξουν πιο αργά και να μειώσετε το χρόνο που απαιτείται για να ολοκληρωθεί η διαδικασία σάρωσης.
     - Χαμηλή - Η προτεραιότητα της διαδικασίας σάρωσης θα είναι χαμηλή. Επιλέγοντας αυτήν την επιλογή, θα επιτρέψετε σε άλλα προγράμματα να τρέξουν γρηγορότερα και να αυξήσουν το χρόνο που απαιτείται για να ολοκληρωθεί η διαδικασία σάρωσης.
   - **Ενέργειες μετά τη σάρωση**. Επιλέξτε την ενέργεια που πρέπει να κάνει το Bitdefender σε περίπτωση που δεν εντοπιστούν απειλές:

- Εμφάνιση παραθύρου Σύνοψης
- Τερματισμός λειτουργίας
- Κλείσιμο παράθυρου Σάρωσης

5. Εάν θέλετε να διαμορφώσετε λεπτομερώς τις επιλογές σάρωσης, κάντε κλικ στο κουμπί **Εμφάνιση προχωρημένων επιλογών**.

   Κάντε κλικ στο κουμπί **Next**. (Επόμενο)

6. Μπορείτε να ενεργοποιήσετε την επιλογή **Προγραμματισμός εργασίας σάρωσης** , εάν θέλετε, και στη συνέχεια να επιλέξετε πότε θα ξεκινήσει η προσαρμοσμένη σάρωση που δημιουργήσατε.

   - Κατά την εκκίνηση του συστήματος
   - Καθημερινά
   - Μηνιαία
   - Εβδομαδιαία

   Αν επιλέξετε Καθημερινά, Μηνιαία ή Εβδομαδιαία, σύρετε την μπάρα κατά μήκος της κλίμακας για να ορίσετε την επιθυμητή χρονική περίοδο κατά την έναρξη της προγραμματισμένης σάρωσης.

7. Κάντε κλικ στο **Αποθήκευση** για να αποθηκεύσετε τις ρυθμίσεις και να κλείσετε το παράθυρο διαμόρφωσης.

   Ανάλογα με τις θέσεις που πρέπει να σαρωθούν, η σάρωση μπορεί να πάρει λίγο χρόνο. Εάν εντοπιστούν απειλές κατά τη διάρκεια της διαδικασίας σάρωσης, θα σας ζητηθεί να επιλέξετε τις ενέργειες που θα ληφθούν σχετικά με τα εντοπισμένα αρχεία.

Αν θέλετε, μπορείτε να εκτελέσετε ξανά γρήγορα μια προηγούμενη προσαρμοσμένη σάρωση πατώντας την αντίστοιχη καταχώρηση στη λίστα διαθέσιμων σαρώσεων

3.3.5. Πώς μπορώ να εξαιρέσω ένα φάκελο από τη σάρωση;

Το Bitdefender επιτρέπει την εξαίρεση συγκεκριμένων αρχείων, φακέλων ή extensions αρχείων από τη σάρωση.

Οι εξαιρέσεις θα πρέπει να χρησιμοποιούνται από χρήστες που έχουν προχωρημένες γνώσεις πληροφορικής και μόνο στις ακόλουθες περιπτώσεις:

- Έχετε ένα φάκελο μεγάλου μεγέθους στο σύστημά σας, όπου κρατάτε ταινίες και μουσική.
- Έχετε μεγάλο χώρο αρχειοθέτησης στο σύστημά σας, όπου τηρείτε διάφορα δεδομένα.
- Τηρείτε φάκελο για εγκατάσταση διαφόρων τύπων λογισμικού και εφαρμογών για δοκιμαστική εγκατάσταση . Η σάρωση του φακέλου μπορεί να οδηγήσει σε απώλεια μερικών δεδομένων.

Για να προσθέσετε ένα φάκελο στη λίστα εξαιρέσεων:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Κάντε κλικ στην καρτέλα **Ρυθμίσεις** .
4. Κάντε κλικ στο **Διαχείριση εξαιρέσεων** .
5. Κάντε κλικ στο **+ Προσθήκη εξαίρεσης** .
6. Εισαγάγετε τη διαδρομή του φακέλου που θέλετε εκτός από τη σάρωση στο αντίστοιχο πεδίο.

   Εναλλακτικά, μπορείτε να πλοηγηθείτε στο φάκελο κάνοντας κλικ στο κουμπί περιήγησης στη δεξιά πλευρά της διεπαφής, επιλέξτε τον και κάντε κλικ στο **OK** .
7. Ενεργοποιήστε το διακόπτη δίπλα στη δυνατότητα προστασίας που δεν πρέπει να σαρώσει το φάκελο. Υπάρχουν τρεις επιλογές:
   - Antivirus
   - ONLINE ΠΡΟΛΗΨΗ ΑΠΕΙΛΩΝ
   - Advanced Threat Defense
8. Κάντε κλικ στο **Αποθήκευση** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

3.3.6. Τι πρέπει να κάνω όταν το Bitdefender εντόπισε ένα καθαρό αρχείο ως μολυσμένο;

Μπορεί να υπάρξουν περιπτώσεις όπου το Bitdefender εσφαλμένα χαρακτηρίζει ένα νόμιμο αρχείο ως απειλή (ψευδώς θετικά). Για να διορθώσετε αυτό το σφάλμα, προσθέστε το αρχείο στην περιοχή Εξαιρέσεων του Bitdefender :

1. Απενεργοποιήστε την σε πραγματικό χρόνο προστασία από τους ιούς του Bitdefender :
   a. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
   b. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
   c. Στο παράθυρο **Advanced** , απενεργοποιήστε το **Bitdefender Shield** .

      Ένα παράθυρο προειδοποίησης εμφανίζεται. Θα πρέπει να επιβεβαιώσετε την επιλογή σας επιλέγοντας από το μενού τη διάρκεια απενεργοποίησης της σε πραγματικό χρόνο προστασίας. Μπορείτε να απενεργοποιήσετε την προστασία πραγματικού χρόνου για 5, 15 ή 30 λεπτά, για μία ώρα, μόνιμα ή μέχρι μια επανεκκίνηση του συστήματος.
2. Εμφάνιση κρυφών αντικειμένων στα Windows. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο *"Εμφάνιση κρυφών αντικειμένων στα Windows."* (p. 81).
3. Επαναφορά αρχείου από την περιοχή Καραντίνας:
   a. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
   b. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
   c. Μεταβείτε στα παράθυρα **Ρυθμίσεις** και κάντε κλικ στο **Διαχείριση καραντίνας** .
   d. Επιλέξτε το αρχείο και, στη συνέχεια, κάντε κλικ στο **Επαναφορά** .
4. Προσθέστε το αρχείο στη λίστα Εξαιρέσεων. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο *"Πώς μπορώ να εξαιρέσω ένα φάκελο από τη σάρωση;"* (p. 60).

   Από προεπιλογή, το Bitdefender κάνει αυτόματη προσθήκη αποκατεστημένων αρχείων στη λίστα εξαιρέσεων.
5. Ενεργοποιήστε την σε πραγματικό χρόνο προστασία από ιούς του Bitdefender .
6. Επικοινωνήστε με τους εκπροσώπους μας της τεχνικής υποστήριξης, ώστε να καταργήσουμε την ανίχνευση της ενημέρωσης πληροφοριών απειλών. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο *"Ζητήσετε βοήθεια"* (p. 345).

3.3.7. Πώς ελέγχω τι απειλές έχει εντοπίσει το Bitdefender;

Κάθε φορά που γίνεται μια σάρωση , δημιουργείται ένα αρχείο καταγραφής της σάρωσης και το Bitdefender καταγράφει τα εντοπισμένα προβλήματα.

Το αρχείο καταγραφής της σάρωσης περιέχει αναλυτικές πληροφορίες για τη διαδικασία σάρωσης που καταγράφηκε , όπως επιλογές σάρωσης, τον στόχο της σάρωσης, τις απειλές που βρέθηκαν και τις ενέργειες που λήφθηκαν σε αυτές τις απειλές.

Μπορείτε να ανοίξετε το αρχείο καταγραφής της σάρωσης απευθείας από τον οδηγό σάρωσης, αφού ολοκληρωθεί η σάρωση, πατώντας **ΕΜΦΑΝΙΣΗ ΑΡΧΕΙΟΥ ΚΑΤΑΓΡΑΦΗΣ**.

Για να ελέγξετε ένα αρχείο καταγραφής της σάρωσης ή οποιοδήποτε μόλυνση έχει εντοπιστεί σε μεταγενέστερο χρόνο:

1. Πατήστε **Ειδοποιήσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **All** επιλέξτε την ειδοποίηση που αφορά την τελευταία σάρωση.

   Εκεί μπορείτε να βρείτε όλα τα συμβάντα σάρωσης απειλών, συμπεριλαμβανομένων των απειλών που εντοπίζονται από τη σάρωση κατά την πρόσβαση, τις σαρώσεις που ξεκίνησε ο χρήστης και τις αλλαγές κατάστασης για αυτόματες σαρώσεις.
3. Στη λίστα ειδοποιήσεων, μπορείτε να ελέγξετε τις σαρώσεις που έχουν διεξαχθεί πρόσφατα. Κάντε κλικ σε μια ειδοποίηση για να δείτε λεπτομέρειες σχετικά με αυτή.
4. Για να ανοίξετε ένα αρχείο καταγραφής της σάρωσης, κάντε κλικ στην επιλογή **Προβολή αρχείου καταγραφής**.

3.4. Γονικός Έλεγχος

3.4.1. Πώς μπορώ να προστατεύσω τα παιδιά μου από διαδικτυακές απειλές;

BitdefenderΟ γονικός έλεγχος σας επιτρέπει να περιορίσετε την πρόσβαση στο διαδίκτυο και σε συγκεκριμένες εφαρμογές, εμποδίζοντας τα παιδιά σας να βλέπουν ακατάλληλο περιεχόμενο όποτε δεν είστε κοντά τους.

Για να ρυθμίσετε τις παραμέτρους του γονικού ελέγχου:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.

2. Στο **ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ** , κάντε κλικ **Ρύθμιση**.

   Θα μεταφερθείτε στην ιστοσελίδα του Bitdefender λογαριασμού. Βεβαιωθείτε ότι έχετε συνδεθεί με τους κωδικούς σας.

3. Ανοίγει ο πίνακας γονικού ελέγχου. Από εδώ μπορείτε να ελέγξετε και να διαμορφώσετε τις ρυθμίσεις του Γονικού Ελέγχου.

4. Κάντε κλικ στο **ΠΡΟΣΘΗΚΗ ΠΡΟΦΙΛ ΠΑΙΔΙΟΥ** .

5. Ορίστε συγκεκριμένες πληροφορίες, όπως όνομα, ημερομηνία γέννησης ή φύλο. Για να προσθέσετε μια εικόνα στο προφίλ του παιδιού σας, κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία **Εικόνα προφίλ**. Κάντε κλικ στο **ΑΠΟΘΗΚΕΥΣΗ** για να συνεχίσετε.

   Με βάση τα πρότυπα ανάπτυξης των παιδιών, τον καθορισμό της ηλικίας του παιδιού φορτώνονται οι αυτόματα προδιαγραφές που θεωρούνται κατάλληλες για την κατηγορία της ηλικίας του.

6. Κάντε κλικ **ΑΣ ΠΡΟΣΘΕΣΟΥΜΕ ΜΙΑ ΣΥΣΚΕΥΗ**

7. Εάν η συσκευή του παιδιού σας έχει ήδη εγκατεστημένο Bitdefender προϊόν , επιλέξτε τη συσκευή του από τη διαθέσιμη λίστα και στη συνέχεια επιλέξτε τον λογαριασμό που θέλετε να παρακολουθήσετε. Κάντε κλικ στο **ΑΝΤΙΣΤΟΙΧΙΣΗ**.

   Εάν το παιδί σας δεν έχει εγκαταστήσει προϊόν Bitdefender στη συσκευή που χρησιμοποιεί, κάντε κλικ στο **Εγκατάσταση σε μια νέα συσκευή** και, στη συνέχεια, κάντε κλικ στο **Αποστολή συνδέσμου λήψης** . Πληκτρολογήστε μια διεύθυνση ηλεκτρονικού ταχυδρομείου στο αντίστοιχο πεδίο και κάντε κλικ στην επιλογή **ΑΠΟΣΤΟΛΗ EMAIL** . Λάβετε υπόψη ότι ο παραγόμενος σύνδεσμος λήψης ισχύει μόνο για τις επόμενες 24 ώρες. Εάν λήξει ο σύνδεσμος, θα πρέπει να δημιουργήσετε ένα νέο, ακολουθώντας τα ίδια βήματα.

   Στη συσκευή που θέλετε να εγκαταστήσετε το Bitdefender, ελέγξτε τον email λογαριασμό που πληκτρολογήσατε και στη συνέχεια κάντε κλικ στο αντίστοιχο κουμπί λήψης.

Σημαντικό

Σε συσκευές που βασίζονται σε Windows και macOS και δεν έχουν εγκατεστημένο προϊόν Bitdefender, θα εγκατασταθεί το πρόγραμμα παρακολούθησης γονικού ελέγχου Bitdefender και θα μπορείτε να παρακολουθείτε τις δραστηριότητες των παιδιών στο διαδίκτυο.

Στις συσκευές Android και iOS, θα γίνει λήψη και εγκατάστασης της εφαρμογής Bitdefender Parental Control.

3.4.2. Πώς μπορώ να εμποδίσω την πρόσβαση του παιδιού μου σε μια ιστοσελίδα;

Bitdefender Γονικός Έλεγχος σας επιτρέπει να ελέγχετε το περιεχόμενο στο οποίο έχει πρόσβαση το παιδί σας ενώ χρησιμοποιεί την συσκευή του και σας επιτρέπει να αποκλείσετε την πρόσβαση του σε έναν ιστότοπο.

Για να αποκλείσετε την πρόσβαση σε έναν ιστότοπο, πρέπει να τον προσθέσετε στη λίστα Εξαιρέσεις, ως εξής:

1. Μετάβαση σε: https://central.bitdefender.com.
2. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Κάντε κλικ στο **Γονικός Έλεγχος** για να αποκτήσετε πρόσβαση στο πίνακα.
4. Επιλέξτε το προφίλ του παιδιού σας.
5. Κάντε κλικ στην καρτέλα **ΕΠΙΛΟΓΕΣ** και, στη συνέχεια, επιλέξτε **Ιστότοποι** .
6. Κάντε κλικ στο **ΔΙΑΧΕΙΡΙΣΗ** .
7. Πληκτρολογήστε τον ιστότοπο που θέλετε να αποκλείσετε στο αντίστοιχο πεδίο.
8. Επιλέξτε **Αποκλεισμός** .
9. Κάντε κλικ στο εικονίδιο για να αποθηκεύσετε τις αλλαγές και, στη συνέχεια, κάντε κλικ στο **ΤΕΛΟΣ** .

Σημείωση
Περιορισμοί μπορούν να οριστούν μόνο για συσκευές Android, macOS και Windows.

3.4.3. Πώς μπορώ να αποτρέψω το παιδί μου από τη χρήση συγκεκριμένων εφαρμογών;

Ο Bitdefender Γονικός Σύμβουλος σας επιτρέπει να ελέγχετε το περιεχόμενο που έχουν πρόσβαση τα παιδιά σας ενώ χρησιμοποιείτε συσκευές.

Για να αποκλείσετε την πρόσβαση σε μια εφαρμογή:

1. Μετάβαση σε: https://central.bitdefender.com.
2. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Κάντε κλικ στο **Γονικός Έλεγχος** για να αποκτήσετε πρόσβαση στο πίνακα.
4. Επιλέξτε ένα παιδικό προφίλ.
5. Κάντε κλικ στο **ΕΠΙΛΟΓΕΣ** και επιλέξτε **Εφαρμογές** .
6. Εμφανίζεται μια λίστα με τις διαθέσιμες συσκευές.

   Επιλέξτε την κάρτα με την συσκευή της οποίας θέλετε να περιορίσετε την πρόσβαση της σε εφαρμογές.
7. Κάντε κλικ **Διαχείριση των εφαρμογών που χρησιμοποιούνται από ...** .

   Εμφανίζεται μια λίστα με τις εγκατεστημένες εφαρμογές.
8. Επιλέξτε **Αποκλεισμός** δίπλα στις εφαρμογές που θέλετε να σταματήσει να χρησιμοποιεί το παιδί σας.
9. Κάντε κλικ στο **ΑΠΟΘΗΚΕΥΣΗ** για να εφαρμόσετε τις ρυθμίσεις.

Σημείωση
Περιορισμοί μπορούν να οριστούν μόνο για συσκευές Android, macOS και Windows.

3.4.4. Πώς μπορώ να ορίσω μια θέση ως ασφαλή ή μη προσβάσιμη για το παιδί μου;

Bitdefender Γονικός Έλεγχος σας επιτρέπει να ορίσετε μια τοποθεσία ως ασφαλή ή περιορισμένη για το παιδί σας.

Για να ορίσετε μια τοποθεσία:

1. Μετάβαση σε: https://central.bitdefender.com.
2. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Κάντε κλικ στο **Γονικός Έλεγχος** για να αποκτήσετε πρόσβαση στο πίνακα.

4. Επιλέξτε το προφίλ του παιδιού σας.
5. Κάντε κλικ στο **ΕΠΙΛΟΓΕΣ** και επιλέξτε **Τοποθεσία παιδιού** .
6. Κάντε κλικ στο **Συσκευές** στο πλαίσιο που έχετε στο παράθυρο **Τοποθεσία παιδιού**.
7. Κάντε κλικ στη συσκευή που θέλετε να διαμορφώσετε.
8. Στο παράθυρο **Περιοχές**, κάντε κλικ στο κουμπί **ΠΡΟΣΘΗΚΗ ΠΕΡΙΟΧΗΣ**.
9. Επιλέξτε το είδος της τοποθεσίας, **SAFE** ή **RESTRICTED**.
10. Πληκτρολογήστε ένα έγκυρο όνομα για την περιοχή όπου το παιδί σας έχει δικαίωμα πρόσβασης ή όχι.
11. Ορίστε το εύρος που πρέπει να εφαρμοσθεί για την παρακολούθηση από τη γραμμή ολίσθησης **Ακτίνα**.
12. Κάντε κλικ στο **ΠΡΟΣΘΗΚΗ ΠΕΡΙΟΧΗΣ** για να αποθηκεύσετε τις ρυθμίσεις σας.

Όποτε θέλετε να ορίσετε μια μη προσβάσιμη τοποθεσία ως ασφαλή, ή μια ασφαλή τοποθεσία ως μη προσβάσιμη, κάντε κλικ επάνω της και στη συνέχεια επιλέξτε το κουμπί**ΕΠΕΞΕΡΓΑΣΙΑ ΠΕΡΙΟΧΗΣ**. Ανάλογα με την αλλαγή που θέλετε να κάνετε, επιλέξτε το **ΑΣΦΑΛΗΣ** ή το **ΜΗ ΠΡΟΣΒΑΣΙΜΗ**, και στη συνέχεια κάντε κλικ στο **ΕΝΗΜΕΡΩΣΗ ΠΕΡΙΟΧΗΣ**.

3.4.5. Πώς μπορώ να αποκλείσω την πρόσβαση του παιδιού μου στις συσκευές που είναι συνδεδεμένες κατά τις καθημερινές δραστηριότητες;

Bitdefender Γονικός Έλεγχος σάς επιτρέπει να περιορίσετε την πρόσβαση του παιδιού σας στις συσκευές που είναι συνδεδεμένεί κατά τις καθημερινές σας δραστηριότητες, όπως είναι οι ώρες σχολείου, όταν πρέπει να γίνει η εργασία ή όταν το παιδί σας πρέπει να κοιμηθεί.

Για να ορίσετε χρονικούς περιορισμούς:

1. Μετάβαση σε: https://central.bitdefender.com.
2. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Κάντε κλικ στο **Γονικός Έλεγχος** για να αποκτήσετε πρόσβαση στο πίνακα.
4. Επιλέξτε το προφίλ του παιδιού που θέλετε να ορίσετε περιορισμούς.

5. Κάντε κλικ στο **ΕΠΙΛΟΓΕΣ** και επιλέξτε **Screentime** .
6. Στην περιοχή **Προγράμματα** , κάντε κλικ στο **Προσθήκη προγράμματος** .
7. Δώστε ένα όνομα στον περιορισμό που θέλετε να ορίσετε (για παράδειγμα, ώρα για κρεβάτι, εργασία, μαθήματα τένις κ.λπ.).
8. Ορίστε το χρονικό πλαίσιο και τις ημέρες κατά τις οποίες πρέπει να εφαρμόζονται οι περιορισμοί και, στη συνέχεια, κάντε κλικ στο **ΠΡΟΣΘΗΚΗ ΠΡΟΓΡΑΜΜΑΤΟΣ** για να αποθηκεύσετε τις ρυθμίσεις.

3.4.6. Πώς μπορώ να αποκλείσω την πρόσβαση του παιδιού μου στιςσυνδεδεμένες συσκευές κατά την διάρκεια της ημέρας ή της νύχτας;

Bitdefender Γονικός Έλεγχος σας επιτρέπει να περιορίσετε την πρόσβαση του παιδιού σας στις συνδεδεμένες συσκευές, σε διαφορετικές ώρες κατά την διάρκεια μιας ημέρας.

Για να ρυθμίσετε την καθημερινή χρήση ορίων:

1. Μετάβαση σε: https://central.bitdefender.com.
2. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Κάντε κλικ στο **Γονικός Έλεγχος** για να αποκτήσετε πρόσβαση στο πίνακα.
4. Επιλέξτε το προφίλ του παιδιού που θέλετε να ορίσετε περιορισμούς.
5. Κάντε κλικ στο **ΕΠΙΛΟΓΕΣ** και επιλέξτε **Screentime** .
6. Στην περιοχή **Ημερήσια χρονικά όρια** , κάντε κλικ στο **ΟΡΙΣΜΟΣ ΗΜΕΡΩΝ ΟΡΩΝ ΧΡΟΝΟΥ** .
7. Ορίστε την ώρα και τις ημέρες κατά τις οποίες πρέπει να εφαρμόζονται οι περιορισμοί και, στη συνέχεια, κάντε κλικ στο **ΑΠΟΘΗΚΕΥΣΗ ΑΛΛΑΓΩΝ** για να αποθηκεύσετε τις ρυθμίσεις.

3.4.7. Πώς να αφαιρέσετε το προφίλ ενός παιδιού

Αν θέλετε να αφαιρέσετε ένα υπάρχον προφίλ παιδιού:

1. Μετάβαση σε: https://central.bitdefender.com.

2. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Κάντε κλικ στο **Γονικός Έλεγχος** για να αποκτήσετε πρόσβαση στο πίνακα.
4. Επιλέξτε το παιδικό προφίλ που θέλετε να διαγράψετε.
5. Κάντε κλικ στο **ΕΠΙΛΟΓΕΣ** και επιλέξτε **Διαγραφή προφίλ** .
6. Επιβεβαιώστε την επιλογή σας.

3.5. Privacy protection

3.5.1. Πώς μπορώ να βεβαιωθώ ότι η διαδικτυακή συναλλαγή μου είναι ασφαλής;

Για να βεβαιωθείτε ότι οι διαδικτυακές δραστηριότητες σας παραμένουν ιδιωτικές, μπορείτε να χρησιμοποιήσετε το πρόγραμμα περιήγησης που παρέχεται από το Bitdefender για να προστατέψει τις συναλλαγές σας και τις εφαρμογές home banking.

Bitdefender Safepay ™ είναι ένα ασφαλές πρόγραμμα περιήγησης σχεδιασμένο για να προστατεύσει τις πληροφορίες της πιστωτικής σας κάρτας, τον αριθμό λογαριασμού ή οποιαδήποτε άλλα ευαίσθητα δεδομένα μπορεί να εισάγετε κατά την πρόσβαση σε διαφορετικές τοποθεσίες στο διαδίκτυο.

Για να διατηρήσετε τις online δραστηριότητες σας ασφαλείς και ιδιωτικές:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Safepay**, πατήστε **Ρυθμίσεις**.
3. Στο παράθυρο **Safepay** , κάντε κλικ στο **Εκκίνηση Safepay** .
4. Κάντε κλικ στο κουμπί για να αποκτήσετε πρόσβαση στο **Εικονικό Πληκτρολόγιο**.

   Χρησιμοποιήστε το **Εικονικό Πληκτρολόγιο** όταν πληκτρολογείτε απόρρητες πληροφορίες όπως τους κωδικούς πρόσβασης σας.

3.5.2. Τι μπορώ να κάνω αν η συσκευή μου έχει κλαπεί;

Η Κλοπή κινητής συσκευής, είτε πρόκειται για ένα smartphone, ένα tablet ή ένα lap-top είναι ένα από τα κύρια ζητήματα που σήμερα επηρεάζουν άτομα και οργανώσεις σε όλο τον κόσμο.

Το Bitdefender Anti-Theft σας επιτρέπει όχι μόνο να εντοπίσετε και να κλειδώσετε την κλεμμένη συσκευή, αλλά και εξαλείψετε όλα τα δεδομένα για να διασφαλιστεί ότι δεν θα χρησιμοποιηθούν από τον κλέφτη.

Για να αποκτήσετε πρόσβαση στα Anti-Theft χαρακτηριστικά από το λογαριασμό σας:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το **Οι συσκευές μου**.
3. Κάντε κλικ στην επιθυμητή κάρτα της συσκευής, στη συνέχεια, επιλέξτε **Anti-Theft**.
4. Επιλέξτε την λειτουργία που θέλετε να χρησιμοποιήσετε
   - **ΕΝΤΟΠΙΣΜΟΣ** - εμφανίζει την τοποθεσία της συσκευής σας στο Google Maps.
   - **Ειδοποίηση** - στέλνει μια ειδοποίηση στη συσκευή.
   - **Κλείδωμα** - κλειδώστε τη συσκευή σας και ορίστε έναν αριθμητικό κωδικό PIN για να το ξεκλειδώσετε. Εναλλακτικά, ενεργοποιήστε την αντίστοιχη επιλογή για να επιτρέψετε το Bitdefender να λαμβάνει στιγμιότυπα του ατόμου που προσπαθεί να αποκτήσει πρόσβαση συσκευή σας.
   - **Διαγραφή** - διαγράψετε όλα τα δεδομένα από τη συσκευή σας.

     Σημαντικό
     Μετά από την απαλοιφή μιας συσκευής, όλες οι λειτουργίες Anti-Theft παύουν να λειτουργούν.

   - **Show IP** - εμφανίζει την τελευταία διεύθυνση IP για την επιλεγμένη συσκευή.

3.5.3. Πώς μπορώ να διαγράψω ένα αρχείο μόνιμα με το Bitdefender;

Αν θέλετε να αφαιρέσετε ένα αρχείο οριστικά από το σύστημά σας, θα πρέπει να διαγράψετε τα δεδομένα με φυσική διαγραφή από το σκληρό σας δίσκο.

Το Bitdefender File Shredder θα σας βοηθήσει να τεμαχίσετε γρήγορα αρχεία ή φακέλους από τη συσκευή σας χρησιμοποιώντας το μενού με τα συμφραζόμενα των Windows ακολουθώντας τα παρακάτω βήματα:

1. Κάντε δεξί κλικ στο αρχείο ή το φάκελο που θέλετε να διαγράψετε οριστικά, δείξτε το στο Bitdefender και επιλέξτε **Καταστροφέας αρχείου**.
2. Κάντε κλικ στο **Διαγραφή μόνιμα** και, στη συνέχεια, επιβεβαιώστε ότι θέλετε να συνεχίσετε τη διαδικασία.

   Περιμένετε να τελειώσει το Bitdefender την καταστροφή των αρχείων.
3. Τα αποτελέσματα εμφανίζονται. Επιλέξτε **ΤΕΛΟΣ** για να βγείτε από τον οδηγό.

3.5.4. Πώς μπορώ να προστατέψω την webcam μου;

Μπορείτε να ορίσετε το Bitdefender προϊόν σας για να επιτρέψετε ή να αρνηθείτε την πρόσβαση των εγκατεστημένων εφαρμογών στην κάμερα web ακολουθώντας τα παρακάτω βήματα:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ΒΙΝΤΕΟ & ΠΡΟΣΤΑΣΙΑ ΗΧΟΥ**, κάντε κλικ στην επιλογή **Ρυθμίσεις**.
3. Μεταβείτε στο παράθυρο **Webcam Protection** και θα δείτε τη λίστα με τις εφαρμογές που έχουν ζητήσει πρόσβαση στην κάμερά σας.
4. Τοποθετήστε το δείκτη στην εφαρμογή που θέλετε να επιτρέψετε ή απαγορεύσετε την πρόσβαση και, στη συνέχεια, κάντε κλικ στο διακόπτη που αντιπροσωπεύεται από μια βιντεοκάμερα, που βρίσκεται δίπλα της.

   Για να δείτε τι έχουν επιλέξει οι άλλοι Bitdefender χρήστες για την επιλεγμένη εφαρμογή, κάντε κλικ στο εικονίδιο. Θα ειδοποιηθείτε κάθε φορά που μία από τις επιτρεπόμενες εφαρμογές έχει αποκλειστεί από τους Bitdefender χρήστες.

Για να προσθέσετε μη αυτόματα εφαρμογές σε αυτήν τη λίστα, κάντε κλικ στο κουμπί **Προσθήκη εφαρμογής** και ορίστε μία από τις δύο επιλογές.

- Από το Windows Store
- Από τις εφαρμογές σας

3.5.5. Πώς μπορώ να επαναφέρω με μη αυτόματο τρόπο τα κρυπτογραφημένα αρχεία όταν αποτύχει η διαδικασία αποκατάστασης;

Σε περίπτωση που τα κρυπτογραφημένα αρχεία δεν μπορούν να επαναφερθούν αυτόματα, μπορείτε να τα επαναφέρετε με μη αυτόματο τρόπο ακολουθώντας τα εξής βήματα:

1. Πατήστε **Ειδοποιήσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **Όλα** , επιλέξτε την ειδοποίηση σχετικά με την τελευταία ανίχνευση συμπεριφοράς ransomware και στην συνέχεια κάντε κλικ **Κρυπτογραφημένα αρχεία** .
3. Εμφανίζεται η λίστα με τα κρυπτογραφημένα αρχεία.

   Κάντε κλικ στο **Ανάκτηση αρχείων** για να συνεχίσετε.
4. Σε περίπτωση αποτυχίας ολόκληρου ή μέρους της διαδικασίας αποκατάστασης, πρέπει εσείς να επιλέξετε την θέση αποθήκευσης των αποκρυπτογραφημένων αρχείων. Κάντε κλικ στο **Επαναφορά τοποθεσίας** και, στη συνέχεια, επιλέξτε μια τοποθεσία στον υπολογιστή σας.
5. Εμφανίζεται ένα παράθυρο επιβεβαίωσης.

   Κάντε κλικ στο **Τέλος** για να τερματίσετε τη διαδικασία επαναφοράς.

Αρχεία με τις ακόλουθες καταλήξεις μπορούν να αποκατασταθούν σε περίπτωση κρυπτογράφησης:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

3.6. Εργαλεία βελτιστοποίησης

3.6.1. Πώς μπορώ να βελτιώσω την απόδοση του συστήματος μου;

Η απόδοση του συστήματος δεν εξαρτάται μόνο από τη διαμόρφωση του υλικού, όπως είναι το φορτίο της CPU, χρήση μνήμης και χώρος στο σκληρό δίσκο. Επίσης, συνδέεται άμεσα και με τη διαμόρφωση του λογισμικού σας και τη διαχείριση των δεδομένων σας.

Στο Bitdefender οι κύριες ενέργειες για τη βελτίωση της ταχύτητας του συστήματος σας και την απόδοση του έχουν ως εξής:

- "*Βελτιστοποίηση της απόδοσης του συστήματός σας με ένα μόνο κλικ*" (p. 73)
- "*Σάρωση του συστήματός σας σε τακτά χρονικά διαστήματα*" (p. 73)

Βελτιστοποίηση της απόδοσης του συστήματός σας με ένα μόνο κλικ

Η επιλογή OneClick Optimizer σας εξοικονομεί πολύτιμο χρόνο όταν θέλετε ένα γρήγορο τρόπο για να βελτιώσετε την απόδοση του συστήματος σας με την ταχεία σάρωση, την ανίχνευση και τον καθαρισμό άχρηστων αρχείων

Για να ξεκινήσετε τη διαδικασία OneClick Optimizer:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Κάντε κλικ στο κουμπί **Βελτιστοποίηση**.
3. Επιτρέψτε στο Bitdefender να αναζητήσει τα αρχεία που μπορούν να διαγραφούν, στη συνέχεια, κάντε κλικ στο κουμπί **Βελτιστοποίηση** (Optimization) για να ολοκληρώσετε τη διαδικασία.

Σάρωση του συστήματός σας σε τακτά χρονικά διαστήματα

Η ταχύτητα του συστήματός σας και γενικά η συμπεριφορά του μπορεί επίσης να επηρεαστεί από κακόβουλο λογισμικό.

Σιγουρευτείτε ότι σαρώνετε το σύστημά σας σε τακτά χρονικά διαστήματα, τουλάχιστον μία φορά την εβδομάδα.

Συνιστάται να χρησιμοποιήσετε τη σάρωση συστήματος, επειδή σαρώνει για όλους τους τύπους απειλών που θέτουν σε κίνδυνο την ασφάλεια του συστήματός σας και σαρώνει επίσης συμπιεσμένα αρχεία.

Για να ξεκινήσετε τη σάρωση του συστήματος:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Κάντε κλικ στο **Εκτέλεση σάρωσης** δίπλα στο **Σάρωση συστήματος** .
4. Ακολουθήστε τα βήματα του οδηγού.

3.7. Χρήσιμες πληροφορίες

3.7.1. Πώς μπορώ να ελέγξω την λύση ασφάλειας μου;

Για να βεβαιωθείτε ότι το Bitdefender προϊόν σας λειτουργεί κανονικά, σας συνιστούμε να χρησιμοποιείτε το EICAR test.

Η δοκιμή EICAR σας επιτρέπει να ελέγξετε την προστασία σας από απειλές χρησιμοποιώντας ένα ασφαλές αρχείο που αναπτύχθηκε για το σκοπό αυτό.

Για να ελέγξετε τη λύση ασφαλείας:

1. Κατεβάστε το τεστ από την επίσημη ιστοσελίδα του οργανισμού EICAR http://www.eicar.org/.
2. Κάντε κλικ στην καρτέλα **Δοκιμαστικό Αρχείο Καταπολέμησης Κακόβουλου λογισμικού** . (Anti-Malware Testfile)
3. Κάντε κλικ στο **Κατεβάστε** στο μενού της αριστερής πλευράς.
4. Από **περιοχή λήψης, χρησιμοποιώντας το πρωτόκολλο http** κάντε κλικ στο **EICAR. Com** αρχείο δοκιμής.
5. Θα ενημερωθείτε ότι στη σελίδα που προσπαθείτε να μπείτε περιέχεται το αρχείο EICAR- Test-(δεν είναι απειλή).

   Εάν κάνετε κλικ **καταλαβαίνω τους κινδύνους, προχωράμε ούτως ή άλλως** , η λήψη του τεστ θα ξεκινήσει και ένα Bitdefender αναδυόμενο παράθυρο θα σας ενημερώσει ότι μία απειλή εντοπίστηκε.

   Κάντε κλικ στο **Περισσότερες λεπτομέρειες** για να μάθετε περισσότερες πληροφορίες σχετικά με τη δράση αυτή.

Εάν δεν λάβετε καμία ειδοποίηση από το Bitdefender , σας προτείνουμε να επικοινωνήσετε με την υποστήριξη του Bitdefender, όπως περιγράφεται στην ενότητα "*Ζητήσετε βοήθεια*" (p. 345).

3.7.2. Πώς μπορώ να απεγκαταστήσω το Bitdefender;

Εάν θέλετε να καταργήσετε το Bitdefender Total Security:

- Στα **Windows 7**:
  1. Κάντε κλικ στο **Εναρξη**, πηγαίνετε στο **Πίνακας Ελέγχου** και κάντε διπλό κλικ στο **Προγράμματα και Δυνατότητες** .
  2. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
  3. Κάντε κλικ στο **Κατάργηση** στο παράθυρο που εμφανίζεται.
  4. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.
- Στα **Windows 8 και στα Windows 8.1**:
  1. Από την οθόνη Έναρξης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Πίνακας Ελέγχου" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του.
  2. Κάντε κλικ στο **Κατάργηση εγκατάστασης προγράμματος** ή στο **Προγράμματα και δυνατότητες** .
  3. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
  4. Κάντε κλικ στο **Κατάργηση** στο παράθυρο που εμφανίζεται.
  5. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.
- Στα **Windows 10**:
  1. Κάντε κλικ στο **Εκκίνηση**και στη συνέχεια, κάντε κλικ στην επιλογή Ρυθμίσεις.
  2. Κάντε κλικ στο εικονίδιο **Σύστημα** στην περιοχή Ρυθμίσεις και στη συνέχεια επιλέξτε **Εφαρμογές**.

3. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
4. Κάντε κλικ στο **Απεγκατάσταση** ξανά για να επιβεβαιώσετε την επιλογή σας.
5. Κάντε κλικ στο **Κατάργηση** στο παράθυρο που εμφανίζεται.
6. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

Σημείωση
Αυτή η διαδικασία επανεγκατάστασης θα διαγράψει οριστικά τις προσαρμοσμένες ρυθμίσεις.

3.7.3. Πώς μπορώ να απεγκαταστήσω το Bitdefender VPN;

Η διαδικασία κατάργησης του Bitdefender VPN είναι παρόμοια με αυτήν που χρησιμοποιείτε για την κατάργηση άλλων προγραμμάτων από τη συσκευή σας:

- Στα **Windows 7**:
  1. Κάντε κλικ στο **Εναρξη**, πηγαίνετε στο **Πίνακας Ελέγχου** και κάντε διπλό κλικ στο **Προγράμματα και Δυνατότητες** .
  2. Εντοπίστε το **Bitdefender VPN** και επιλέξτε **Κατάργηση εγκατάστασης**.

     Παρακαλούμε περιμένετε για την ολοκλήρωση της απεγκατάστασης.
- Στα **Windows 8 και στα Windows 8.1**:
  1. Από την οθόνη Έναρξης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Πίνακας Ελέγχου" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του.
  2. Κάντε κλικ στο **Κατάργηση εγκατάστασης προγράμματος** ή στο **Προγράμματα και δυνατότητες** .
  3. Εντοπίστε το **Bitdefender VPN** και επιλέξτε **Κατάργηση εγκατάστασης**.

     Παρακαλούμε περιμένετε για την ολοκλήρωση της απεγκατάστασης.
- Στα **Windows 10**:

1. Κάντε κλικ στο **Εκκίνηση**και στη συνέχεια, κάντε κλικ στην επιλογή Ρυθμίσεις.
2. Κάντε κλικ στο εικονίδιο **Σύστημα** στην περιοχή Ρυθμίσεις, στη συνέχεια, επιλέξτε **Εγκατεστημένες εφαρμογές**.
3. Εντοπίστε το **Bitdefender VPN** και επιλέξτε **Κατάργηση εγκατάστασης**.
4. Κάντε κλικ στο **Απεγκατάσταση** ξανά για να επιβεβαιώσετε την επιλογή σας.

   Παρακαλούμε περιμένετε για την ολοκλήρωση της απεγκατάστασης.

3.7.4. Πώς μπορώ να καταργήσω την επέκταση Bitdefender Anti-tracker;

Ανάλογα με το πρόγραμμα περιήγησης που χρησιμοποιείτε, ακολουθήστε τα παρακάτω βήματα για να καταργήσετε την εγκατάσταση της επέκτασης Bitdefender Anti-tracker:

- Internet Explorer

  1. Κάντε κλικ στο κουμπί δίπλα στη γραμμή αναζήτησης και στη συνέχεια, επιλέξτε Διαχείριση πρόσθετων.

     Εμφανίζεται μια λίστα με τις εγκατεστημένες επεκτάσεις.
  2. Κάντε κλικ στην επιλογή Bitdefender Anti-tracker.
  3. Κάντε κλικ στην επιλογή **Απενεργοποίηση** στην κάτω δεξιά γωνία.

- Google Chrome

  1. Κάντε κλικ στο κουμπί δίπλα στη γραμμή αναζήτησης.
  2. Επιλέξτε **Περισσότερα εργαλεία** και στη συνέχεια, **Επεκτάσεις**.

     Εμφανίζεται μια λίστα με τις εγκατεστημένες επεκτάσεις.
  3. Κάντε κλικ στην επιλογή **Κατάργηση** στο Bitdefender Anti-tracker κάρτα.
  4. Κάντε κλικ στο **Κατάργηση** στο αναδυόμενο παράθυρο που εμφανίζεται.

- Mozilla Firefox

1. Κάντε κλικ στο κουμπί ≡ δίπλα στη γραμμή αναζήτησης.
2. Επιλέξτε **Πρόσθετα** και στη συνέχεια **Επεκτάσεις**.

   Εμφανίζεται μια λίστα με τις εγκατεστημένες επεκτάσεις.

3. Κάντε κλικ στο ••• και, στη συνέχεια, επιλέξτε **Κατάργηση** .

3.7.5. Πώς μπορώ να κλείσω αυτόματα τη συσκευή αφού ολοκληρωθεί η σάρωση;

Το Bitdefender προσφέρει πολλαπλές εργασίες σάρωσης που μπορείτε να χρησιμοποιήσετε για να βεβαιωθείτε ότι το σύστημά σας δεν έχει μολυνθεί με απειλές. Η σάρωση ολόκληρης της συσκευής ενδέχεται να διαρκέσει περισσότερο χρόνο, ανάλογα με τη διαμόρφωση του υλικού και του λογισμικού του συστήματός σας.

Για το λόγο αυτό, το Bitdefender σας επιτρέπει να το ρυθμίσετε για να κλείσει αυτόματα το σύστημά μόλις η σάρωση τελειώσει.

Εξετάστε αυτό το παράδειγμα: έχετε τελειώσει τη δουλειά σας και θέλετε να κοιμηθείτε. Θα θέλατε το Bitdefender να ελέγξει ολόκληρο το σύστημά σας για απειλές.

Για να κλείσετε τη συσκευή όταν τελειώσει η γρήγορη σάρωση ή η σάρωση συστήματος:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στο παράθυρο **Σάρωση** , κάντε κλικ στο ••• δίπλα στη Γρήγορη σάρωση ή Σάρωση συστήματος και επιλέξτε **Επεξεργασία** .
4. Προσαρμόστε τη σάρωση σύμφωνα με τις ανάγκες σας και κάντε κλικ στο **Επόμενο** .
5. Επιλέξτε το πλαίσιο δίπλα στο **Επιλέξτε πότε να προγραμματίσετε αυτήν την εργασία** και, στη συνέχεια, επιλέξτε πότε θα ξεκινήσει η εργασία.

   Αν επιλέξετε Καθημερινά, Μηνιαία ή Εβδομαδιαία, σύρετε την μπάρα κατά μήκος της κλίμακας για να ορίσετε την επιθυμητή χρονική περίοδο κατά την έναρξη της προγραμματισμένης σάρωσης.

6. Κάντε κλικ στο **Αποθήκευση**.

Για να κλείσετε τη συσκευή όταν τελειώσει μια προσαρμοσμένη σάρωση:

1. Κάντε κλικ στο κουμπί ••• δίπλα στην προσαρμοσμένη σάρωση που δημιουργήσατε.
2. Κάντε κλικ στο **Επόμενο** και, στη συνέχεια, κάντε ξανά κλικ στο **Επόμενο** .
3. Επιλέξτε το πλαίσιο δίπλα στο **Επιλέξτε πότε να προγραμματίσετε αυτήν την εργασία** και, στη συνέχεια, επιλέξτε πότε θα ξεκινήσει η εργασία.
4. Κάντε κλικ στο **Αποθήκευση**.

Εάν δεν βρεθούν απειλές, η συσκευή θα τερματιστεί.

Εάν υπάρχουν παραμένουσες μη εξουδετερωμένες απειλές, θα σας ζητηθεί να επιλέξετε τις ενέργειες που πρέπει να εφαρμοστούν σε αυτές. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Οδηγός σαρωτή Antivirus "* (p. 98).

3.7.6. Πώς μπορώ να ρυθμίσω το Bitdefender να χρησιμοποιήσει μια σύνδεση διακομιστή μεσολάβησης (proxy) του Internet;

Εάν η συσκευή σας συνδεθεί στο Διαδίκτυο μέσω διακομιστή μεσολάβησης, πρέπει να διαμορφώσετε το Bitdefender με τις ρυθμίσεις διακομιστή μεσολάβησης. Κανονικά, το Bitdefender εντοπίζει αυτόματα και εισάγει τις ρυθμίσεις διακομιστή μεσολάβησης από το σύστημά σας.

Σημαντικό
Οικιακές Συνδέσεις στο Διαδίκτυο συνήθως δεν χρησιμοποιούν διακομιστή μεσολάβησης. Ως γενικός κανόνας, ελέγχετε και διαμορφώστε τις ρυθμίσεις του διακομιστή μεσολάβησης σύνδεση στο Bitdefender πρόγραμμά σας, όταν οι ενημερώσεις δεν λειτουργούν. Εάν το Bitdefender μπορεί να ενημερωθεί, τότε είναι σωστά ρυθμισμένο για σύνδεση με το Internet.

Για να διαχειριστείτε τις ρυθμίσεις του proxy:

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Επιλέξτε την καρτέλα **Advanced**.

3. Ενεργοποιήστε τον **Proxy server**.
4. Επιλέξτε **Αλλαγή Proxy**.
5. Υπάρχουν δύο επιλογές για να ορίσετε τις ρυθμίσεις διακομιστή μεσολάβησης:
   - **Εισαγωγή Ρυθμίσεων μεσολάβησης από το προεπιλεγμένο πρόγραμμα περιήγησης** - proxy ρυθμίσεις του τρέχοντος χρήστη, που ανακτάται από το προεπιλεγμένο πρόγραμμα περιήγησης. Εάν ο διακομιστής μεσολάβησης απαιτεί ένα όνομα χρήστη και έναν κωδικό πρόσβασης, θα πρέπει να τα καθορίσετε στα αντίστοιχα πεδία.

     Σημείωση
     Το Bitdefender μπορεί να εισάγει ρυθμίσεις του διακομιστή μεσολάβησης (proxy) από τα πιο δημοφιλή προγράμματα περιήγησης, συμπεριλαμβανομένων των πιο πρόσφατων εκδόσεων του Internet Explorer, Mozilla Firefox και Google Chrome.

   - **Προσαρμοσμένες Ρυθμίσεις μεσολάβησης** - proxy ρυθμίσεις που μπορείτε να προσαρμόσετε μόνοι σας. Θα πρέπει να ορίσετε τις εξής ρυθμίσεις:
     - **Διεύθυνση** - πληκτρολογήστε την IP διεύθυνση του διακομιστή μεσολάβησης.
     - **Θύρα** - πληκτρολογήστε τη θύρα την οποία το Bitdefender χρησιμοποιεί για να συνδεθεί με το διακομιστή μεσολάβησης.
     - **Όνομα Χρήστη** - πληκτρολογήστε ένα όνομα χρήστη που αναγνωρίζεται από τον διακομιστή μεσαολάβησης.
     - **Κωδικός πρόσβασης** - πληκτρολογήστε τον έγκυρο κωδικό πρόσβασης του προηγουμένως καθορισμένου χρήστη.
6. Κάντε κλικ στο **OK** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

το Bitdefender θα χρησιμοποιήσει τις διαθέσιμες ρυθμίσεις διακομιστή μεσολάβησης μέχρι να καταφέρει να συνδεθεί στο Internet..

3.7.7. Χρησιμοποιώ μ 32 bit ή 64 bit version των Windows?

Για να βρείτε εάν έχετε λειτουργικό σύστημα 32 bit ή 64 bit.

- Στα **Windows 7**:
  1. Κάντε κλικ στο **εκκίνηση** .

2. Εντοπίστε **ο υπολογιστής μου** από το μενού **Έναρξη** .
3. Κάντε δεξί κλικ στο **Ο Υπολογιστής μου** και επιλέξτε **Ιδιότητες** .
4. Κοιτάξτε στο **Σύστημα** , προκειμένου να ελέγξετε τις πληροφορίες σχετικά με το σύστημά σας.

- Στα **Windows 8**:

1. Από την οθόνη Έναρξη των Windows, εντοπίστε **ο Υπολογιστής μου** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Υπολογιστής" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε δεξί κλικ στο εικονίδιό του.

   Στα **Windows 8.1**, εντοπίστε το **This PC**.
2. Επιλέξτε **Ιδιότητες** στο κάτω μέρος του μενού επιλογών
3. Ψάξτε στην περιοχή Συστήματος για να βρείτε τον τύπο του συστήματος σας.

- Στα **Windows 10**:

1. Πληκτρολογήστε "System" στο πλαίσιο αναζήτησης από τη γραμμή εργασιών και κάντε κλικ στο εικονίδιο του.
2. Ψάξτε στην περιοχή του συστήματος για να βρείτε πληροφορίες σχετικά με τον τύπο του συστήματός σας.

3.7.8. Εμφάνιση κρυφών αντικειμένων στα Windows.

Τα βήματα αυτά είναι χρήσιμα σε περιπτώσεις όπου έχουμε να κάνουμε με μία περίπτωση απειλής και θα πρέπει να βρούμε και να καταργήσουμε τα μολυσμένα αρχεία, τα οποία θα μπορούσαν να είναι κρυμμένα.

Ακολουθήστε τα παρακάτω βήματα για να εμφανίσετε κρυφά αντικείμενα στα Windows:

1. Κάντε κλικ στο **εκκίνηση** , και πηγαίνετε στο **Πίνακας Ελέγχου** .

   Στα **Windows 8 και στα Windows 8.1**: Από την οθόνη εκκίνησης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα μπορείτε να αρχίσετε να πληκτρολογείτε "Πίνακας Ελέγχου" κατευθείαν στην οθόνη εκκίνησης των Windows) και κατόπιν να κάνετε κλικ στο εικονίδιο του.
2. Επιλέξτε **Επιλογές φακέλων** .
3. Πηγαίνετε στη καρτέλα **Προβολή** .

4. Επιλέξτε **Εμφάνιση κρυφών αρχείων και φακέλων** .
5. Αποεπιλέξτε **Απόκρυψη επεκτάσεων για γνωστούς τύπους αρχείων** .
6. Αποεπιλέξτε **Απόκρυψη προστατευμένων αρχείων λειτουργικού συστήματος** .
7. Κάντε κλικ στο **Εφαρμογή**, στη συνέχεια κάντε κλικ στο **OK**.

Στα **Windows 10**:

1. Πληκτρολογήστε "Εμφάνιση κρυφών αρχείων και φακέλων" στο πλαίσιο αναζήτησης από τη γραμμή εργασιών και κάντε κλικ στο εικονίδιο του.
2. Επιλέξτε **Εμφάνιση κρυφών αρχείων, φακέλων και μονάδων δίσκου** .
3. Αποεπιλέξτε **Απόκρυψη επεκτάσεων για γνωστούς τύπους αρχείων** .
4. Αποεπιλέξτε **Απόκρυψη προστατευμένων αρχείων λειτουργικού συστήματος** .
5. Κάντε κλικ στο **Εφαρμογή**, στη συνέχεια κάντε κλικ στο **OK**.

3.7.9. Πώς μπορώ να καταργήσω τις άλλες λύσεις ασφάλειας;

Ο κύριος λόγος για τη χρήση μιας λύσης ασφάλειας είναι να παρέχει προστασία και ασφάλεια για τα δεδομένα σας. Τι συμβαίνει όμως όταν έχετε περισσότερα από ένα προϊόν ασφάλειας στο ίδιο σύστημα;

Όταν χρησιμοποιείτε περισσότερες από μία λύσεις ασφαλείας στην ίδια συσκευή, το σύστημα γίνεται ασταθές. Ο Bitdefender Total Security εγκαταστάτης ανιχνεύει αυτόματα άλλα προγράμματα ασφαλείας και σας προσφέρει την δυνατότητα να τα απεγκαταστήσετε.

Αν δεν αφαιρέσατε τις άλλες λύσεις ασφαλείας κατά τη διάρκεια της αρχικής εγκατάστασης:

- Στα **Windows 7**:
  1. Κάντε κλικ στο **Εναρξη**, πηγαίνετε στο **Πίνακας Ελέγχου** και κάντε διπλό κλικ στο **Προγράμματα και Δυνατότητες** .
  2. Περιμένετε μερικά λεπτά μέχρι να εμφανιστεί ο κατάλογος του εγκατεστημένου λογισμικού.
  3. Βρείτε το όνομα του προγράμματος που θέλετε να καταργήσετε και επιλέξτε **Απεγκατάσταση**.

4. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

- Στα **Windows 8 και στα Windows 8.1**:

1. Από την οθόνη Έναρξης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Πίνακας Ελέγχου" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του.
2. Κάντε κλικ στο **Κατάργηση εγκατάστασης προγράμματος** ή στο **Προγράμματα και δυνατότητες** .
3. Περιμένετε μερικά λεπτά μέχρι να εμφανιστεί ο κατάλογος του εγκατεστημένου λογισμικού.
4. Βρείτε το όνομα του προγράμματος που θέλετε να καταργήσετε και επιλέξτε **Απεγκατάσταση**.
5. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

- Στα **Windows 10**:

1. Κάντε κλικ στο **Εκκίνηση**και στη συνέχεια, κάντε κλικ στην επιλογή Ρυθμίσεις.
2. Κάντε κλικ στο εικονίδιο **Σύστημα** στην περιοχή Ρυθμίσεις και στη συνέχεια επιλέξτε **Εφαρμογές**.
3. Βρείτε το όνομα του προγράμματος που θέλετε να καταργήσετε και επιλέξτε **Απεγκατάσταση**.
4. Κάντε κλικ στο **Απεγκατάσταση** ξανά για να επιβεβαιώσετε την επιλογή σας.
5. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

Αν δεν τα καταφέρετε να απομακρύνετε την άλλη λύση ασφάλειας από το σύστημά σας, αποκτήστε το εργαλείο απεγκατάστασης από την ιστοσελίδα του προμηθευτή ή επικοινωνήστε απευθείας μαζί του για να σας δώσει τις κατευθυντήριες γραμμές για απεγκατάσταση.

3.7.10. Πώς μπορώ να κάνω επανεκκίνηση σε ασφαλή λειτουργία;

Η ασφαλής λειτουργία είναι ένας διαγνωστικός τρόπος λειτουργίας, η οποία χρησιμοποιείται κυρίως για την αντιμετώπιση προβλημάτων που επηρεάζουν την κανονική λειτουργία των Windows. Τέτοια προβλήματα κυμαίνονται από conflicting drivers μέχρι απειλές που εμποδίζουν την κανονική εκκίνηση των Windows. Σε Ασφλαή λειτουργία εργάζονται λίγες μόνο εφαρμογές και τα Windows φορτώνουν μόνο τα βασικά προγράμματα οδήγησης και ένα ελάχιστο σετ υποσυστημάτων του λειτουργικού συστήματος. Για αυτό οι περισσότερες απειλές είναι ανενεργές όταν τα Windows χρησιμοποιούνται σε ασφαλή λειτουργία και μπορούν να αφαιρεθούν εύκολα.

Για να ξεκινήσετε τα Windows σε κατάσταση ασφαλούς λειτουργίας.

- Στα **Windows 7**:
  1. Επανεκκινήστε τη συσκευή.
  2. Πατήστε το **F8** πλήκτρο, αρκετές φορές πριν από την εκκίνηση των Windows, για να αποκτήσετε πρόσβαση στο μενού εκκίνησης.
  3. Επιλέξτε **Ασφαλής λειτουργία** στο μενού εκκίνησης ή **ασφαλής λειτουργία με σύνδεση δικτύου** , αν θέλετε να έχετε πρόσβαση στο Internet
  4. Πατήστε το **Enter** και περιμένετε όσο τα Windows ξεκινούν σε κατάσταση ασφαλούς λειτουργίας.
  5. Αυτή η διαδικασία ολοκληρώνεται με ένα μήνυμα επιβεβαίωσης. Κάντε κλικ στο κουμπί **OK** για να αποδεχθείτε
  6. Για να ξεκινήσετε τα Windows κανονικά, απλά κάντε επανεκκίνηση του συστήματος
- Στα **Windows 8, Windows 8.1 και στα Windows 10**:
  1. Ξεκινήστε το **System Configuration** στα Windows πατώντας ταυτόχρονα τα πλήκτρα **Windows + R** στο πληκτρολόγιο σας.
  2. Γράψτε **msconfig** στο παράθυρο διαλόγου **Open**, στη συνέχεια κάντε κλικ στο κουμπί **OK**.
  3. Επιλέξτε την καρτέλα **Boot**.
  4. Στην περιοχή **Boot options**, επιλέξτε το πλαίσιο ελέγχου **Safe boot**.

5. Κάντε κλικ στο **Network** και μετά στο **OK**.
6. Κάντε κλικ στο **OK**, στο παράθυρο του **System Configuration** που σας ενημερώνει ότι πρέπει να γίνει επανεκκίνηση του συστήματος, ώστε να είναι σε θέση να κάνει τις αλλαγές που έχετε ορίσει.

   Το σύστημά σας θα επανεκκίνηση σε Safe Mode με Networking.

Για να κάνετε επανεκκίνηση σε κανονική λειτουργία, επιστρέψετε τις ρυθμίσεις επιλέγοντας πάλι το **System Operation** και απο-επιλέγοντας το **Safe boot**. Κάντε κλικ στο **OK** και μετά στο **Restart**. Περιμένετε για να εφαρμοστούν οι νέες ρυθμίσεις.

4. ΔΙΑΧΕΊΡΙΣΗ ΤΗΣ ΑΣΦΆΛΕΙΑΣ ΣΑΣ

4.1. Antivirus Προστασία

Το Bitdefender προστατεύει τη συσκευή σας από κάθε είδους απειλή (κακόβουλο λογισμικό, Trojans, spyware, rootkits και ούτω καθεξής). Η προστασία που προσφέρει το Bitdefender χωρίζεται σε δύο κατηγορίες:

- Η Σάρωση κατά την πρόσβαση - αποτρέπει την εισβολή νέων απειλών στο σύστημά σας. Το Bitdefender για παράδειγμα θα σαρώσει ένα έγγραφο του Word για γνωστές απειλές όταν το ανοίξετε, ή ένα μήνυμα ηλεκτρονικού ταχυδρομείου, όταν το λαμβάνετε

  Η σάρωση κατά την πρόσβαση εξασφαλίζει σε πραγματικό χρόνο προστασία ενάντια σε απειλές, και είναι ουσιώδες χαρακτηριστικό κάθε προγράμματος ασφάλειας των υπολογιστών.

  Σημαντικό
  Για να αποφύγετε τη μόλυνση των απειλών από τη συσκευή σας, διατηρήστε ενεργοποιημένη την **σάρωση πρόσβασης**

- Η On-demand σάρωση (σάρωση κατά απαίτηση) - επιτρέπει τον εντοπισμό και την απομάκρυνση του κακόβουλου λογισμικού που βρίσκεται ήδη στο σύστημα. Αυτή είναι η κλασική σάρωση που ξεκίνησε από το χρήστη - μπορείτε να επιλέξετε ποια μονάδα δίσκου, φάκελο ή αρχείο πρέπει να σαρώσει το Bitdefender και το Bitdefender το σαρώνει - κατά απαίτηση σας

Το Bitdefender σαρώνει αυτόματα όλα τα αφαιρούμενα μέσα που είναι συνδεδεμένα στη συσκευή για να βεβαιωθείτε ότι μπορεί να προσεγγιστεί με ασφάλεια. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Αυτόματη σάρωση των αφαιρούμενων μέσων"* (p. 102).

Οι προχωρημένοι χρήστες μπορούν να ρυθμίσουν εξαιρέσεις σάρωσης, εάν δεν θέλουν να σαρωθούν συγκεκριμένα αρχεία ή τύποι αρχείων. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Διαμόρφωση εξαιρέσεων σάρωσης."* (p. 104).

Όταν το Bitdefender εντοπίσει μία απειλή, θα προσπαθήσει αυτόματα να αφαιρέσει τον κώδικα κακόβουλου λογισμικού από το μολυσμένο αρχείο και να ανακατασκευάσει το αρχικό αρχείο. Αυτή η λειτουργία αναφέρεται ως απολύμανση. Τα αρχεία που δεν μπορούν να απολυμανθούν

μετακινούνται στην καραντίνα προκειμένου να απομονωθεί η μόλυνση. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Διαχείριση αρχείων σε καραντίνα"* (p. 107).

Εάν η συσκευή σας έχει μολυνθεί από απειλές, ανατρέξτε στο *"Αφαίρεση απειλών από το σύστημά σας"* (p. 217). Για να σας βοηθήσουμε να καθαρίσετε τη συσκευή σας από απειλές που δεν μπορούν να αφαιρεθούν από το λειτουργικό σύστημα των Windows, το Bitdefender σάς παρέχει *"Περιβάλλον διάσωσης"* (p. 218). Αυτό είναι ένα αξιόπιστο περιβάλλον, ειδικά σχεδιασμένο για την αφαίρεση απειλών, το οποίο σας επιτρέπει να εκκινήσετε τη συσκευή σας ανεξάρτητα από τα Windows. Όταν η συσκευή εκτελείται σε περιβάλλον διάσωσης, οι απειλές των Windows είναι ανενεργές, καθιστώντας εύκολη την κατάργησή τους.

4.1.1. Σάρωση κατά την πρόσβαση (σε πραγματικό χρόνο προστασία)

Το Bitdefender παρέχει συνεχή, σε πραγματικό χρόνο προστασία ενάντια σε ένα ευρύ φάσμα απειλών σαρώνοντας όλα τα προσβάσιμα αρχεία και μηνύματα ηλεκτρονικού ταχυδρομείου.

Ενεργοποίηση ή απενεργοποίηση της σε πραγματικό χρόνο προστασίας

Για να ενεργοποιήσετε ή να απενεργοποιήσετε την real-time προστασία εναντίων των απειλών:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στο παράθυρο **Για προχωρημένους**, ενεργοποιήστε ή απενεργοποιήστε το **Bitdefender Shield** .
4. Αν θέλετε να απενεργοποιήσετε την προστασία σε πραγματικό χρόνο, εμφανίζεται ένα παράθυρο προειδοποίησης. Θα πρέπει να επιβεβαιώσετε την επιλογή σας επιλέγοντας από το μενού τη διάρκεια απενεργοποίησης της σε πραγματικό χρόνο προστασίας. Μπορείτε να απενεργοποιήσετε την προστασία πραγματικού χρόνου για 5, 15 ή 30 λεπτά, για μία ώρα, μόνιμα ή μέχρι μια επανεκκίνηση του συστήματος. Η προστασία σε πραγματικό χρόνο θα ενεργοποιηθεί αυτόματα όταν το επιλεγμένο χρονικό διάστημα θα λήξει.

Προειδοποίηση

Αυτό είναι ένα κρίσιμο ζήτημα ασφάλειας. Σας συνιστούμε να απενεργοποιήσετε την προστασία κατά την πρόσβαση για τον ελάχιστο δυνατό χρόνο, και μόνο εφόσον είναι αναγκαία η απενεργοποίηση. Αν η σε πραγματικό χρόνο προστασία είναι απενεργοποιημένη, δεν θα προστατεύεστε από απειλές.

Διαμόρφωση των ρυθμίσεων προστασίας σε πραγματικό χρόνο για προχωρημένους

Οι προχωρημένοι χρήστες μπορεί να θέλουν να επωφεληθούν από τις ρυθμίσεις σάρωσης του Bitdefender . Μπορείτε να διαμορφώσετε τις ρυθμίσεις προστασίας σε πραγματικό χρόνο με λεπτομέρεια δημιουργώντας ένα προσαρμοσμένο επίπεδο προστασίας.

Για να διαμορφώσετε τις προηγμένες ρυθμίσεις προστασίας σε πραγματικό χρόνο:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στο παράθυρο **Για προχωρημένους**, μπορείτε να διαμορφώσετε τις ρυθμίσεις σάρωσης όπως απαιτείται.

Πληροφορίες σχετικά με τις επιλογές σάρωσης

Μπορείτε να βρείτε αυτές τις πληροφορίες χρήσιμες:

- **Σάρωση εφαρμογών μόνο:** Μπορείτε να ορίσετε το Bitdefender για να σαρώσετε μόνο τις εφαρμογές που έχουν πρόσβαση.
- **Σάρωση δυνητικά ανεπιθύμητων εφαρμογών.** Επιλέξτε αυτήν την επιλογή για να σαρώσετε ανεπιθύμητες εφαρμογές. Μια δυνητικά κακόβουλη εφαρμογή (PUA) ή δυνητικά κακόβουλο πρόγραμμα (PUP) είναι ένα λογισμικό που συνήθως συνοδεύεται από δωρεάν λογισμικό και θα εμφανίσει αναδυόμενα παράθυρα ή θα εγκαταστήσει μια γραμμή εργαλείων στο προεπιλεγμένο πρόγραμμα περιήγησης. Μερικοί εφαρμογές θα αλλάξουν την αρχική σελίδα ή τη μηχανή αναζήτησης, ή άλλες θα εκτελέσουν πολλές διαδικασίες στο παρασκήνιο που επιβραδύνουν τον υπολογιστή ή θα εμφανίσουν πολλές διαφημίσεις. Αυτά τα προγράμματα μπορούν να εγκατασταθούν χωρίς τη συγκατάθεσή σας (επίσης αποκαλούμενα adware) ή θα συμπεριληφθούν από

προεπιλογή στο κιτ γρήγορης εγκατάστασης (που υποστηρίζεται από διαφημίσεις).

- **Σάρωση scripts.** Η λειτουργία Σάρωση σάρωσης επιτρέπει στο Bitdefender να σαρώσει γραφήματα powerhell και έγγραφα γραφείου που θα μπορούσαν να περιέχουν malware με βάση το script.
- **Σάρωση κομματιών του δικτύου.** Για ασφαλή πρόσβαση σε ένα απομακρυσμένο δίκτυο από τη συσκευή σας, σας συνιστούμε να διατηρήσετε ενεργοποιημένη την επιλογή Σάρωση μεριδίων δικτύου.
- **Σάρωση αρχείων προς φύλαξη.** Σάρωση μέσα σε συμπιεσμένα αρχεία είναι μια αργή και έντασης πόρων διαδικασία, η οποία, ως εκ τούτου, δεν συνιστάται για την προστασία σε πραγματικό χρόνο. Συμπιεσμένα αρχεία που περιέχουν μολυσμένα αρχεία δεν αποτελούν άμεση απειλή για την ασφάλεια του συστήματός σας. Η απειλή μπορεί να επηρεάσει το σύστημά σας μόνο εάν το μολυσμένο αρχείο εξαχθεί από το συμπιεσμένο αρχείο και εκτελεστεί χωρίς να έχει ενεργοποιηθεί η σε πραγματικό χρόνο προστασία.

  Εάν αποφασίσετε να χρησιμοποιήσετε αυτήν την επιλογή, ενεργοποιήστε την και μετά σύρετε το διακόπτη κατά μήκος της κλίμακας για να αποκλείσετε από τη σάρωση αρχεία που είναι μεγαλύτερα από μια δεδομένη τιμή σε MB (Megabyte).
- **Τομείς εκκίνησης σάρωσης.** Μπορείτε να ρυθμίσετε το Bitdefender για να σαρώσετε τους τομείς εκκίνησης του σκληρού σας δίσκου. Ο τομέας του σκληρού δίσκου περιέχει τον απαραίτητο κώδικα υπολογιστή για την ενεργοποίηση της διαδικασίας εκκίνησης. Όταν μία απειλή μολύνει τον τομέα εκκίνησης, ο δίσκος μπορεί να γίνει απρόσιτος και μπορεί να μην είστε σε θέση να ξεκινήσετε το σύστημά σας και να έχετε πρόσβαση στα δεδομένα σας.
- **Σάρωση μόνο νέων και τροποποιημένων αρχείων.** Με τη σάρωση μόνο των νέων και τροποποιημένων αρχείων, μπορείτε να βελτιώσετε σημαντικά τη συνολική απόκριση του συστήματος με μία ελάχιστη έκπτωση στον τομέα της ασφάλειας.
- **Σάρωση για keyloggers.** Επιλέξτε αυτήν την επιλογή για να σαρώσετε το σύστημά σας για τις εφαρμογές keylogger. Keyloggers καταγράφουν ό,τι πληκτρολογείτε στο πληκτρολόγιό σας και στέλνουν αναφορές μέσω του Διαδικτύου σε ένα κακόβουλο πρόσωπο (hacker). Ο χάκερ μπορεί να βρει ευαίσθητες πληροφορίες από τα κλεμμένα δεδομένα,

όπως αριθμούς τραπεζικών λογαριασμών και κωδικούς πρόσβασης, και να το χρησιμοποιήσει για να αποκομίσει προσωπικά οφέλη.

- **Σάρωση Πρώιμης εκκίνησης.** Επιλέξτε το **Early boot scan** για να σαρώσετε το σύστημά σας κατά την εκκίνηση, την στιγμή που όλες οι κρίσιμες υπηρεσίες είναι φορτωμένες. Ο σκοπός αυτού του χαρακτηριστικού είναι να βελτιώσει την ανίχνευση της απειλής κατά την εκκίνηση του συστήματος και τον χρόνο εκκίνησης του συστήματος σας.

Οι δράσεις που αναλαμβάνονται σχετικά με την απειλή που ανιχθεύθηκε

Μπορείτε να διαμορφώσετε τις ενέργειες στιος οποίες θα προχωρεί η προστασία σε πραγματικό χρόνο ακολουθώντας τα παρακάτω βήματα:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στο παράθυρο **Για προχωρημένους** , κάντε κύλιση προς τα κάτω στο παράθυρο μέχρι να δείτε την επιλογή **Απειλές** .
4. Διαμορφώστε τις ρυθμίσεις σάρωσης, όπως απαιτείται.

Οι ακόλουθες ενέργειες μπορούν να γίνουν από την προστασία σε πραγματικό χρόνο στο Bitdefender:

Κάντε τις απαραίτητες ενέργειες

Το Bitdefender θα εκτελέσει τις προτεινόμενες ενέργειες, ανάλογα με τον τύπο του ανιχνευμένου αρχείου:

- **Αρχεία που μολύνθηκαν.** Τα αρχεία που ανιχνεύονται ως μολυσμένα ταιριάζουν με μια βάση δεδομένων πληροφοριών απειλών στη βάση δεδομένων της Bitdefender. Το Bitdefender θα προσπαθήσει αυτόματα να αφαιρέσει τον κώδικα κακόβουλου λογισμικού από το μολυσμένο αρχείο και να ανακατασκευάσει το αρχικό αρχείο. Αυτή η λειτουργία αναφέρεται ως απολύμανση.

  Τα αρχεία που δεν μπορούν να απολυμανθούν μετακινούνται στην καραντίνα προκειμένου να απομονωθεί η μόλυνση. Αρχεία σε καραντίνα δεν μπορούν να εκτελεστούν ή να ανοίξουν. Ως εκ τούτου, ο κίνδυνος να μολυνθείτε εξαφανίζεται. Για περισσότερες πληροφορίες, ανατρέξτε στην "*Διαχείριση αρχείων σε καραντίνα*" (p. 107).

Σημαντικό
Για συγκεκριμένους τύπους απειλών, η επιδιόρθωση δεν είναι δυνατή επειδή το ανιχνευμένο αρχείο είναι εντελώς κακόβουλο. Σε τέτοιες περιπτώσεις, το μολυσμένο αρχείο διαγράφεται από το δίσκο.

- **Ύποπτα αρχεία.** Τα αρχεία ανιχνεύονται ως ύποπτα από την ευρετική ανάλυση. Τα ύποπτα αρχεία δεν μπορούν να επιδιορθωθούν, επειδή δεν είναι διαθέσιμη καμία ρουτίνα απολύμανσης. Θα μετακινηθούν στην καραντίνα για να αποτραπεί μια πιθανή μόλυνση.

  Από προεπιλογή, τα αρχεία σε καραντίνα αποστέλλονται αυτόματα στα εργαστήρια της Bitdefender, προκειμένου να αναλυθούν από τους ερευνητές απειλών της Bitdefender. Εάν επιβεβαιωθεί η ύπαρξη απειλής, απελευθερώνεται μια ενημέρωση πληροφοριών απειλής για να καταργηθεί η απειλή.

- **Συμπιεσμένα αρχεία που περιέχουν μολυσμένα αρχεία.**
  - Τα συμπιεσμένα αρχεία που περιέχουν μόνο μολυσμένα αρχεία διαγράφονται αυτόματα.
  - Εάν ένα αρχείο περιέχει τόσο μολυσμένα και καθαρά αρχεία, το Bitdefender θα προσπαθήσει να διαγράψει τα μολυσμένα αρχεία με την προϋπόθεση ότι μπορεί να ανακατασκευάσει το αρχείο με τα καθαρά αρχεία. Αν η ανοικοδόμηση του αρχείου δεν είναι δυνατή, θα ενημερωθείτε ότι δεν μπορεί να ληφθεί κανένα μέτρο ώστε να αποφευχθεί η απώλεια καθαρών αρχείων.

Μετακίνηση σε "Καραντίνα"
Μετακινεί τα ανιχνευμένα αρχεία στην Καραντίνα Αρχεία σε καραντίνα δεν μπορούν να εκτελεστούν ή να ανοίξουν. Ως εκ τούτου, ο κίνδυνος να μολυνθείτε εξαφανίζεται. Για περισσότερες πληροφορίες, ανατρέξτε στην "*Διαχείριση αρχείων σε καραντίνα*" (p. 107).

Άρνηση πρόσβασης
Σε περίπτωση που εντοπιστεί ένα μολυσμένο αρχείο, η πρόσβαση σε αυτό θα πρέπει να απαγορευτεί.

Επαναφορά των προεπιλεγμένων ρυθμίσεων

Οι προεπιλεγμένες ρυθμίσεις προστασίας σε πραγματικό χρόνο εξασφαλίζουν καλή προστασία από απειλές, με ελάχιστες επιπτώσεις στην απόδοση του συστήματος.

Για να επαναφέρετε τις ρυθμίσεις προστασίας στην προεπιλογή:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στο παράθυρο **Για προχωρημένους** , κάντε κύλιση προς τα κάτω στο παράθυρο μέχρι να δείτε την επιλογή **Επαναφορά ρυθμίσεων για προχωρημένους** . Επιλέξτε αυτήν την επιλογή για να επαναφέρετε τις προεπιλεγμένες ρυθμίσεις της προστασίας από ιούς.

4.1.2. On-demand σάρωση

Ο κύριος στόχος για το Bitdefender είναι να διατηρείτε τη συσκευή σας καθαρή από απειλές. Αυτό γίνεται διατηρώντας νέες απειλές εκτός της συσκευής σας και σαρώνοντας τα μηνύματα email σας και τυχόν νέα αρχεία που έχουν ληφθεί ή αντιγραφεί στο σύστημά σας.

Υπάρχει ο κίνδυνος ότι μία απειλή έχει ήδη εισχωρήσει στο σύστημά σας, πριν καν να εγκαταστήσετε το Bitdefender. Αυτός είναι ο λόγος για τον οποίο είναι πολύ καλή ιδέα να σαρώσετε τη συσκευή σας για απειλές κατοίκων μετά την εγκατάσταση του Bitdefender. Και είναι σίγουρα καλή ιδέα να σαρώσετε συχνά τη συσκευή σας για απειλές.

Η On-demand σάρωση βασίζεται στις εργασίες σάρωσης. Οι εργασίες σάρωσης καθορίζουν τις επιλογές σάρωσης και τα αντικείμενα που πρόκειται να σαρωθούν. Μπορείτε να σαρώσετε τη συσκευή όποτε θέλετε εκτελώντας τις προεπιλεγμένες εργασίες ή τις δικές σας εργασίες σάρωσης (εργασίες καθορισμένες από το χρήστη). Εάν θέλετε να σαρώσετε συγκεκριμένες τοποθεσίες στη συσκευή σας ή να διαμορφώσετε τις επιλογές σάρωσης, διαμορφώστε και εκτελέστε μια προσαρμοσμένη σάρωση.

Σάρωση αρχείου ή φάκελου για απειλές

Θα πρέπει να σαρώσετε τα αρχεία και τους φακέλους κάθε φορά που υποψιάζεστε ότι μπορεί να έχουν μολυνθεί. Κάντε δεξί κλικ στο αρχείο ή το φάκελο που θέλετε να σαρώσετε, δείξτε στο **Bitdefender** και **σάρωση με το Bitdefender** . Ο Antivirus Scan wizard θα εμφανιστεί και θα σας καθοδηγήσει στη διαδικασία σάρωσης. Στο τέλος της σάρωσης, θα σας ζητηθεί να επιλέξετε τις ενέργειες που πρέπει να ληφθούν για τα εντοπισμένα αρχεία, εάν εντοπισθούν κάποια μολυσμένα.

Εκτέλεση γρήγορης σάρωσης

Η γρήγορη σάρωση χρησιμοποιεί τη σάρωση στο cloud για την ανίχνευση απειλών που εκτελούνται στο σύστημά σας. Η εκτέλεση της Γρήγορη σάρωσης συνήθως διαρκεί λιγότερο από ένα λεπτό και χρησιμοποιεί ένα τμήμα των πόρων του συστήματος που χρειάζεται ένα κανονικό πρόγραμμα ανίχνευσης ιών.

Για να εκτελέσετε μια γρήγορη σάρωση:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στα παράθυρα **Σάρωση** , κάντε κλικ στο κουμπί **Εκτέλεση σάρωσης** δίπλα στο **Γρήγορη σάρωση** .
4. Ακολουθήστε τον Οδηγό Σάρωσης Antivirus για να ολοκληρώσετε τη σάρωση. Το Bitdefender θα αναλάβει αυτόματα τις προτεινόμενες ενέργειες στα αρχεία που ανιχνεύτηκαν. Εάν υπάρχουν παραμένουσες μη εξουδετερωμένες απειλές, θα σας ζητηθεί να επιλέξετε τις ενέργειες που πρέπει να εφαρμοστούν σε αυτές.

Εκτέλεση Σάρωσης Συστήματος

Η εργασία System Scan σαρώνει ολόκληρη τη συσκευή για όλους τους τύπους απειλών που θέτουν σε κίνδυνο την ασφάλειά της, όπως malware, spyware, adware, rootkits και άλλα.

Σημείωση

Επειδή η **Σάρωση Συστήματος** εκτελεί μια πλήρη σάρωση του όλου συστήματος, η σάρωση μπορεί να πάρει λίγο χρόνο. Επομένως, συνιστάται να εκτελέσετε αυτήν την εργασία όταν δεν χρησιμοποιείτε τη συσκευή σας.

Πριν την εκτέλεση Σάρωσης Συστήματος, συνιστώνται τα εξής:

- Βεβαιωθείτε ότι το Bitdefender είναι ενημερωμένο με τη βάση δεδομένων πληροφοριών απειλών. Η σάρωση της συσκευής σας χρησιμοποιώντας μια παλιά βάση δεδομένων πληροφοριών για απειλές ενδέχεται να εμποδίσει το Bitdefender να εντοπίσει νέες απειλές που βρέθηκαν από την τελευταία ενημέρωση. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Διατηρώντας το Bitdefender ενημερωμένο με τις πιο πρόσφατες ενημερώσεις"* (p. 42).
- Τερματίστε όλα τα ανοιχτά προγράμματα.

Εάν θέλετε να σαρώσετε συγκεκριμένες τοποθεσίες στη συσκευή σας ή να διαμορφώσετε τις επιλογές σάρωσης, διαμορφώστε και εκτελέστε μια προσαρμοσμένη σάρωση. Για περισσότερες πληροφορίες, ανατρέξτε στην "*Ρύθμιση προσαρμοσμένης σάρωσης*" (p. 94).

Για να εκτελέσετε μια σάρωση του συστήματος:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στα παράθυρα **Σάρωση** , κάντε κλικ στο κουμπί **Εκτέλεση σάρωσης** δίπλα στο **Σάρωση συστήματος** .
4. Την πρώτη φορά που εκτελείτε μια σάρωση συστήματος, σας παρουσιάζεται το χαρακτηριστικό. Κάντε κλικ στο **Ok, το κατάλαβα** για να συνεχίσετε.
5. Ακολουθήστε τον Οδηγό Σάρωσης Antivirus για να ολοκληρώσετε τη σάρωση. Το Bitdefender θα αναλάβει αυτόματα τις προτεινόμενες ενέργειες στα αρχεία που ανιχνεύτηκαν. Εάν υπάρχουν παραμένουσες μη εξουδετερωμένες απειλές, θα σας ζητηθεί να επιλέξετε τις ενέργειες που πρέπει να εφαρμοστούν σε αυτές.

Ρύθμιση προσαρμοσμένης σάρωσης

Στο παράθυρο **Διαχείριση σαρώσεων** , μπορείτε να ρυθμίσετε το Bitdefender για εκτέλεση σαρώσεων όποτε θεωρείτε ότι η συσκευή σας χρειάζεται έλεγχο για πιθανές απειλές. Μπορείτε να επιλέξετε να προγραμματίσετε μία Σάρωση Συστήματος ή μία Γρήγορη σάρωση ή μπορείτε να δημιουργήσετε μια προσαρμοσμένη σάρωση, όπως σας εξυπηρετεί.

Για να διαμορφώσετε λεπτομερώς μια νέα προσαρμοσμένη σάρωση:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στα παράθυρα **Σάρωση** , κάντε κλικ στο **+ Δημιουργία σάρωσης** .
4. Στο πεδίο **Όνομα εργασίας** , πληκτρολογήστε ένα όνομα για τη σάρωση και, στη συνέχεια, επιλέξτε τις τοποθεσίες που θέλετε να σαρώσετε και, στη συνέχεια, κάντε κλικ στο **Επόμενο** .
5. Διαμορφώστε αυτές τις γενικές επιλογές:

- **Σάρωση εφαρμογών μόνο**. Μπορείτε να ορίσετε το Bitdefender για να σαρώσετε μόνο τις εφαρμογές που έχουν πρόσβαση.
- **Προτεραιότητα στόχου σάρωσης**. Μπορείτε να επιλέξετε τον αντίκτυπο που θα πρέπει να έχει μια διαδικασία σάρωσης στην απόδοση του συστήματός σας.
  - Αυτόματα - Η προτεραιότητα της διαδικασίας σάρωσης θα εξαρτηθεί από τη δραστηριότητα του συστήματος. Για να βεβαιωθείτε ότι η διαδικασία σάρωσης δεν επηρεάζει τη δραστηριότητα του συστήματος, το Bitdefender θα αποφασίσει αν η διαδικασία σάρωσης θα πρέπει να εκτελείται με υψηλή ή χαμηλή προτεραιότητα.
  - Υψηλή - Η προτεραιότητα της διαδικασίας σάρωσης θα είναι υψηλή. Επιλέγοντας αυτή την επιλογή, θα επιτρέψετε σε άλλα προγράμματα να τρέξουν πιο αργά και να μειώσετε το χρόνο που απαιτείται για να ολοκληρωθεί η διαδικασία σάρωσης.
  - Χαμηλή - Η προτεραιότητα της διαδικασίας σάρωσης θα είναι χαμηλή. Επιλέγοντας αυτήν την επιλογή, θα επιτρέψετε σε άλλα προγράμματα να τρέξουν γρηγορότερα και να αυξήσουν το χρόνο που απαιτείται για να ολοκληρωθεί η διαδικασία σάρωσης.
- **Ενέργειες μετά τη σάρωση**. Επιλέξτε την ενέργεια που πρέπει να κάνει το Bitdefender σε περίπτωση που δεν εντοπιστούν απειλές:
  - Εμφάνιση παραθύρου Σύνοψης
  - Τερματισμός λειτουργίας
  - Κλείσιμο παράθυρου Σάρωσης

6. Εάν θέλετε να διαμορφώσετε λεπτομερώς τις επιλογές σάρωσης, κάντε κλικ στο κουμπί **Εμφάνιση προχωρημένων επιλογών**. Μπορείτε να βρείτε πληροφορίες για τις καταχωρημένες σαρώσεις στο τέλος αυτής της ενότητας.

   Κάντε κλικ στο κουμπί **Next**. (Επόμενο)

7. Μπορείτε να ενεργοποιήσετε το **Προγραμματισμός εργασίας σάρωσης** αν θέλετε και, στη συνέχεια, να επιλέξετε πότε θα ξεκινήσει η προσαρμοσμένη σάρωση που δημιουργήσατε.
   - Κατά την εκκίνηση του συστήματος
   - Καθημερινά
   - Μηνιαία

- Εβδομαδιαία

  Αν επιλέξετε Καθημερινά, Μηνιαία ή Εβδομαδιαία, σύρετε την μπάρα κατά μήκος της κλίμακας για να ορίσετε την επιθυμητή χρονική περίοδο κατά την έναρξη της προγραμματισμένης σάρωσης.

8. Κάντε κλικ στο **Αποθήκευση** για να αποθηκεύσετε τις ρυθμίσεις και να κλείσετε το παράθυρο διαμόρφωσης.

   Ανάλογα με τις θέσεις που πρέπει να σαρωθούν, η σάρωση μπορεί να πάρει λίγο χρόνο. Εάν εντοπιστούν απειλές κατά τη διάρκεια της διαδικασίας σάρωσης, θα σας ζητηθεί να επιλέξετε τις ενέργειες που θα ληφθούν σχετικά με τα εντοπισμένα αρχεία.

Πληροφορίες σχετικά με τις επιλογές σάρωσης

Μπορείτε να βρείτε αυτές τις πληροφορίες χρήσιμες:

- Εάν δεν είστε εξοικειωμένοι με μερικούς από τους όρους, ελέγξτε τους στο γλωσσάριο . Μπορείτε επίσης να βρείτε χρήσιμες πληροφορίες από την αναζήτηση στο Internet.
- **Σάρωση δυνητικά ανεπιθύμητων εφαρμογών.** Επιλέξτε αυτήν την επιλογή για να σαρώσετε ανεπιθύμητες εφαρμογές. Μια δυνητικά κακόβουλη εφαρμογή (PUA) ή δυνητικά κακόβουλο πρόγραμμα (PUP) είναι ένα λογισμικό που συνήθως συνοδεύεται από δωρεάν λογισμικό και θα εμφανίσει αναδυόμενα παράθυρα ή θα εγκαταστήσει μια γραμμή εργαλείων στο προεπιλεγμένο πρόγραμμα περιήγησης. Μερικοί εφαρμογές θα αλλάξουν την αρχική σελίδα ή τη μηχανή αναζήτησης, ή άλλες θα εκτελέσουν πολλές διαδικασίες στο παρασκήνιο που επιβραδύνουν τον υπολογιστή ή θα εμφανίσουν πολλές διαφημίσεις. Αυτά τα προγράμματα μπορούν να εγκατασταθούν χωρίς τη συγκατάθεσή σας (επίσης αποκαλούμενα adware) ή θα συμπεριληφθούν από προεπιλογή στο κιτ γρήγορης εγκατάστασης (που υποστηρίζεται από διαφημίσεις).
- **Σάρωση αρχείων προς φύλαξη.** Συμπιεσμένα αρχεία που περιέχουν μολυσμένα αρχεία δεν αποτελούν άμεση απειλή για την ασφάλεια του συστήματός σας. Η απειλή μπορεί να επηρεάσει το σύστημά σας μόνο εάν το μολυσμένο αρχείο εξαχθεί από το συμπιεσμένο αρχείο και εκτελεστεί χωρίς να έχει ενεργοποιηθεί η σε πραγματικό χρόνο προστασία. Ωστόσο, συνιστάται να χρησιμοποιήσετε αυτή την επιλογή για να εντοπίζετε και να απομακρύνετε κάθε πιθανή απειλή, ακόμη και αν αυτή δεν αποτελεί άμεση απειλή.

Σύρετε το διακόπτη κατά μήκος της κλίμακας για να αποκλείσετε από τη σάρωση αρχείων που είναι μεγαλύτερα από μια δεδομένη τιμή σε MB (Megabyte).

Σημείωση
Η Σάρωση συμπισμένων αρχείων αυξάνει τον συνολικό χρόνο σάρωσης και απαιτεί περισσότερους πόρους συστήματος.

- **Σάρωση μόνο νέων και τροποποιημένων αρχείων.** Με τη σάρωση μόνο των νέων και τροποποιημένων αρχείων, μπορείτε να βελτιώσετε σημαντικά τη συνολική απόκριση του συστήματος με μία ελάχιστη έκπτωση στον τομέα της ασφάλειας.
- **Τομείς εκκίνησης σάρωσης.** Μπορείτε να ρυθμίσετε το Bitdefender για να σαρώσετε τους τομείς εκκίνησης του σκληρού σας δίσκου. Ο τομέας του σκληρού δίσκου περιέχει τον απαραίτητο κώδικα υπολογιστή για την ενεργοποίηση της διαδικασίας εκκίνησης. Όταν μία απειλή μολύνει τον τομέα εκκίνησης, ο δίσκος μπορεί να γίνει απρόσιτος και μπορεί να μην είστε σε θέση να ξεκινήσετε το σύστημά σας και να έχετε πρόσβαση στα δεδομένα σας.
- **Σάρωση μνήμης.** Επιλέξτε αυτήν την επιλογή για να σαρώνετε τα προγράμματα που τρέχουν στη μνήμη του συστήματος σας.
- **Σάρωση μητρώου.** Επιλέξτε αυτήν την επιλογή για να σαρώσετε το μητρώο. Το Windows Registry (Μητρώο) είναι μια βάση δεδομένων που αποθηκεύει ρυθμίσεις και επιλογές για τα στοιχεία του λειτουργικού συστήματος των Windows, καθώς και για τις εγκατεστημένες εφαρμογές.
- **Σάρωση cookies.** Ορίστε αυτήν την επιλογή για να σαρώσετε τα cookie που είναι αποθηκευμένα από προγράμματα περιήγησης στη συσκευή σας.
- **Σάρωση για keyloggers.** Επιλέξτε αυτήν την επιλογή για να σαρώσετε το σύστημά σας για τις εφαρμογές keylogger. Keyloggers καταγράφουν ό,τι πληκτρολογείτε στο πληκτρολόγιό σας και στέλνουν αναφορές μέσω του Διαδικτύου σε ένα κακόβουλο πρόσωπο (hacker). Ο χάκερ μπορεί να βρει ευαίσθητες πληροφορίες από τα κλεμμένα δεδομένα, όπως αριθμούς τραπεζικών λογαριασμών και κωδικούς πρόσβασης, και να το χρησιμοποιήσει για να αποκομίσει προσωπικά οφέλη.

Οδηγός σαρωτή Antivirus

Κάθε φορά που θα ξεκινήσετε μια σάρωση κατ' απαίτηση (για παράδειγμα, κάντε δεξί κλικ σε ένα φάκελο, δείξτε στο Bitdefender και επιλέξτε **Σάρωση με Bitdefender**), θα εμφανιστεί ο οδηγός Antivirus Scan του Bitdefender Ακολουθείστε τον οδηγό για να ολοκληρώσετε τη διαδικασία σάρωσης.

Σημείωση

Εάν δεν εμφανιστεί ο οδηγός σάρωσης, η σάρωση μπορεί να έχει ρυθμιστεί ώστε να τρέχει σιωπηλά στο παρασκήνιο. Αναζητήστε το εικονίδιο προόδου σάρωσης στην περιοχή ειδοποιήσεων. Μπορείτε να κάνετε κλικ σε αυτό το εικονίδιο για να ανοίξετε το παράθυρο σάρωσης και να δείτε την πρόοδο της σάρωσης.

Βήμα 1 - Πραγματοποιήστε σάρωση

Το Bitdefender θα ξεκινήσει τη σάρωση των επιλεγμένων αντικειμένων. Μπορείτε να δείτε σε πραγματικό χρόνο πληροφορίες σχετικά με την κατάσταση σάρωσης και στατιστικά στοιχεία (συμπεριλαμβανομένου του χρόνου που παρήλθε, μια εκτίμηση του χρόνου που απομένει και τον αριθμό των εντοπισμένων απειλών).

Περιμένετε το Bitdefender ολοκληρώσει τη σάρωση. Η διαδικασία σάρωσης μπορεί να πάρει λίγο χρόνο, ανάλογα με την πολυπλοκότητα της σάρωσης.

Διακοπή ή παύση της σάρωσης. Μπορείτε να σταματήσετε τη σάρωση όποτε θέλετε κάνοντας κλικ **ΔΙΑΚΟΠΗ** . Θα σας πάει κατευθείαν στο τελευταίο βήμα του οδηγού. Για να διακόψετε προσωρινά τη διαδικασία σάρωσης, απλά κάντε κλικ στο **ΠΑΥΣΗ**. Θα πρέπει να επιλέξετε **ΣΥΝΕΧΙΣΗ** για να συνεχίσετε τη σάρωση.

Συμπιεσμένα Αρχεία προστατευμένα με κωδικό ασφαλείας. Όταν εντοπιστεί συμπιεσμένο αρχείο που προστατεύεται με κωδικό πρόσβασης, ανάλογα με τις ρυθμίσεις σάρωσης, μπορεί να σας ζητηθεί να δώσετε τον κωδικό. Προστατευόμενα με κωδικό πρόσβασης συμπιεσμένα αρχεία δεν μπορεί να σαρωθούν εκτός και αν δώσετε τον κωδικό πρόσβασης. Διαθέσιμες επιλογές:

- **Κωδικός πρόσβασης.** Αν θέλετε το Bitdefender να σαρώσει το συμπιεσμένο αρχείο, επιλέξτε αυτήν την επιλογή και πληκτρολογήστε τον κωδικό πρόσβασης. Εάν δεν γνωρίζετε τον κωδικό πρόσβασης, επιλέξτε μία από τις άλλες επιλογές.

- **Να μην ερωτηθώ για κωδικό πρόσβασης και να παραλειφθεί αυτό το στοιχείο από την σάρωση.** Επιλέξτε αυτήν την επιλογή για να παρακάμψετε τη σάρωση αυτού του συμπιεσμένου αρχείου.
- **Παράλειψη όλων στοιχείων που προστατεύονται με κωδικό πρόσβασης χωρίς να σαρωθούν.** Επιλέξτε αυτήν την επιλογή εάν δεν θέλετε να ενοχλείστε σχετικά με προστατευμένα με κωδικό πρόσβασης αρχεία. Το Bitdefender δεν θα είναι σε θέση να τα σαρώσει, αλλά ένα ιστορικό θα φυλάσσεται στο αρχείο καταγραφής της σάρωσης.

Επιλέξτε την επιθυμητή επιλογή και κάντε κλικ στο **OK** για να συνεχίσετε τη σάρωση.

Βήμα 2 - Επιλέξτε ενέργειες

Στο τέλος της σάρωσης, θα σας ζητηθεί να επιλέξετε τις ενέργειες που πρέπει να ληφθούν για τα εντοπισμένα αρχεία, εάν εντοπισθούν κάποια μολυσμένα.

Σημείωση

Όταν εκτελέσετε μια γρήγορη σάρωση ή μια πλήρη σάρωση του συστήματος, το Bitdefender θα εκτελέσει αυτόματα τις προτεινόμενες ενέργειες σχετικά με τα ανιχνευμένα αρχεία κατά τη διάρκεια της σάρωσης. Εάν υπάρχουν παραμένουσες μη εξουδετερωμένες απειλές, θα σας ζητηθεί να επιλέξετε τις ενέργειες που πρέπει να εφαρμοστούν σε αυτές.

Τα μολυσμένα αντικείμενα εμφανίζονται σε ομάδες, με βάση την απειλή με την οποία έχουν μολυνθεί. Κάντε κλικ στο σύνδεσμο που αντιστοιχεί σε μια απειλή για να μάθετε περισσότερες πληροφορίες σχετικά με τα μολυσμένα αντικείμενα.

Μπορείτε να επιλέξετε μια καθολική ενέργεια που θα εκτελεστεί για όλα τα θέματα ή μπορείτε να επιλέξετε ξεχωριστές ενέργειες για κάθε κατηγορία θεμάτων. Μία ή περισσότερες από τις παρακάτω επιλογές μπορεί να εμφανιστεί στο μενού:

Κάντε τις απαραίτητες ενέργειες

Το Bitdefender θα εκτελέσει τις προτεινόμενες ενέργειες, ανάλογα με τον τύπο του ανιχνευμένου αρχείου:

- **Αρχεία που μολύνθηκαν.** Τα αρχεία που ανιχνεύονται ως μολυσμένα ταιριάζουν με μια βάση δεδομένων πληροφοριών απειλών στη βάση δεδομένων της Bitdefender. Το Bitdefender θα προσπαθήσει αυτόματα

να αφαιρέσει τον κώδικα κακόβουλου λογισμικού από το μολυσμένο αρχείο και να ανακατασκευάσει το αρχικό αρχείο. Αυτή η λειτουργία αναφέρεται ως απολύμανση.

Τα αρχεία που δεν μπορούν να απολυμανθούν μετακινούνται στην καραντίνα προκειμένου να απομονωθεί η μόλυνση. Αρχεία σε καραντίνα δεν μπορούν να εκτελεστούν ή να ανοίξουν. Ως εκ τούτου, ο κίνδυνος να μολυνθείτε εξαφανίζεται. Για περισσότερες πληροφορίες, ανατρέξτε στην "*Διαχείριση αρχείων σε καραντίνα*" (p. 107).

Σημαντικό

Για συγκεκριμένους τύπους απειλών, η επιδιόρθωση δεν είναι δυνατή επειδή το ανιχνευμένο αρχείο είναι εντελώς κακόβουλο. Σε τέτοιες περιπτώσεις, το μολυσμένο αρχείο διαγράφεται από το δίσκο.

- **Ύποπτα αρχεία.** Τα αρχεία ανιχνεύονται ως ύποπτα από την ευρετική ανάλυση. Τα ύποπτα αρχεία δεν μπορούν να επιδιορθωθούν, επειδή δεν είναι διαθέσιμη καμία ρουτίνα απολύμανσης. Θα μετακινηθούν στην καραντίνα για να αποτραπεί μια πιθανή μόλυνση.

  Από προεπιλογή, τα αρχεία σε καραντίνα αποστέλλονται αυτόματα στα εργαστήρια της Bitdefender, προκειμένου να αναλυθούν από τους ερευνητές απειλών της Bitdefender. Εάν επιβεβαιωθεί η ύπαρξη απειλής, απελευθερώνεται μια ενημέρωση πληροφοριών απειλής για να καταργηθεί η απειλή.

- **Συμπιεσμένα αρχεία που περιέχουν μολυσμένα αρχεία.**
  - Τα συμπιεσμένα αρχεία που περιέχουν μόνο μολυσμένα αρχεία διαγράφονται αυτόματα.
  - Εάν ένα αρχείο περιέχει τόσο μολυσμένα και καθαρά αρχεία, το Bitdefender θα προσπαθήσει να διαγράψει τα μολυσμένα αρχεία με την προϋπόθεση ότι μπορεί να ανακατασκευάσει το αρχείο με τα καθαρά αρχεία. Αν η ανοικοδόμηση του αρχείου δεν είναι δυνατή, θα ενημερωθείτε ότι δεν μπορεί να ληφθεί κανένα μέτρο ώστε να αποφευχθεί η απώλεια καθαρών αρχείων.

ΔΙΑΓΡΑΦΗ

Αφαιρεί τα εντοπισμένα αρχεία από το δίσκο.

Αν τα μολυσμένα αρχεία είναι αποθηκευμένα σε ένα αρχείο αρχειοθέτησης μαζί με καθαρά αρχεία, το Bitdefender θα προσπαθήσει

να διαγράψει τα μολυσμένα αρχεία και να ανακατασκευάσει το αρχείο με τα καθαρά αρχεία. Αν η ανοικοδόμηση του αρχείου δεν είναι δυνατή, θα ενημερωθείτε ότι δεν μπορεί να ληφθεί κανένα μέτρο ώστε να αποφευχθεί η απώλεια καθαρών αρχείων.

Καμία ενέργεια

Καμία ενέργεια δεν θα ληφθεί για τα εντοπισμένα αρχεία. Μετά την ολοκλήρωση της σάρωσης, μπορείτε να ανοίξετε το αρχείο καταγραφής της σάρωσης για να δείτε πληροφορίες σχετικά με αυτά τα αρχεία.

Κάντε κλικ στη **Συνέχεια** για να εφαρμοστούν οι καθορισμένες ενέργειες.

Βήμα 3 - Περίληψη

Όταν το Bitdefender τελειώσει την επιδιόρθωση των θεμάτων, τα αποτελέσματα της σάρωσης θα εμφανιστούν σε ένα νέο παράθυρο. Αν θέλετε ολοκληρωμένη πληροφορία για τη διαδικασία σάρωσης, επιλέξτε **ΕΜΦΑΝΙΣΗ ΑΡΧΕΙΟΥ ΚΑΤΑΓΡΑΦΗΣ** για να δείτε το αρχείο καταγραφής της σάρωσης.

Σημαντικό

Στις περισσότερες περιπτώσεις, το Bitdefender καθαρίζει με επιτυχία τα μολυσμένα αρχεία που εντοπίζει ή να απομονώνει τη μόλυνση. Ωστόσο, υπάρχουν ζητήματα που δεν μπορούν να επιλυθούν αυτόματα. Αν είναι απαραίτητο, κάντε επανεκκίνηση του συστήματός σας, προκειμένου να ολοκληρωθεί η διαδικασία καθαρισμού. Για περισσότερες πληροφορίες και οδηγίες σχετικά με το πώς να αφαιρέσετε το κακόβουλο λογισμικό με μη αυτόματο τρόπο, ανατρέξτε στο *"Αφαίρεση απειλών από το σύστημά σας"* (p. 217).

Έλεγχος ανίχνευσης αρχείων καταγραφής

Κάθε φορά που γίνεται μια σάρωση , δημιουργείται ένα αρχείο καταγραφής της σάρωσης και το Bitdefender καταγράφει τα εντοπισμένα προβλήματα στο παράθυρο Antivirus. Το αρχείο καταγραφής της σάρωσης περιέχει αναλυτικές πληροφορίες για τη διαδικασία σάρωσης που καταγράφηκε , όπως επιλογές σάρωσης, τον στόχο της σάρωσης, τις απειλές που βρέθηκαν και τις ενέργειες που λήφθηκαν σε αυτές τις απειλές.

Μπορείτε να ανοίξετε το αρχείο καταγραφής της σάρωσης απευθείας από τον οδηγό σάρωσης, αφού ολοκληρωθεί η σάρωση, πατώντας **ΕΜΦΑΝΙΣΗ ΑΡΧΕΙΟΥ ΚΑΤΑΓΡΑΦΗΣ**.

Για να ελέγξετε ένα αρχείο καταγραφής της σάρωσης ή οποιοδήποτε μόλυνση έχει εντοπιστεί σε μεταγενέστερο χρόνο:

1. Πατήστε **Ειδοποιήσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **All** επιλέξτε την ειδοποίηση που αφορά την τελευταία σάρωση.

   Εκεί μπορείτε να βρείτε όλα τα συμβάντα σάρωσης απειλών, συμπεριλαμβανομένων των απειλών που εντοπίζονται από τη σάρωση κατά την πρόσβαση, τις σαρώσεις που ξεκίνησε ο χρήστης και τις αλλαγές κατάστασης για αυτόματες σαρώσεις.
3. Στη λίστα ειδοποιήσεων, μπορείτε να ελέγξετε τις σαρώσεις που έχουν διεξαχθεί πρόσφατα. Κάντε κλικ σε μια ειδοποίηση για να δείτε λεπτομέρειες σχετικά με αυτή.
4. Για να ανοίξετε ένα αρχείο καταγραφής της σάρωσης, κάντε κλικ στην επιλογή **Προβολή αρχείου καταγραφής** (View log.).

4.1.3. Αυτόματη σάρωση των αφαιρούμενων μέσων

Το Bitdefender εντοπίζει αυτόματα όταν συνδέετε μια αφαιρούμενη συσκευή αποθήκευσης στη συσκευή σας και τη σαρώνει στο παρασκήνιο όταν είναι ενεργοποιημένη η επιλογή Autoscan. Αυτό συνιστάται για την αποφυγή μολύνσεων στη συσκευή σας.

Οι εντοπισθείσες συσκευές εμπίπτουν σε μία από αυτές τις κατηγορίες:

- CDs/DVDs
- Συσκευές αποθήκευσης USB, όπως φλασάκια και εξωτερικές μονάδες σκληρού δίσκου
- Αντιστοιχισθείσες (mapped) απομακρυσμένες μονάδες δικτύου

Μπορείτε να ρυθμίσετε την αυτόματη σάρωση χωριστά για κάθε κατηγορία συσκευών αποθήκευσης. Η Αυτόματη σάρωση αντιστοιχισμένων μονάδων δίσκων δικτύου είναι απενεργοποιημένη από προεπιλογή.

Πώς λειτουργεί?

Όταν ανιχνεύει μια αφαιρούμενη συσκευή αποθήκευσης, το Bitdefender ξεκινά τη σάρωση για απειλές στο παρασκήνιο (με την προυπόθεση ότι η αυτόματη σάρωση είναι ενεργοποιημένη για αυτό το είδος της συσκευής). θα ενημερωθείτε από ένα αναδυόμενο παράθυρο για την σύνδεση νέας συσκευής και την σάρωσή της.

Το Bitdefender εικονίδιο σάρωσης θα εμφανιστεί στην περιοχή ειδοποιήσεων. Μπορείτε να κάνετε κλικ σε αυτό το εικονίδιο για να ανοίξετε το παράθυρο σάρωσης και να δείτε την πρόοδο της σάρωσης.

Όταν η σάρωση ολοκληρωθεί, το παράθυρο αποτελεσμάτων σάρωσης εμφανίζεται για ενημερωθειτε εάν μπορείτε να έχετε πρόσβαση με ασφάλεια στα αρχεία του αφαιρούμενου μέσου.

Στις περισσότερες περιπτώσεις, το Bitdefender καταργεί αυτόματα τις απειλές ή απομονώνει τα μολυσμένα αρχεία στην καραντίνα. Εάν υπάρχουν παραμένουσες μη εξουδετερωμένες απειλές μετά τη σάρωση, θα σας ζητηθεί να επιλέξετε τις ενέργειες που πρέπει να εφαρμοστούν σε αυτές.

Σημείωση

Λάβετε υπόψη ότι δεν μπορεί να αναληφθεί δράση για μολυσμένα ή ύποπτα αρχεία που ανιχνεύονται σε CD / DVD. Ομοίως, καμία δράση δεν μπορεί να ληφθεί σε μολυσμένα ή ύποπτα αρχεία που ανιχνεύονται σε αντιστοιχισμένες μονάδες δίσκων δικτύου αν δεν έχετε τα κατάλληλα δικαιώματα.

Αυτή η πληροφορία μπορεί να σας είναι χρήσιμη:

- Παρακαλώ να είστε προσεκτικοί όταν χρησιμοποιείτε μολυσμένα CD / DVD, καθώς οι απειλές δεν μπορούν να αφαιρεθούν από το δίσκο (το μέσο αποθήκευσης είναι μόνο για ανάγνωση). Βεβαιωθείτε η σε πραγματικό χρόνο προστασία είναι ενεργοποιημένη για να αποτρέψει τη διάδοση απειλών στο σύστημά σας. Είναι βέλτιστη πρακτική η αντιγραφή όλων των πολύτιμων δεδομένων από τον δίσκο στο σύστημά σας και στη συνέχεια η απόρριψη του δίσκου.
- Σε ορισμένες περιπτώσεις, το Bitdefender μπορεί να μην είναι σε θέση να αφαιρέσει το κακόβουλο λογισμικό από συγκεκριμένα αρχεία λόγω νομικών ή τεχνικών περιορισμών. Ένα τέτοιο παράδειγμα είναι αρχεία που έχουν συμπιεστεί χρησιμοποιώντας μια ιδιόκτητη τεχνολογία (αυτό συμβαίνει επειδή το συμπιεσμένο αρχείο δεν θα μπορεί να αναπαραχθεί σωστά).

  Για να μάθετε πώς να αντιμετωπίζετε απειλές, ανατρέξτε στο *"Αφαίρεση απειλών από το σύστημά σας"* (p. 217).

Διαχείριση σάρωσης αφαιρούμενων μέσων

Για να διαχειριστείτε την αυτόματη σάρωση των αφαιρούμενων μέσων:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.

2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Επιλέξτε το παράθυρο **Ρυθμίσεις** .

Οι επιλογές σάρωσης είναι ρυθμισμένες εκ των προτέρων για τα καλύτερα αποτελέσματα ανίχνευσης. Εάν εντοπιστούν προσβεβλημένα αρχεία, το Bitdefender θα προσπαθήσει να τα απολυμάνει (να αφαιρέσει τον κώδικα του κακόβουλου λογισμικού) ή να τα μεταφέρει στην καραντίνα. Εάν αποτύχουν και οι δύο ενέργειες, ο οδηγός Antivirus Scan θα σας επιτρέψει να καθορίσετε άλλες ενέργειες που πρέπει να ληφθούν για τα προσβεβλημένα αρχεία. Οι επιλογές σάρωσης είναι τυποποιημένες και δεν μπορείτε να τις αλλάξετε.

Για καλύτερη προστασία, συνιστάται να ενεργοποιήσετε την επιλογή **Αυτόματη σάρωση** για όλους τους τύπους των αφαιρούμενων μέσων αποθήκευσης.

4.1.4. Σάρωση αρχείων

Το αρχείο hosts έρχεται από προεπιλογή με την εγκατάσταση του λειτουργικού σας συστήματος και χρησιμοποιείται για την αντιστοίχιση ονομάτων κεντρικού υπολογιστή σε διευθύνσεις IP κάθε φορά που κάνετε πρόσβαση σε μια νέα ιστοσελίδα, συνδεθείτε σε ένα FTP ή σε άλλους servers στο Διαδίκτυο. Είναι ένα απλό αρχείο κειμένου και κακόβουλα προγράμματα μπορεί να το τροποποιήσουν. Οι προχωρημένοι χρήστες ξέρουν πώς να το χρησιμοποιούν για να μπλοκάρουν τις ενοχλητικές διαφημίσεις, banners, και τα cookies.

Για να ρυθμίσετε τις παραμέτρους σάρωσης των αρχείων hosts:

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Επιλέξτε την καρτέλα **Advanced**.
3. Ενεργοποιήστε ή απενεργοποιήστε το **Σάρωση hosts file**.

4.1.5. Διαμόρφωση εξαιρέσεων σάρωσης.

Το Bitdefender επιτρέπει την εξαίρεση συγκεκριμένων αρχείων, φακέλων ή extensions αρχείων από τη σάρωση. Αυτή η λειτουργία έχει σκοπό να αποφεύγονται παρεμβολές στην εργασία σας και μπορεί επίσης να συμβάλει στη βελτίωση της απόδοσης του συστήματος. Εξαιρέσεις θα πρέπει να χρησιμοποιούνται από τους χρήστες που έχουν προχωρημένες γνώσεις υπολογιστών ή, αλλιώς, ακολουθώντας τις συστάσεις εκπροσώπου της Bitdefender.

Μπορείτε να ρυθμίσετε εξαιρέσεις που ισχύουν για την κατά την πρόσβαση σάρωση, για την κατόπιν αιτήματος σάρωση μόνο, ή και για τις δύο. Τα αντικείμενα που εξαιρούνται από την κατά την πρόσβαση σάρωση δεν θα σαρωθούν, είτε τα προσπελάζετε εσείς είτε μία εφαρμογή,

Σημείωση

Εξαιρέσεις ΔΕΝ θα ισχύουν για τη σάρωση με βάση τα συμφραζόμενα. Η Εξειδικευμένη σάρωση είναι ένα είδος σάρωσης on-demand : κάντε δεξί κλικ στο αρχείο ή στο φάκελο που θέλετε να σαρώσετε και επιλέξτε **Σάρωση με Bitdefender**.

Εξαίρεση αρχείων και φακέλων από τη σάρωση

Για να εξαιρέσετε συγκεκριμένα αρχεία και φακέλους από τη σάρωση:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στο παράθυρο **Ρυθμίσεις** , κάντε κλικ στην επιλογή **Διαχείριση εξαιρέσεων** .
4. Κάντε κλικ στο **+ Προσθήκη εξαίρεσης** .
5. Εισαγάγετε τη διαδρομή του φακέλου που θέλετε εκτός από τη σάρωση στο αντίστοιχο πεδίο.

   Εναλλακτικά, μπορείτε να πλοηγηθείτε στο φάκελο κάνοντας κλικ στο κουμπί περιήγησης στη δεξιά πλευρά της διεπαφής, επιλέξτε τον και κάντε κλικ στο **OK** .
6. Ενεργοποιήστε το διακόπτη δίπλα στη δυνατότητα προστασίας που δεν πρέπει να σαρώσει το φάκελο. Υπάρχουν τρεις επιλογές:
   - Antivirus
   - ONLINE ΠΡΟΛΗΨΗ ΑΠΕΙΛΩΝ
   - Advanced Threat Defense
7. Κάντε κλικ στο **Αποθήκευση** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

Εξαιρώντας επεκτάσεις από τη σάρωση

Όταν εξαιρείτε μια επέκταση αρχείου από τη σάρωση, το Bitdefender δεν θα σαρώσει πλέον αρχεία με αυτήν την επέκταση, ανεξάρτητα από τη θέση

τους στη συσκευή σας. Η εξαίρεση αυτή ισχύει και για τα αρχεία σε αφαιρούμενα μέσα, όπως: CD, DVD, συσκευές αποθήκευσης USB ή μονάδες δικτύου.

Σημαντικό
Να είστε προσεκτικοί όταν εξαιρείτε τις επεκτάσεις από τη σάρωση, επειδή τέτοιες εξαιρέσεις μπορούν να κάνουν τη συσκευή σας ευάλωτη σε απειλές.

Για να εξαιρέσετε extensions αρχείων από τη σάρωση:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στο παράθυρο **Ρυθμίσεις** , κάντε κλικ στην επιλογή **Διαχείριση εξαιρέσεων** .
4. Κάντε κλικ στο **+ Προσθήκη εξαίρεσης** .
5. Πληκτρολογήστε τις επεκτάσεις που θέλετε να εξαιρέσετε από τη σάρωση με μια τελεία πριν από αυτές, διαχωρίζοντάς τις με ερωτηματικά (;).

   txt;avi;jpg
6. Ενεργοποιήστε το διακόπτη δίπλα στη λειτουργία προστασίας που δεν πρέπει να σαρώσει την επέκταση.
7. Κάντε κλικ στο **Αποθήκευση**.

Διαμόρφωση εξαιρέσεων σάρωσης.

Εάν οι διαμορφωμένες εξαιρέσεις σάρωσης δεν είναι πλέον απαραίτητες, συνιστάται να διαγράψετε ή να απενεργοποιήσετε τις εξαιρέσεις σάρωσης.

Για να διαχειριστείτε τις εξαιρέσεις σάρωσης:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στο παράθυρο **Ρυθμίσεις** , κάντε κλικ στην επιλογή **Διαχείριση εξαιρέσεων** . Θα εμφανιστεί μια λίστα με όλες τις εξαιρέσεις σας.
4. Για να καταργήσετε ή να επεξεργαστείτε εξαιρέσεις σάρωσης, κάντε κλικ σε ένα από τα διαθέσιμα κουμπιά. Ακολουθήστε την εξής διαδικασία:

- Για να καταργήσετε μια καταχώριση από τη λίστα, κάντε κλικ στο κουμπί 🗑 δίπλα σε αυτήν.
- Για να επεξεργαστείτε μια καταχώριση από τον πίνακα, κάντε κλικ στο κουμπί **Επεξεργασία** δίπλα του. Εμφανίζεται ένα νέο παράθυρο όπου μπορείτε να αλλάξετε την επέκταση ή τη διαδρομή προς εξαίρεση και τη δυνατότητα ασφαλείας από την οποία θέλετε να εξαιρούνται, όπως απαιτείται. Κάντε τις απαραίτητες αλλαγές και στη συνέχεια επιλέξτε **ΤΡΟΠΟΠΟΙΗΣΗ**

4.1.6. Διαχείριση αρχείων σε καραντίνα

Το Bitdefender απομονώνει τα αρχεία που έχουν μολυνθεί από απειλές και που δεν μπορεί να τα καθαρίσει καθώς και τα ύποπτα αρχεία και τα τοποθετεί σε μια ασφαλή περιοχή με την ονομασία καραντίνα. Όταν μία απειλή είναι σε καραντίνα δεν μπορεί να κάνει οποιαδήποτε ζημιά, διότι δεν μπορεί να εκτελεστεί ή να διαβαστεί.

Από προεπιλογή, τα αρχεία σε καραντίνα αποστέλλονται αυτόματα στα εργαστήρια της Bitdefender, προκειμένου να αναλυθούν από τους ερευνητές απειλών της Bitdefender. Εάν επιβεβαιωθεί η ύπαρξη απειλής, απελευθερώνεται μια ενημέρωση πληροφοριών απειλής για να καταργηθεί η απειλή.

Επιπλέον, το Bitdefender σαρώνει τα αρχεία σε καραντίνα μετά από κάθε ενημέρωση. Τα καθαρισμένα αρχεία μετακινούνται αυτόματα πίσω στην αρχική τους θέση.

Για να ελέγξετε και να διαχειριστείτε αρχεία σε καραντίνα:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Μεταβείτε στο παράθυρο **Ρυθμίσεις** .

   Εδώ μπορείτε να δείτε το όνομα των αρχείων στην καραντίνα, την αρχική τους θέση και το όνομα των απειλών που εντοπίστηκαν.
4. Τα αρχεία σε καραντίνα διαχειρίζονται αυτόματα από το Bitdefender σύμφωνα με τις προεπιλεγμένες ρυθμίσεις καραντίνας.

   Αν και δεν συνιστάται, μπορείτε να προσαρμόσετε τις ρυθμίσεις της καραντίνας σύμφωνα με τις προτιμήσεις σας επιλέγοντας **Προβολή Ρυθμίσεων**.

Κάντε κλικ στους διακόπτες για να ενεργοποιήσετε ή να απενεργοποιήσετε:

Επανασάρωση καραντίνας μετά από ενημέρωση.
Κρατήστε αυτή την επιλογή ενεργοποιημένη για να ανιχνεύσει αυτόματα αρχεία σε καραντίνα μετά από κάθε ενημέρωση. Τα καθαρισμένα αρχεία μετακινούνται αυτόματα πίσω στην αρχική τους θέση.

Διαγραφή περιεχομένου παλαιοτέρου από 30 ημέρες
Αρχεία που βρίσκονται στην καραντίνα σε διάστημα μεγαλύτερο των 30 ημερών αυτόματα θα διαγράφονται.

Δημιουργείστε εξαίρεση για τα αποκατεστημένα αρχεία
Τα αρχεία που επαναφέρετε από την καραντίνα μετακινούνται πίσω στην αρχική τους θέση χωρίς να καθαριστούν και αποκλείονται αυτόματα από μελλοντικές σαρώσεις.

5. Για να διαγράψετε ένα αρχείο σε καραντίνα, επιλέξτε το και κάντε κλικ στο κουμπί**Διαγραφή**. Αν θέλετε να επαναφέρετε το αρχείο σε καραντίνα στην αρχική του θέση, επιλέξτε το και κάντε κλικ στο κουμπί **Επαναφορά**.

4.2. Advanced Threat Defense

Το Bitdefender Advanced Threat Defense είναι μια πρωτοποριακή δυναμική τεχνολογία ανίχνευσης που χρησιμοποιεί προηγμένες ευρετικές μεθόδους οι οποίες ανιχνεύουν νέες πιθανές απειλές σε πραγματικό χρόνο.

Το Advanced Threat Defense παρακολουθεί συνεχώς τις εφαρμογές που εκτελούνται στη συσκευή, αναζητώντας ενέργειες που μοιάζουν με απειλές. Κάθε μία από αυτές τις δράσεις βαθμολογείται και υπολογίζεται μια συνολική βαθμολογία για κάθε διαδικασία.

Ως μέτρο ασφάλειας, θα ενημερώνεστε κάθε φορά που ανιχνεύονται και αποκλείονται απειλές και ενδεχομένως κακόβουλες διαδικασίες.

Ενεργοποιώντας ή απενεργοποιώντας το Advanced Threat Defense

Για να ενεργοποιήσετε ή να απενεργοποιήσετε το Advanced Threat Defense:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ADVANCED THREAT DEFENSE** οθόνη, επιλέξτε **Άνοιγμα**.

3. Μεταβείτε στο παράθυρο **Ρυθμίσεις** και κάντε κλικ στο διακόπτη δίπλα στο **Bitdefender Advanced Threat Defense** .

Σημείωση
Για να διατηρήσετε το σύστημά σας προστατευμένο από ransomware και άλλες απειλές, σας συνιστούμε να διατηρείτε ενεργοποιημένο το Advanced Threat Defense όσο το δυνατόν περισσότερο.

Ελέγχοντας υπόπτες απειλές που ανιχνεύθηκαν

Όποτε εντοπίζονται απειλές ή δυνητικά κακόβουλες διαδικασίες, το Bitdefender θα τις αποκλείει για να αποτρέψει τη μόλυνση της συσκευής σας από ransomware ή άλλο κακόβουλο λογισμικό. Μπορείτε να ελέγξετε ανά πάσα στιγμή τη λίστα των κακόβουλων επιθέσεων που ανιχνεύθηκαν ακολουθώντας τα εξής βήματα:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ADVANCED THREAT DEFENSE** οθόνη, επιλέξτε **Άνοιγμα**.
3. Μεταβείτε στο παράθυρο **Threat Defense** .

   Εμφανίζονται οι επιθέσεις που εντοπίστηκαν τις τελευταίες 90 ημέρες. Για να βρείτε λεπτομέρειες σχετικά με τον τύπο ransomware που ανιχνεύθηκε, τη διαδρομή της κακόβουλης διαδικασίας ή εάν ο καθαρισμός ήταν επιτυχής, απλά κάντε κλικ σε αυτό.

Προσθέτοντας processes στις εξαιρέσεις

Μπορείτε να ρυθμίσετε τους κανόνες αποκλεισμού για τις αξιόπιστες εφαρμογές, έτσι ώστε το Advanced Threat Defense να μην τις αποκλείει θεωρώντας τις ως κακόβουλες.

Για να ξεκινήσετε την προσθήκη processes στη λίστα εξαιρέσεων για Advanced Threat Defense:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ADVANCED THREAT DEFENSE** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στο παράθυρο **Ρυθμίσεις** , κάντε κλικ στην επιλογή **Διαχείριση εξαιρέσεων** .
4. Κάντε κλικ στο **+ Προσθήκη εξαίρεσης** .
5. Εισαγάγετε τη διαδρομή του φακέλου που θέλετε εκτός από τη σάρωση στο αντίστοιχο πεδίο.

Εναλλακτικά, μπορείτε να πλοηγηθείτε στο εκτελέσιμο κάνοντας κλικ στο κουμπί περιήγησης στη δεξιά πλευρά της διεπαφής, επιλέξτε το και κάντε κλικ στο **OK** .

6. Ενεργοποιήστε το διακόπτη δίπλα στο **Advanced Threat Defense** .
7. Κάντε κλικ στο **Αποθήκευση**.

Ανίχνευση exploits

Ένας τρόπος που χρησιμοποιούν οι χάκερ για να παραβιάζουν τα συστήματα, είναι να επωφεληθούν από συγκεκριμένα σφάλματα ή τρωτά σημεία που υπάρχουν στο λογισμικό (εφαρμογές ή plugins) και το υλικό. Για να βεβαιωθείτε ότι η συσκευή σας παραμένει μακριά από τέτοιες επιθέσεις, που συνήθως εξαπλώνονται πολύ γρήγορα, το Bitdefender χρησιμοποιεί τις νεότερες τεχνολογίες κατά της εκμετάλλευσης.

Ενεργοποίηση ή απενεργοποίηση εντοπισμού exploit

Για να ενεργοποιήσετε ή να απενεργοποιήσετε τον εντοπισμό exploit:

- Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
- Στην **ADVANCED THREAT DEFENSE** οθόνη, επιλέξτε **Άνοιγμα**.
- Μεταβείτε στο παράθυρο **Ρυθμίσεις** και κάντε κλικ στο διακόπτη δίπλα στο **Ανίχνευση εκμετάλλευσης** για να ενεργοποιήσετε ή να απενεργοποιήσετε τη λειτουργία.

Σημείωση
Η επιλογή εντοπισμού exploit είναι ενεργοποιημένη από προεπιλογή.

4.3. ONLINE ΠΡΟΛΗΨΗ ΑΠΕΙΛΩΝ

Το Bitdefender Online Threat Prevention εξασφαλίζει μια εμπειρία Ασφαλούς περιήγησης προειδοποιώντας σας για πιθανές κακόβουλες ιστοσελίδες.

Το Bitdefender παρέχει διαδικτυακή προστασία σε πραγματικό χρόνο για:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

- Bitdefender Safepay™
- Opera

Για να ρυθμίσετε τις παραμέτρους του Online Threat Prevention:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ONLINE THREAT PREVENTION**, επιλέξτε **Ρυθμίσεις**.

Στις ενότητες **Προστασία Ιστού** , κάντε κλικ στους διακόπτες για ενεργοποίηση ή απενεργοποίηση:

- Το Web Attack Prevention αποκλείει τις απειλές που προέρχονται από το διαδίκτυο, συμπεριλαμβανομένων των downloads.
- Ο Σύμβουλος Αναζήτησης , ένα στοιχείο που βαθμολογεί τα αποτελέσματα των ερωτημάτων στη μηχανή αναζήτησής σας και τις συνδέσεις που δημοσιεύτηκαν στις ιστοσελίδες κοινωνικής δικτύωσης, τοποθετώντας ένα εικονίδιο δίπλα σε κάθε αποτέλεσμα:

  Δεν πρέπει να επισκέπτεστε αυτή την ιστοσελίδα.

  Αυτή η ιστοσελίδα μπορεί να περιέχει επικίνδυνο περιεχόμενο. Να είστε προσεκτικοί αν αποφασίσετε να την επισκεφτείτε.

  Αυτή είναι μια ασφαλής σελίδα για να επισκεφθείτε.

  ο Σύμβουλος Αναζήτησης βαθμολογεί τα αποτελέσματα αναζήτησης από τις ακόλουθες μηχανές αναζήτησης:
  - Google
  - Yahoo!
  - Bing
  - Baidu

  Ο Σύμβουλος Αναζήτησης βαθμολογεί τις συνδέσεις που δημοσιεύτηκαν στις ακόλουθες διαδικτυακές υπηρεσίες κοινωνικής δικτύωσης:
  - Facebook
  - Twitter
- Κρυπτογραφημένη σάρωση Web.

  Πιο εξελιγμένες επιθέσεις θα μπορούσαν να χρησιμοποιήσουν την ασφαλή κυκλοφορία στο Web για να παραπλανήσουν τα θύματά τους. Επομένως, σας συνιστούμε να συνεχίσετε να έχετε ενεργοποιημένη την επιλογή σάρωση κρυπτογραφημένης web κίνησης.
- Προστασία από απάτη.

- Προστασία από Phishing.

Κάντε κύλιση προς τα κάτω και θα μεταβείτε στην ενότητα **Πρόληψη απειλών δικτύου** . Εδώ έχετε την επιλογή **Πρόληψη απειλών δικτύου** . Για να κρατήσετε τη συσκευή σας μακριά από επιθέσεις από περίπλοκα κακόβουλα προγράμματα (όπως ransomware) μέσω της εκμετάλλευσης ευπαθειών, διατηρήστε αυτήν την επιλογή ενεργοποιημένη.

Μπορείτε να δημιουργήσετε μια λίστα με ιστότοπους, domains και διευθύνσεις IP που δεν θα σαρωθούν από τους μηχανισμούς του Bitdefender anti-threat, antiphishing, και antifraud engines. Η λίστα θα πρέπει να περιέχει μόνο ιστότοπους, domains και διευθύνσεις IP που εμπιστεύεστε πλήρως.

Για να διαμορφώσετε και να διαχειριστείτε ιστότοπους, domains και IP διευθύνσεις χρησιμοποιώντας το Online Threat Prevention που παρέχεται από το Bitdefender:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ONLINE THREAT PREVENTION**, επιλέξτε **Ρυθμίσεις**.
3. Κάντε κλικ στο **Διαχείριση εξαιρέσεων** .
4. Κάντε κλικ στο **+ Προσθήκη εξαίρεσης** .
5. Πληκτρολογήστε στο αντίστοιχο πεδίο το όνομα του ιστότοπου, το όνομα του τομέα ή τη διεύθυνση IP που θέλετε να προσθέσετε στις εξαιρέσεις.
6. Κάντε κλικ στον διακόπτη δίπλα στο **Online Threat Prevention** .
7. Για να καταργήσετε μια καταχώριση από τη λίστα, κάντε κλικ στο κουμπί δίπλα σε αυτήν.

   Κάντε κλικ στο **Αποθήκευση** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

Bitdefender ειδοποιήσεις στο πρόγραμμα πλοήγησης

Κάθε φορά που προσπαθείτε να επισκεφθείτε μια ιστοσελίδα που έχει ταξινομηθεί ως μη ασφαλής, η ιστοσελίδα έχει αποκλειστεί και μια προειδοποιητική σελίδα εμφανίζεται στο πρόγραμμα πλοήγησης σας.

Η σελίδα περιέχει πληροφορίες όπως η διεύθυνση URL της ιστοσελίδας και την εντοπισμένη απειλή.

Θα πρέπει να αποφασίσετε τι θα κάνετε στη συνέχεια. Διαθέσιμες επιλογές:

- Πλοηγηθείτε μακριά από τον ιστότοπο, κάνοντας κλικ στο κουμπί **ΕΠΙΣΤΡΟΦΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ**.
- Προχωρήστε στην ιστοσελίδα, παρά την προειδοποίηση, κάνοντας κλικ **I understand the risks, take me there anyway**.
- Εάν είστε βέβαιοι ότι ο συγκεκριμένος ιστότοπος είναι ασφαλής, κάντε κλικ στο κουμπί **ΥΠΟΒΟΛΗ** για να το προσθέσετε σε εξαιρέσεις. Σας συνιστούμε να προσθέσετε μόνο ιστότοπους που εμπιστεύεστε πλήρως.

4.4. Antispam

Το spam είναι ένας όρος που χρησιμοποιείται για να περιγράψει ανεπίκλητα μηνύματα ηλεκτρονικού ταχυδρομείου. Spam είναι ένα αυξανόμενο πρόβλημα, τόσο για τους ιδιώτες όσο και για τις οργανώσεις. Δεν είναι όμορφο, Δεν θα θέλατε τα παιδιά σας να το δούν, μπορεί να σας απολύσουν (για σπατάλη πάρα πολύ χρόνου ή από τη λήψη πορνό στο εταιρικό σας e-mail) και δεν μπορείτε να σταματήσετε κάποιους από την αποστολή. Το επόμενο καλύτερο πράγμα για αυτό είναι, προφανώς, να σταματήσετε τη λήψη του. Δυστυχώς, το Spam έρχεται σε μια ευρεία ποικιλία σχημάτων και μεγεθών, και υπάρχει πολύ από αυτή.

Το Bitdefender Antispam χρησιμοποιεί αξιοσημείωτες τεχνολογικές καινοτομίες και βιομηχανικά πρότυπα φίλτρα antispam για να εξαλείψει το spam πριν φτάσει στο Inbox του χρήστη. Για περισσότερες πληροφορίες, ανατρέξτε στην "*Τα εσωτερικά των Antispam*" (p. 114).

Η Προστασία Antispam του Bitdefender είναι διαθέσιμη μόνο για τους πελάτες e-mail που είναι ρυθμισμένα ώστε να λαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου μέσω του πρωτοκόλλου POP3. Το POP3 είναι ένα από τα πιο ευρέως χρησιμοποιούμενα πρωτόκολλα για τη λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου από ένα διακομιστή αλληλογραφίας.

Σημείωση
Το Bitdefender δεν παρέχει προστασία antispam για λογαριασμούς e-mail που έχετε πρόσβαση μέσω μιας διαδικτυακής υπηρεσίας e-mail.

Τα ανεπιθύμητα μηνύματα ανιχνεύονται από το Bitdefender και σημειώνονται με το πρόθεμα [spam] στη γραμμή του θέματος. Το Bitdefender μετακινεί αυτόματα τα ανεπιθύμητα μηνύματα σε ένα συγκεκριμένο φάκελο, ως εξής:

- Στο Microsoft Outlook, τα ανεπιθύμητα μηνύματα μετακινούνται σε ένα φάκελο **Spam**, που βρίσκεται στο φάκελο **Διεγραμμένα Στοιχεία**. Ο φάκελος **Spam** δημιουργείται όταν ένα e-mail χαρακτηρίζεται ως ανεπιθύμητο.
- Στο Mozilla Thunderbird, τα ανεπιθύμητα μηνύματα μετακινούνται σε ένα φάκελο **Spam**, που βρίσκεται στο φάκελο **Trash**. Ο φάκελος **Spam** δημιουργείται όταν ένα e-mail χαρακτηρίζεται ως ανεπιθύμητο.

Αν χρησιμοποιείτε άλλες εφαρμογές (clients) ηλεκτρονικού ταχυδρομείου, θα πρέπει να δημιουργήσετε έναν κανόνα για να μετακινήσετε τα μηνύματα e-mail που το Bitdefender χαρακτηρίζει ως [spam] (ανεπιθύμητα) από σε προσαρμοσμένο φάκελο καραντίνας . Όταν οι Deleted Item ή Trash σβηστούν, τότε θα σβηστεί επίσης και ο φάκελος Spam. Παρόλα αυτά, ο φάκελος Spam θα ξαναδημιουργηθεί μόλις ένα e-mail χαρακτηριστεί ως ανεπιθύμητο.

4.4.1. Τα εσωτερικά των Antispam

Φίλτρα προστασίας από spam

Το Bitdefender Antispam μηχανή ενσωματώνει την cloud προστασία και άλλα πολλά διαφορετικά φίλτρα που εξασφαλίζουν ότι τα Εισερχόμενα είναι ελεύθερα από Spam (ανεπιθύμητα μηνύματα), όπως λίστα φίλων , Spammers Λίστα και φίλτρο σετ χαρακτήρων.

Κατάλογος Φίλων / κατάλογος Spammers

Οι περισσότεροι άνθρωποι επικοινωνούν τακτικά με μια ομάδα ανθρώπων ή ακόμα λαμβάνουν μηνύματα από εταιρείες ή οργανισμούς στον ίδιο τομέα. Χρησιμοποιόντας τον **κατάλογος φίλων ή spammers**, μπορείτε εύκολα να ταξινομήσετε από ποιούς ανθρώπους θέλετε να λαμβάνετε e-mail (φίλοι) ανεξάρτητα από τι περιέχει το μήνυμα, ή από ποιούς ανθρώπους δεν θέλετε να ακούσετε ποτέ ξανά (spammers).

Σημείωση

Σας συνιστούμε να προσθέσετε τα ονόματα των φίλων σας και τις διευθύνσεις ηλεκτρονικού ταχυδρομείου στη **Λίστα Φίλων**. Το Bitdefender δεν μπλοκάρει μηνύματα από τα άτομα στη λίστα. Γι' αυτό, η προσθήκη φίλων διασφαλίζει τη διέλευση νόμιμων μηνυμάτων ηλεκτρονικής αλληλογραφίας.

Φίλτρο Σύνολοχαρακτήρων

Πολλά ανεπιθύμητα μηνύματα γραμμένα σε κυριλλικά και / ή ασιατικά σύνολα χαρακτήρων. Το Φίλτρο Σύνολοχαρακτήρων ανιχνεύει τέτοιου είδους μηνύματα και τα σημειώνει ως SPAM.

Λειτουργία Antispam

Ο μηχανισμός Antispam του Bitdefender χρησιμοποιεί όλα τα φίλτρα antispam συνδυαστικά για να καθοριστεί αν ένα συγκεκριμένο μήνυμα ηλεκτρονικού ταχυδρομείου θα πρέπει να μπει στα **Εισερχόμενα** σας ή όχι.

Κάθε e-mail που έρχεται από το Διαδίκτυο ελέγχεται πρώτα με το φίλτρο Λίστα Φίλων/Λίστα Spammers. Εάν διαπιστωθεί ότι η διεύθυνση του αποστολέα είναι στη Λίστα Φίλων το e-mail μεταφέρεται κατευθείαν στα **Εισερχόμενα** σας.

Σε αντίθετη περίπτωση, το φίλτρο της Λίστας Spammers θα αναλάβει το e-mail για να ελέγξει αν η διεύθυνση του αποστολέα βρίσκεται στη λίστα του. Εάν γίνει μια αντιστοιχία, το e-mail θα σημανθεί ως SPAM και θα μετακινηθεί στο φάκελο **Spam**.

Αλλιώς, το φίλτρο Συνολοχαρακτήρων θα ελέγξει αν το e-mail είναι γραμμένο σε κυριλλικούς ή ασιατικούς χαρακτήρες. Αν ναι το e-mail θα σημανθεί ως SPAM και θα μετακινηθεί στο φάκελο **Spam**.

Σημείωση

Αν το e-mail είναι χαρακτηρισμένο ως σεξουαλικού χαρακτήρα στη γραμμή θέματος, το Bitdefender θα το θεωρήσει SPAM.

Υποστηριζόμενοι πελάτες e-mail και πρωτόκολλα

Η προστασία Antispam παρέχεται για όλους τους POP3/SMTP e-mail πελάτες. Η γραμμή εργαλείων Antispam του Bitdefender όμως έχει ενσωματωθεί μόνο σε:

- Microsoft Outlook εκδόσεις 2007, 2010, 2013 / 2016
- Mozilla Thunderbird 14 ή μεταγενέστερο

4.4.2. Ενεργοποίηση ή απενεργοποίηση της antispam προστασίας

Η προστασία Antispam είναι ενεργοποιημένη από προεπιλογή.

Για να ενεργοποιήσετε ή να απενεργοποιήσετε τη δυνατότητα Anti Spam:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ANTISPAM**, θέστε on ή off τον διακόπτη.

4.4.3. Χρησιμοποιώντας τη γραμμή εργαλείων antispam στο παράθυρο του ηλεκτρονικού ταχυδρομείου σας

Στην επάνω περιοχή του παραθύρου πελάτη ηλεκτρονικού ταχυδρομείου σας, μπορείτε να δείτε τη γραμμή εργαλείων Antispam. Η γραμμή εργαλείων Antispam σας βοηθά να διαχειριστείτε την antispam προστασία απευθείας από την εφαρμογή ηλεκτρονικού ταχυδρομείου σας. Μπορείτε να διορθώσετε εύκολα το Bitdefender αν χαρακτηρίσει ένα νόμιμο μήνυμα ως spam.

Σημαντικό

Το Bitdefender ενσωματώνεται στις πιο συχνά χρησιμοποιούμενες εφαρμογές ηλεκτρονικού ταχυδρομείου μέσω της εύχρηστης γραμμής εργαλείων antispam. Για μια πλήρη λίστα των υποστηριζόμενων εφαρμογών ηλεκτρονικού ταχυδρομείου, παρακαλούμε ανατρέξτε στο *"Υποστηριζόμενοι πελάτες e-mail και πρωτόκολλα"* (p. 115).

Κάθε πλήκτρο από την Bitdefender γραμμή εργαλείων θα εξηγηθεί παρακάτω:

Ρυθμίσεις - Ανοίγει ένα παράθυρο όπου μπορείτε να ρυθμίσετε τα φίλτρα antispam και τις ρυθμίσεις της γραμμής εργαλείων.

είναι spam - υποδηλώνει ότι το επιλεγμένο e-mail είναι ανεπιθύμητο. Το e-mail θα μεταφέρεται αμέσως στο φάκελο **Spam** (Ανεπιθύμητη αλληλογραφία). Αν ενεργοποιηθούν οι υπηρεσίες cloud antispam, το μήνυμα αποστέλλεται στο Bitdefender Cloud για περαιτέρω ανάλυση.

Not Spam - υποδηλώνει ότι το επιλεγμένο ηλεκτρονικό ταχυδρομείο δεν είναι spam και το Bitdefender δεν θα πρέπει να το χαρακτηρίσει σαν spam Το e-mail θα πρέπει να μετακινηθεί από τον **Spam** φάκελο στον κατάλογο **Εισερχόμενα** . Αν ενεργοποιηθούν οι υπηρεσίες cloud antispam, το μήνυμα αποστέλλεται στο Bitdefender Cloud για περαιτέρω ανάλυση.

Σημαντικό

Το **Not Spam** πλήκτρο ενεργοποιείται, όταν επιλέξετε ένα μήνυμα χαρακτηρισμένο ως spam από το Bitdefender (συνήθως αυτά τα μηνύματα βρίσκονται στο **Spam** φάκελο).

Προσθήκη Spammer - προσθέτει τον αποστολέα του επιλεγμένου ηλεκτρονικού ταχυδρομείου στη λίστα spammers. Μπορεί να χρειαστεί να κάνετε κλικ στο κουμπί **OK** για να αποδεχτείτε. Τα μηνύματα e-mail που ελήφθησαν από τις διευθύνσεις της λίστας Spammers επισημαίνονται αυτόματα ως [spam]..

Προσθήκη Φίλου - προσθέτει τον αποστολέα του επιλεγμένου ηλεκτρονικού ταχυδρομείου στη λίστα Φίλων. Μπορεί να χρειαστεί να κάνετε κλικ στο κουμπί **OK** για να αποδεχτείτε. Θα λαμβάνετε πάντα μηνύματα e-mail από την διεύθυνση αυτή ανεξάρτητα από το περιεχόμενο.

Το **Spammers** ανοίγει την **Spammers list** (λίστα Spammers) που περιέχει όλες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου από τις οποίες δεν θέλετε να λάβετε μηνύματα, ανεξάρτητα από το περιεχόμενό τους. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Διαμόρφωση του καταλόγου Spammers"* (p. 120).

Το **Φίλοι** ανοίγει την **Λίστα Φίλων** που περιέχει όλες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου από τις οποίες θέλετε πάντα να λαμβάνετε τα e-mail, ανεξάρτητα από το περιεχόμενό τους. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Διαμόρφωση του καταλόγου φίλων"* (p. 119).

Υπόδειξη σφαλμάτων ανίχνευσης

Εάν χρησιμοποιείτε μια υποστηριζόμενη εφαρμογή ηλεκτρονικού ταχυδρομείου, μπορείτε εύκολα να διορθώσετε το antispam φίλτρο (αναφέροντας ποια μηνύματα e-mail δεν θα έπρεπε να έχουν σημανθεί ως [spam]). Με αυτόν τον τρόπο συμβάλλει στη βελτίωση της αποτελεσματικότητας του φίλτρου antispam. Ακολουθείστε αυτά τα βήματα:

1. Ανοίξτε την εφαρμογή του ηλεκτρονικού ταχυδρομείου σας.
2. Πηγαίνετε στο φάκελο ανεπιθύμητης αλληλογραφίας όπου μετακινούνται τα μηνύματα spam.
3. Επιλέξτε το νόμιμο μήνυμα που εσφαλμένα χαρακτηρίστηκε ως [spam] από το Bitdefender.
4. Κάντε κλικ στο **Προσθήκη στους φίλους κουμπί** στην Bitdefender antispam γραμμή εργαλείων για να προσθέσετε τον αποστολέα στη λίστα Φίλων. Μπορεί να χρειαστεί να κάνετε κλικ στο κουμπί **OK** για να αποδεχτείτε. Θα λαμβάνετε πάντα μηνύματα e-mail από την διεύθυνση αυτή ανεξάρτητα από το περιεχόμενο.

5. Κάντε κλικ στο **Not Spam** κουμπί στην Bitdefender antispam μπάρας εργαλείων (συνήθως βρίσκεται στο πάνω μέρος του παραθύρου της εφαρμογής ηλεκτρονικού ταχυδρομείου). Το μήνυμα ηλεκτρονικού ταχυδρομείου θα μετακινηθεί στο φάκελο Εισερχόμενα.

Υποδεικνύοντας μη ανιχνευθέντα spam μηνύματα

Εάν χρησιμοποιείτε μία υποστηριζόμενη εφαρμογή ηλεκτρονικού ταχυδρομείου, μπορείτε εύκολα να υποδείξετε ποιά e- mail θα έπρεπε να είχαν ανιχνευθεί ως spam. Με αυτόν τον τρόπο συμβάλλει στη βελτίωση της αποτελεσματικότητας του φίλτρου antispam. Ακολουθείστε αυτά τα βήματα:

1. Ανοίξτε την εφαρμογή του ηλεκτρονικού ταχυδρομείου σας.
2. Πηγαίνετε στο φάκελο Εισερχόμενα.
3. Επιλέξτε τα μη ανιχνευθέντα spam μηνύματα
4. Κάντε κλικ στο **Is Spam** κουμπί στην Bitdefender antispam μπάρα εργαλείων (συνήθως βρίσκεται στο πάνω μέρος του παραθύρου της εφαρμογής ηλεκτρονικού ταχυδρομείου). Αυτά σημειώνονται αμέσως ως [spam] και μεταφέρονται στο φάκελο ανεπιθύμητης αλληλογραφίας.

Διαμόρφωση ρυθμίσεων της γραμμής εργαλείων

Για να διαμορφώσετε τις ρυθμίσεις της γραμμής εργαλείων antispam για την εφαρμογή e-mail σας, κάντε κλικ στην επιλογή **Settings** κουμπί στη γραμμή εργαλείων και στη συνέχεια στην **Toolbar Settings** καρτέλα.

Εδώ έχετε τις εξής επιλογές:

- **Σήμανση ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου ως «αναγνωσμένα»** - σηματοδοτεί τα spam μηνύματα ως αναγνωσμένα αυτόματα, έτσι ώστε να μην ενοχλούν όταν φτάσουν.
- Μπορείτε να επιλέξετε αν θέλετε ή όχι να εμφανίσετε τα παράθυρα επιβεβαίωσης όταν κάνετε κλικ στο **Προσθήκη Spammer** και **Προσθήκη φίλου** κουμπιά στην γραμμή εργαλείων antispam .

  Τα Παράθυρα επιβεβαίωσης μπορεί να αποτρέψουν την τυχαία προσθήκη αποστολέων e-mail στους φίλους / λίστα spammers.

4.4.4. Διαμόρφωση του καταλόγου φίλων

Τα **Friends list** είναι ένας κατάλογος όλων των διευθύνσεων ηλεκτρονικού ταχυδρομείου από τις οποίες θέλετε πάντα να λάβετε τα μηνύματα, ανεξάρτητα από το περιεχόμενό τους. Τα μηνύματα από τους φίλους σας δεν χαρακτηρίζονται ως spam, ακόμα κι αν το περιεχόμενο μοιάζει με spam.

Σημείωση

Κάθε αλληλογραφία που προέρχεται από μια διεύθυνση που περιέχονται στη **Λίστα φίλων** , αυτόματα θα παραδοθεί στα Εισερχόμενα σας χωρίς περαιτέρω μεταποίηση.

Για να διαμορφώσετε και διαχειριστείτε τη λίστα φίλων :

- Εάν χρησιμοποιείτε το Microsoft Outlook ή το Thunderbird, κάντε κλικ στο **Friends** κουμπί στο Bitdefender antispam toolbar.
- Εναλλακτικά:
  1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
  2. Στο παράθυρο **ANTISPAM**, πατήστε **Ρυθμίσεις**.
  3. Μεταβείτε στο παράθυρο **Διαχείριση φίλων** .

Για να προσθέσετε μια διεύθυνση ηλεκτρονικού ταχυδρομείου, επιλέξτε την επιλογή **Email address**, εισάγετε τη διεύθυνση και πατήστε έπειτα **ADD**. Σύνταξη: name@domain.com.

Για να προσθέσετε όλες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου από ένα συγκεκριμένο domain **Domain name**, εισάγετε το όνομα του domain και πατήστε έπειτα **ADD**. Σύνταξη

- @domain.com και domain.com - όλα τα εισερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου από το domain.com θα φθάσουν στο **Inbox** σας ανεξάρτητα από το περιεχόμενό τους:
- domain - όλα τα λαμβανόμενα μηνύματα ηλεκτρονικού ταχυδρομείου από domain (ανεξάρτητα από τα επιθέματα Domain) θα χαρακτηριστούν ως SPAM
- com - όλα τα λαμβανόμενα μηνύματα ηλεκτρονικού ταχυδρομείου που έχουν το επίθεμα com Domains θα χαρακτηριστούν ως SPAM;

Σας προτείνουμε να να αποφύγετε την προσθήκη ολόκληρων Domains, αλλά αυτό μπορεί να είναι χρήσιμο σε μερικές περιπτώσεις. Παραδείγματος χάριν, μπορείτε να προσθέσετε το Domain ηλεκτρονικού ταχυδρομείου

της επιχείρησης που εργάζεστε για, ή εκείνο των εμπίστων συνεργατών σας.

Για να διαγράψετε ένα στοιχείο από τη λίστα, κάντε κλικ στο αντίστοιχο κουμπί δίπλα του. Για να διαγράψετε όλες τις καταχωρίσεις από τη λίστα, κάντε κλικ στο **Εκκαθάριση λίστας** .

Μπορείτε να αποθηκεύσετε τη λίστα φίλων σε ένα αρχείο, ώστε να μπορείτε να τη χρησιμοποιήσετε σε άλλη συσκευή ή μετά την επανεγκατάσταση του προϊόντος. Για να σώσετε τη λίστα φίλων, πατήστε το κουμπί **Save** και σώστε τη λίστα στην επιθυμητή θέση. Το αρχείο θα έχει μία .bwl επέκταση.

Για να φορτώσετε μια λίστα φίλων που έχετε ήδη αποθηκεύσει, κάντε κλικ στο **Φόρτωση** και ανοίξτε το αντίστοιχο αρχείο .bwl . Για να επαναφέρετε το περιεχόμενο της υπάρχουσας λίστας κατά τη φόρτωση μιας προηγούμενης αποθηκευμένης λίστας, επιλέξτε το πλαίσιο δίπλα στο **Αντικατάσταση τρέχουσας λίστας** .

4.4.5. Διαμόρφωση του καταλόγου Spammers

Το **Spammers list** είναι ένας κατάλογος όλων των διευθύνσεων ηλεκτρονικού ταχυδρομείου από τις οποίες δεν θέλετε να λάβετε τα μηνύματα, ανεξάρτητα από το περιεχόμενό τους. Οποιοδήποτε μήνυμα ηλεκτρονικού ταχυδρομείου που παραλαμβάνεται από μια διεύθυνση που περιλαμβάνεται στα **Spammers list** θα χαρακτηριστεί αυτόματα ως SPAM, χωρίς περαιτέρω επεξεργασία.

Για να διαμορφώσετε και διαχειριστείτε τη λίστα Spammers :

- Εάν χρησιμοποιείτε το Microsoft Outlook ή το Thunderbird, κάντε κλικ **Spammers** στην Bitdefender antispam toolbar που είναι ενσωματωμένο στον client του ηλεκτρονικού σας ταχυδρομείου.
- Εναλλακτικά:
  1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
  2. Στο παράθυρο **ANTISPAM**, πατήστε **Ρυθμίσεις**.
  3. Μεταβείτε στο παράθυρο **Διαχείριση ανεπιθύμητων μηνυμάτων** .

Για να προσθέσετε μια διεύθυνση ηλεκτρονικού ταχυδρομείου, επιλέξτε την επιλογή **Email address**, εισάγετε τη διεύθυνση και πατήστε έπειτα **ADD**. Σύνταξη: name@domain.com.

Για να προσθέσετε όλες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου από ένα συγκεκριμένο domain **Domain name**, εισάγετε το όνομα του domain και πατήστε έπειτα **ADD**. Σύνταξη

- @domain.com και domain.com - όλα τα εισερχόμενα μηνύματα ηλεκτρονικού ταχυδρομείου από το domain.com θα φθάσουν στο **Inbox** σας ανεξάρτητα από το περιεχόμενό τους:
- domain - όλα τα λαμβανόμενα μηνύματα ηλεκτρονικού ταχυδρομείου από domain (ανεξάρτητα από τα επιθέματα Domain) θα χαρακτηριστούν ως SPAM
- com - όλα τα λαμβανόμενα μηνύματα ηλεκτρονικού ταχυδρομείου που έχουν το επίθεμα com Domains θα χαρακτηριστούν ως SPAM.

Σας προτείνουμε να να αποφύγετε την προσθήκη ολόκληρων Domains, αλλά αυτό μπορεί να είναι χρήσιμο σε μερικές περιπτώσεις.

Προειδοποίηση

Μην προσθέστε Domains των νόμιμων βασισμένων στο WEB υπηρεσιών ηλεκτρονικού ταχυδρομείου (όπως Yahoo, Gmail, Hotmail ή άλλο) στον κατάλογο Spammers. Διαφορετικά, τα μηνύματα ηλεκτρονικού ταχυδρομείου που παραλαμβάνονται από οποιοδήποτε εγγραμμένο χρήστη μιας τέτοιας υπηρεσίας θα ανιχνευθούν ως spam. Εάν, παραδείγματος χάριν, προσθέτετε το yahoo.com στο Spammers κατάλογο, όλα τα μηνύματα ηλεκτρονικού ταχυδρομείου που προέρχονται από διευθύνσεις του yahoo.com θα χαρακτηριστούν ως [spam] .

Για να διαγράψετε ένα στοιχείο από τη λίστα, κάντε κλικ στο αντίστοιχο κουμπί δίπλα του. Για να διαγράψετε όλες τις καταχωρίσεις από τη λίστα, κάντε κλικ στο **Εκκαθάριση λίστας** .

Μπορείτε να αποθηκεύσετε τη λίστα Spammers σε ένα αρχείο, ώστε να μπορείτε να τη χρησιμοποιήσετε σε άλλη συσκευή ή μετά την επανεγκατάσταση του προϊόντος. Για να σώσετε τον κατάλογο Spammers, πατήστε το κουμπί **Save** και σώστε τη λίστα στην επιθυμητή θέση. Το αρχείο θα έχει μία .bwl επέκταση.

Για να φορτώσετε έναν προηγουμένως σωσμένο κατάλογο Spammers, πατήστε το **LOAD** και ανοίξτε το αντίστοιχο .bwl αρχείο. Για να επαναρυθμίσετε το περιεχόμενο του υπάρχοντος καταλόγου κατά τη φόρτωση ενός προηγουμένως σωσμένου καταλόγου, επιλέξτε **Overwrite current list**.

4.4.6. Διαμόρφωση των τοπικών φίλτρων antispam

Όπως περιγράφεται στο *"Τα εσωτερικά των Antispam"* (p. 114), το Bitdefender χρησιμοποιεί έναν συνδυασμό διαφορετικών φίλτρων antispam για να προσδιορίσει το spam. Τα φίλτρα antispam είναι προ-ρυθμισμένα για πιό αποδοτική προστασία.

Σημαντικό

Ανάλογα με το κατά πόσον λαμβάνετε ή όχι νόμιμα ηλεκτρονικά ταχυδρομεία που γράφονται σε ασιατικούς ή κυριλλικούς χαρακτήρες, θέστε εκτός λειτουργίας ή ενεργοποιήστε τη ρύθμιση που εμποδίζει αυτόματα τέτοια ηλεκτρονικά ταχυδρομεία. Η αντίστοιχη ρύθμιση είναι εκτός λειτουργίας στις τοπικοποιημένες εκδόσεις του προγράμματος που χρησιμοποιούν τέτοια charsets (παραδείγματος χάριν, στη ρωσική ή κινεζική εκδοχή).

Διαμόρφωση των τοπικών φίλτρων antispam:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ANTISPAM**, πατήστε **Ρυθμίσεις**.
3. Μεταβείτε στο παράθυρο **Ρυθμίσεις** και κάντε κλικ στους αντίστοιχους διακόπτες ενεργοποίησης ή απενεργοποίησης.

Εάν χρησιμοποιείτε το Microsoft Outlook ή το Thunderbird, μπορείτε να διαμορφώσετε τα τοπικά φίλτρα antispam άμεσα από την εφαρμογή ηλεκτρονικού ταχυδρομείου σας. Κάντε κλικ στο ⚙ **Settings** κουμπί στην Bitdefender antispam toolbar (συνήθως βρίσκεται στο πάνω μέρος του παραθύρου της εφαρμογής ηλεκτρονικού ταχυδρομείου) και κατόπιν την καρτέλλα **Antispam Filters** tab.

4.4.7. Διαμόρφωση ρυθμίσεων cloud

Η ανίχνευση cloud κάνει χρήση των Bitdefender Cloud υπηρεσιών για να σας παρέχει αποτελεσματική και πάντα ενημερωμένη προστασία antispam.

Η προστασίας cloud λειτουργεί για όσο διάστημα κρατάτε το Bitdefender Antispam ενεργοποιημένο.

Δείγματα των νόμιμων ή spam e-mails μπορεί να υποβληθούν στο Bitdefender Cloud όταν αναφέρετε σφάλματα ανίχνευσης ή μη ανιχνευθέντα spam e-mails. Αυτό συμβάλλει στη βελτίωση της Bitdefender antispam ανίχνευσης

Διαμορφώστε το σύστημα ηλεκτρονικής υποβολής του δείγματος mail στο Bitdefender Cloud επιλέγοντας τις επιθυμητές επιλογές ακολουθώντας τα παρακάτω βήματα:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ANTISPAM**, πατήστε **Ρυθμίσεις**.
3. Μεταβείτε στο παράθυρο **Ρυθμίσεις** και κάντε κλικ στους αντίστοιχους διακόπτες ενεργοποίησης ή απενεργοποίησης.

Εάν χρησιμοποιείτε το Microsoft Outlook ή το Thunderbird, μπορείτε να διαμορφώσετε το cloud detection άμεσα από την εφαρμογή ηλεκτρονικού ταχυδρομείου σας. Κάντε κλικ στο ⚙ **Settings** κουμπί στην Bitdefender antispam toolbar (συνήθως βρίσκεται στο πάνω μέρος του παραθύρου της εφαρμογής ηλεκτρονικού ταχυδρομείου) και κατόπιν στο **Cloud Settings** tab.

4.5. Firewall

Το Τείχος προστασίας προστατεύει τη συσκευή σας από μη εξουσιοδοτημένες προσπάθειες εισερχόμενης και εξερχόμενης σύνδεσης, τόσο σε τοπικά δίκτυα όσο και στο Διαδίκτυο. Είναι αρκετά παρόμοιο με έναν φρουρό στην πύλη σας - παρακολουθεί τις απόπειρες σύνδεσης και αποφασίζει ποια να επιτραπεί και ποια να απαγορευτεί.

Το Bitdefender firewall χρησιμοποιεί ένα σύνολο κανόνων για να φιλτράρετε τα δεδομένα που μεταδίδονται προς και από το σύστημά σας.

Υπό κανονικές συνθήκες, το Bitdefender δημιουργεί αυτόματα ένα κανόνα όταν μια εφαρμογή προσπαθεί να αποκτήσει πρόσβαση στο Internet. Μπορείτε επίσης να προσθέσετε ή να επεξεργαστείτε με μη αυτόματο τρόπο τους κανόνες για εφαρμογές.

Ως μέτρο ασφάλειας, θα ενημερώνεστε κάθε φορά που μια δυνητικά κακόβουλη εφαρμογή αποκλείεται από την πρόσβαση στο διαδίκτυο.

Το Bitdefender εκχωρεί αυτόματα έναν τύπο δικτύου για κάθε δικτυακή σύνδεση που ανιχνεύει. Ανάλογα με τον τύπο του δικτύου, η προστασία firewall έχει ρυθμιστεί στο κατάλληλο επίπεδο για κάθε σύνδεση.

Για να μάθετε περισσότερα σχετικά με τις ρυθμίσεις του τείχους προστασίας (firewall) για κάθε τύπο δικτύου και πώς μπορείτε να επεξεργαστείτε τις ρυθμίσεις δικτύου, παρακαλούμε ανατρέξτε στο *"Διαχείριση των ρυθμίσεων σύνδεσης"* (p. 127).

Ενεργοποίηση ή απενεργοποίηση της firewall προστασίας

Για να ενεργοποιήσετε ή απενεργοποιήσετε το firewall:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **FIREWALL**, θέστε on ή off τον διακόπτη.

Προειδοποίηση

Επειδή εκθέτει τη συσκευή σας σε μη εξουσιοδοτημένες συνδέσεις, η απενεργοποίηση του τείχους προστασίας πρέπει να αποτελεί προσωρινό μέτρο. Επαναφέρετε το firewall σε ενέργεια το συντομότερο δυνατόν.

4.5.1. Διαχείριση κανόνων εφαρμογής

Για να δείτε και να διαχειριστείτε τους κανόνες του firewall που ελέγχουν την πρόσβαση των εφαρμογών σε πόρους δικτύου και του Internet:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **FIREWALL**, πατήστε **Ρυθμίσεις**.
3. Μεταβείτε στο παράθυρο **Πρόσβαση εφαρμογών**.

Μπορείτε να δείτε τα τελευταία προγράμματα (processes) που έχουν περάσει από το Bitdefender Firewall και το δίκτυο στο οποίο είστε συνδεδεμένοι. Για να δείτε τους κανόνες που δημιουργήθηκαν για μια συγκεκριμένη εφαρμογή, απλώς το επιλέγετε και στη συνέχεια κάντε κλικ στο σύνδεσμο **Προβολή κανόνων εφαρμογών** . Ανοίγει το παράθυρο **ΚΑΝΟΝΕΣ**.

Για κάθε κανόνα εμφανίζονται οι ακόλουθες πληροφορίες:

- **ΔΙΚΤΥΟ** - οι μέθοδοι και οι τύποι προσαρμογέων δικτύου (Home/ Office, Public ή All) στους οποίους ισχύει ο κανόνας. Οι κανόνες δημιουργούνται αυτόματα για να φιλτράρετε δικτυακή ή διαδκτυακή πρόσβαση μέσω του προσαρμογέα. Από προεπιλογή, οι κανόνες ισχύουν για κάθε δίκτυο. Μπορείτε να δημιουργήσετε με μη αυτόματο τρόπο κανόνες ή να επεξεργαστείτε υπάρχοντες κανόνες για το φιλτράρισμα δικτυακής ή Διαδικτυακής πρόσβασης μιάς εφαρμογής μέσω ειδικού αντάπτορα (για παράδειγμα, ένας προσαρμογέας ασύρματου δικτύου).
- **Πρωτόκολλο** - το πρωτόκολλο IP στο οποίο εφαρμόζεται ο κανόνας. Από προεπιλογή, οι κανόνες εφαρμόζονται σε κάθε πρωτόκολλο

- **TRAFFIC** - Ο κανόνας ισχύει και στις δύο κατευθύνσεις, εισερχόμενη και εξερχόμενη.
- **PORTS** - το PORT πρωτόκολλο στο οποίο εφαρμόζεται ο κανόνας. Από προεπιλογή, οι κανόνες εφαρμόζονται σε όλα τα ports.
- **IP** - το internet πρωτόκολλο (IP) στο οποίο εφαρμόζεται ο κανόνας. Από προεπιλογή, οι κανόνες εφαρμόζονται σε τις διευθύσεις IP.
- **ΠΡΟΣΒΑΣΗ** - αν επιτρέπεται ή απαγορεύεται η πρόσβαση της εφαρμογής σε δίκτυο ή Internet κάτω από τις συγκεκριμένες συνθήκες.

Για να επεξεργαστείτε ή να διαγράψετε τους κανόνες για την επιλεγμένη εφαρμογή, κάντε κλικ στο εικονίδιο ⋯.

- **Επεξεργασία κανόνα** - Ανοίγει ένα παράθυρο όπου μπορείτε να επεξεργαστείτε ένα κανόνα.
- **Διαγραφή κανόνα** - μπορείτε να επιλέξετε να καταργήσετε το τρέχον σύνολο κανόνων για την επιλεγμένη εφαρμογή.

Προσθήκη κανόνων εφαρμογών

Για να προσθέσετε έναν κανονόνα εφαρμογής:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **FIREWALL**, πατήστε **Ρυθμίσεις**.
3. Στο παράθυρο **Κανόνες**, πατήστε **Προσθήκη κανόνα**.

Εδώ μπορείτε να εφαρμόσετε τις ακόλουθες αλλαγές:

- **Εφαρμογή του κανόνα σε όλες τις εφαρμογές.** Ενεργοποιήστε αυτή την επιλογή για να εφαρμοστεί ο κανόνας σε όλες τις εφαρμογές.
- **Διαδρομή προγράμματος.** Κάντε κλικ στο **ΠΕΡΙΗΓΗΣΗ** και επιλέξτε την εφαρμογή για την οποία ισχύει ο κανόνας.
- **Δικαιώματα.** Επιλέξτε μια από τις διαθέσιμες εξουσιοδοτήσεις:

Δικαιώματα	Περιγραφή
Να επιτρέπεται	Στην καθορισμένη εφαρμογή θα επιτρέπεται η πρόσβαση στο δίκτυο / internet υπό τις συγκεκριμένες συνθήκες.
Off	Θα απαγορευτεί η δικτυακή/Διαδικτυακή πρόσβαση στη συγκεκριμένη εφαρμογή υπό τις συγκεκριμένες συνθήκες.

- **Τύπος Δικτύου.** Επιλέξτε τον τύπο δικτύου για τον οποίο ισχύει ο κανόνας. Μπορείτε να αλλάξετε τον τύπο με το άνοιγμα αναδιπλούμενου μενού επιλογών **Network Type** και την επιλογή ενός από τους διαθέσιμους τύπους από τον κατάλογο.

Τύπος Δικτύου	Περιγραφή
Όλα	Επιτρέψτε όλη την κίνηση μεταξύ της συσκευής σας και άλλων συσκευών ανεξάρτητα από τον τύπο δικτύου.
Home/Office	Επιτρέψτε όλη την κίνηση μεταξύ της συσκευής σας και διαφορετικών στο τοπικό δίκτυο.
Δημόσια	Η κίνηση φιλτράρεται.

- **Protocol.** Επιλέξτε από το το μενού το πρωτόκολλο IP για το οποίο ισχύει ο κανόνας
  - Εάν θέλετε ο κανόνας να εφαρμοστεί σε όλα τα πρωτόκολλα, επιλέξτε το **Any**.
  - Εάν θέλετε ο κανόνας να εφαρμοστεί στο TCP, επιλέξτε το **TCP**.
  - Εάν θέλετε ο κανόνας να εφαρμοστεί στο UDP, επιλέξτε το **UDP**.
  - Εάν θέλετε ο κανόνας να εφαρμοστεί στο ICMP, επιλέξτε το **ICMP**.
  - Εάν θέλετε ο κανόνας να εφαρμοστεί στο IGMP, επιλέξτε το **IGMP**.
  - Εάν θέλετε ο κανόνας να ισχύει για το GRE, επιλέξτε **GRE** .
  - Εάν θέλετε ο κανόνας να εφαρμοστεί σε ένα συγκεκριμένο πρωτόκολλο, πληκτρολογήστε τον αριθμό που αντιστοιχεί στο πρωτόκολλο που θέλετε να φιλτράρετε στο κενό πεδίο που μπορείτε να γράψετε

> **Σημείωση**
>
> Οι αριθμοί IP πρωτοκόλλων αποδίδονται από την Internet Assigned Numbers Authority (IANA). Μπορείτε να βρείτε τον πλήρη κατάλογο ορισμένων αριθμών πρωτοκόλλου IP http://www.iana.org/assignments/protocol-numbers.

- **Οδηγία.** Επιλέξτε από το το μενού τη διεύθυνση κυκλοφορίας (εξερχόμενη/εισερχόμενη) για την οποία ισχύει ο κανόνας

Οδηγία	Περιγραφή
Εξερχόμενος	Ο κανόνας αυτός ισχύει μόνο για την εξερχόμενη κίνηση.
Εισερχόμενος	Ο κανόνας αυτός ισχύει μόνο για την εισερχόμενη κίνηση.
Και τα δύο	Ο κανόνας ισχύει και στις δύο κατευθύνσεις.

Κάντε κλικ στο κουμπί **Σύνθετες ρυθμίσεις** στο κάτω μέρος του παραθύρου για να προσαρμόσετε τις ακόλουθες ρυθμίσεις:

- **Προσαρμοσμένη Τοπική Διεύθυνση.** Καθορίστε την τοπική διεύθυνση IP και την θύρα για την οποία ισχύει ο κανόνας.
- **Προσαρμοσμένη Απομακρυσμένη Διεύθυνση.** Καθορίστε την απομακρυσμένη διεύθυνση IP και την θύρα για την οποία ισχύει ο κανόνας.

Για να καταργήσετε το τρέχον σύνολο κανόνων και να επαναφέρετε τις προεπιλεγμένες, κάντε κλικ στο **Επαναφορά κανόνων** στο παράθυρο **Κανόνες**.

4.5.2. Διαχείριση των ρυθμίσεων σύνδεσης

Είτε συνδέεστε στο διαδίκτυο χρησιμοποιώντας έναν προσαρμογέα Wi-Fi ή Ethernet, μπορείτε να ρυθμίσετε τις ρυθμίσεις που πρέπει να εφαρμοστούν για ασφαλή πλοήγηση. Οι επιλογές από τις οποίες μπορείτε να επιλέξετε είναι:

- **Dynamic** - ο τύπος δικτύου θα οριστεί αυτόματα με βάση το προφίλ του συνδεδεμένου δικτύου, Home / Office ή Public. Όταν συμβεί αυτό, ισχύουν μόνο οι κανόνες του Firewall για τον συγκεκριμένο τύπο δικτύου ή αυτοί που ορίζονται για να ισχύουν για όλους τους τύπους δικτύου.
- **Home / Office** - ο τύπος δικτύου θα είναι πάντα Home / Office, χωρίς να λαμβάνεται υπόψη το προφίλ του συνδεδεμένου δικτύου. Όταν συμβεί αυτό, ισχύουν μόνο οι κανόνες του Firewall για τον συγκεκριμένο τύπο δικτύου ή αυτοί που ορίζονται για να ισχύουν για όλους τους τύπους δικτύου.
- **Public** - ο τύπος δικτύου θα είναι πάντα Public, χωρίς να λαμβάνεται υπόψη το προφίλ του συνδεδεμένου δικτύου. Όταν συμβεί αυτό, ισχύουν

μόνο οι κανόνες του Firewall για το Public ή αυτοί που ορίζονται για να ισχύουν για όλους τους τύπους δικτύου.

Για να διαμορφώσετε τους προσαρμογείς δικτύου:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **FIREWALL**, πατήστε **Ρυθμίσεις**.
3. Επιλέξτε το παράθυρο **Network Adapters** .
4. Επιλέξτε τις ρυθμίσεις που θέλετε να εφαρμόσετε κατά τη σύνδεση με τους ακόλουθους προσαρμογείς:
   - Wi-Fi
   - Ethernet

4.5.3. Διαμόρφωση ρυθμίσεων για προχωρημένους

Για να διαμορφώσετε τις ρυθμίσεις για προχωρημένους του firewall:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **FIREWALL**, πατήστε **Ρυθμίσεις**.
3. Επιλέξτε το παράθυρο **Ρυθμίσεις** .

Μπορούν να ρυθμιστούν οι ακόλουθες λειτουργίες:

- **Προστασία Port scan** - ανιχνεύει και μπλοκάρει τις προσπάθειες για να ανίχνευση των ανοιχτών θυρών.

  Οι σαρώσεις θύρας χρησιμοποιούνται συχνά από εισβολείς για να μάθουν ποιες θύρες είναι ανοιχτές στη συσκευή σας. Στη συνέχεια, ενδέχεται να εισέλθουν στη συσκευή σας εάν εντοπίσουν μια λιγότερο ασφαλή ή ευάλωτη θύρα.

- **Alert mode** - ειδοποιήσεις εμφανίζονται κάθε φορά που μια εφαρμογή προσπαθεί να συνδεθεί στο διαδίκτυο. Επιλέξτε **Αποδοχή** ή **Άρνηση**. Όταν είναι ενεργοποιημένη η λειτουργία ειδοποίησης, η λειτουργία Profiles απενεργοποιείται αυτόματα. Το Alert mode μπορεί να χρησιμοποιηθεί ταυτόχρονα με τη λειτουργία **Battery Mode**.

- **Να επιτρέπεται η πρόσβαση στο domain του δικτύου** - Να επιτρέπεται ή να απαγορεύεται η πρόσβαση σε πόρους και κοινόχρηστα στοιχεία που ορίζονται από τους ελεγκτές domain.

- **Λειτουργία Stealth** - αν μπορείτε να εντοπιστείτε από άλλες συσκευές. Κάντε κλικ στο **Επεξεργασία ρυθμίσεων stealth** για να επιλέξετε πότε η συσκευή σας πρέπει ή όχι να είναι ορατή σε άλλες συσκευές.
- **Προεπιλεγμένη συμπεριφορά εφαρμογής** - επιτρέψτε στο Bitdefender να εφαρμόσει αυτόματες ρυθμίσεις σε εφαρμογές χωρίς καθορισμένους κανόνες. Κάντε κλικ στο **Διαμόρφωση προεπιλεγμένων κανόνων** για να επιλέξετε αν θα πρέπει να εφαρμοστούν ή όχι οι αυτόματες ρυθμίσεις.
  - Αυτόματη - η πρόσβαση σε εφαρμογές θα επιτρέπεται ή θα απορρίπτεται με βάση τους κανόνες του αυτόματου Firewall και του χρήστη.
  - Επιτρέψτε - οι εφαρμογές που δεν έχουν οριστεί βάσει κανόνων του Firewall θα επιτρέπονται αυτόματα.
  - Αποκλεισμός - οι εφαρμογές που δεν έχουν οριστεί βάσει κανόνων του Firewall θα αποκλειστούν αυτόματα.

4.6. ΕΥΠΑΘΕΙΑ

Ένα σημαντικό βήμα για την προστασία της συσκευής σας από κακόβουλες ενέργειες και εφαρμογές είναι να διατηρείτε ενημερωμένο το λειτουργικό σύστημα και τις εφαρμογές που χρησιμοποιείτε τακτικά. Επιπλέον, για την αποφυγή μη εξουσιοδοτημένης φυσικής πρόσβασης στη συσκευή σας, πρέπει να διαμορφώνονται ισχυροί κωδικοί πρόσβασης (κωδικοί πρόσβασης που δεν μπορούν να μαντευτούν εύκολα) για κάθε λογαριασμό χρήστη των Windows και για τα δίκτυα Wi-Fi στα οποία συνδέεστε επίσης.

Το Bitdefender παρέχει δύο εύκολους τρόπους για να διορθώσετε τις ευπάθειες του συστήματος σας:

- Μπορείτε να σαρώσετε το σύστημά σας για τρωτά σημεία και να τα διορθώσετε βήμα προς βήμα χρησιμοποιώντας την επιλογή **Σάρωση για Ευπάθειες**.
- Χρησιμοποιώντας την αυτόματη παρακολούθηση ευπάθειας, μπορείτε να ελέγξετε και να διορθώσετε τις ευπάθειες που ανιχνεύονται στο παράθυρο Notifications.

Θα πρέπει να ελέγξετε και να διορθώσετε τις ευπάθειες του συστήματος, κάθε μία ή δύο εβδομάδες.

4.6.1. Σάρωση του συστήματός σας για ευπάθειες

Για να εντοπίσετε τα τρωτά σημεία του συστήματος, το Bitdefender απαιτεί μια ενεργή σύνδεση στο διαδίκτυο.

Για να σαρώσετε το σύστημά σας για ευπάθειες:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Ευπάθεια** , κάντε κλικ στο **Άνοιγμα** .
3. Στην καρτέλα **Σάρωση ευπάθειας** κάντε κλικ στο **Έναρξη σάρωσης** και, στη συνέχεια, περιμένετε έως ότου το Bitdefender ελέγξει το σύστημά σας για ευπάθειες. Οι ανιχνευόμενες ευπάθειες ομαδοποιούνται στις τρεις κατηγορίες:

   - **ΛΕΙΤΟΥΡΓΙΚΟ ΣΥΣΤΗΜΑ**

     - **Ασφάλεια λειτουργικού συστήματος**

       Τροποποιημένες ρυθμίσεις συστήματος που ενδέχεται να θέσουν σε κίνδυνο τη συσκευή και τα δεδομένα σας, όπως να μην εμφανίζονται προειδοποιήσεις όταν εκτελούνται αρχεία εκτελούν αλλαγές στο σύστημά σας χωρίς την άδειά σας ή όταν συσκευές MTP όπως τηλέφωνα ή κάμερες συνδέονται και εκτελούν διαφορετικές λειτουργίες χωρίς να το γνωρίζετε.

     - **Κρίσιμα Microsoft Updates**

       Εμφανίζεται μια λίστα κρίσιμων ενημερώσεων των Windows που δεν έχουν εγκατασταθεί στον υπολογιστή σας. Μπορεί να χρειαστεί επανεκκίνηση του συστήματος για να επιτρέψετε στο Bitdefender να ολοκληρώσει την εγκατάσταση. Λάβετε υπόψη ότι μπορεί να χρειαστεί λίγος χρόνος για την εγκατάσταση των ενημερώσεων.

     - **Αδύναμοι windows κωδικοί**

       Μπορείτε να δείτε τη λίστα των λογαριασμών χρηστών των Windows που έχουν διαμορφωθεί στη συσκευή σας και το επίπεδο προστασίας που παρέχει ο κωδικός πρόσβασης. Μπορείτε να επιλέξετε είτε να ζητηθεί από το χρήστη να αλλάξει τον κωδικό πρόσβασης στην επόμενη σύνδεση ή να αλλάξετε τον κωδικό πρόσβασης αμέσως. Για να ορίσετε έναν νέο κωδικό πρόσβασης για το σύστημά σας, επιλέξτε **Αλλαγή κωδικού πρόσβασης τώρα**.

       Για να δημιουργήσετε έναν ισχυρό κωδικό πρόσβασης, σας συνιστούμε να χρησιμοποιήσετε ένα συνδυασμό κεφαλαίων και

πεζών γραμμάτων, αριθμών και ειδικών χαρακτήρων (όπως #, $ ή @).

- **ΕΦΑΡΜΟΓΕΣ**
  - **Ασφάλεια Πλοήγησης**

    Αλλάξτε τις ρυθμίσεις της συσκευής σας που επιτρέπουν την εκτέλεση αρχείων και προγραμμάτων που λαμβάνονται μέσω του Internet Explorer χωρίς επικύρωση ακεραιότητας, γεγονός που μπορεί να οδηγήσει σε παραβίαση της συσκευής σας.
  - **Ανανεώσεις Εφαρμογών**

    Για να δείτε πληροφορίες σχετικά με την εφαρμογή που πρέπει να ενημερωθεί, κάντε κλικ στο όνομά της από τη λίστα.

    Εάν μια εφαρμογή δεν είναι ενημερωμένη, κάντε κλικ στο **Λήψη νέας έκδοσης** για να πραγματοποιήσετε λήψη της πιο πρόσφατης έκδοσης.
- **ΔΙΚΤΥΟ**
  - **Δίκτυο και διαπιστευτήρια**

    Τροποποιημένες ρυθμίσεις συστήματος, όπως αυτόματη σύνδεση σε ανοιχτά δίκτυα hotspot χωρίς να το γνωρίζετε, ή μη επιβολή κρυπτογράφησης στην εξερχόμενη ασφαλή κυκλοφορία καναλιών.
  - **Wi-Fi δίκτυα και routers**

    Για να μάθετε περισσότερα σχετικά με το ασύρματο δίκτυο και το δρομολογητή στο οποίο είστε συνδεδεμένοι, κάντε κλικ στο όνομά του από τη λίστα. Συνιστάται να ορίσετε έναν ισχυρό κωδικό πρόσβασης για το οικιακό σας δίκτυο, βεβαιωθείτε ότι ακολουθείτε τις οδηγίες μας, ώστε να μπορείτε να παραμείνετε συνδεδεμένοι χωρίς να ανησυχείτε για το απόρρητό σας.

    Όταν άλλες συστάσεις είναι διαθέσιμες, ακολουθήστε τις οδηγίες που παρέχονται για να βεβαιωθείτε ότι το οικιακό σας δίκτυο παραμένει ασφαλές από τα αδιάκριτα μάτια των χάκερ.

4.6.2. Χρήση της αυτόματης παρακολούθησης ευπάθειας

Το Bitdefender σαρώνει το σύστημά σας για ευπάθειες τακτικά, στο παρασκήνιο, και κρατά σε αρχεία τα θέματα που ανιχνεύονται, στα Ειδοποιήσεις.

Για να ελέγξετε και να διορθώσετε θέματα που ανιχνεύτηκαν:

1. Πατήστε **Ειδοποιήσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **All**, επιλέξτε την ειδοποίηση που αφορά την σάρωση ευπάθειας.
3. Μπορείτε να δείτε λεπτομερείς πληροφορίες σχετικά με τις ανιχνευμένες ευπάθειες του συστήματος. Ανάλογα με το θέμα, για να διορθώσετε μια συγκεκριμένη ευπάθεια προχωρήστε ως εξής:
   - Εάν είναι διαθέσιμες ενημερώσεις των Windows, κάντε κλικ στο **Εγκατάσταση**.
   - Εάν η αυτόματη ενημέρωση των Windows είναι απενεργοποιημένη, κάντε κλικ στην επιλογή **Ενεργοποίηση**.
   - Εάν μια εφαρμογή δεν είναι ενημερωμένη, κάντε κλικ στο **Update now** για να βρείτε ένα σύνδεσμο προς την ιστοσελίδα του προμηθευτή από όπου μπορείτε να εγκαταστήσετε την πιο πρόσφατη έκδοση της εφαρμογής.
   - Εάν ένας λογαριασμός χρήστη των Windows έχει έναν αδύναμο κωδικό πρόσβασης, κάντε κλικ στην επιλογή **Αλλαγή κωδικού πρόσβασης** για να αναγκάσετε τον χρήστη να αλλάξει τον κωδικό πρόσβασης στην επόμενη σύνδεση ή για να αλλάξετε εσείς τον κωδικό πρόσβασης σας. Για έναν ισχυρό κωδικό πρόσβασης, χρησιμοποιήστε ένα συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμούς και ειδικούς χαρακτήρες (όπως #, $ ή @).
   - Εάν η δυνατότητα Windows Autorun είναι ενεργοποιημένη, κάντε κλικ στην επιλογή **Διόρθωση** για να την απενεργοποιήσετε.
   - Εάν ο router σας έχει ρυθμιστεί με ένα αδύναμο κωδικό πρόσβασης, κάντε κλικ στο **Change password** για να μπείτε σε interface του από όπου μπορείτε να ορίσετε ένα ισχυρότερο κωδικό.
   - Εάν το δίκτυο είστε συνδεδεμένοι έχει τρωτά σημεία που μπορεί να εκθέσει το σύστημά σας σε κίνδυνο, κάντε κλικ στο **Change Wi-Fi settings**.

Για να διαμορφώσετε τις ρυθμίσεις παρακολούθησης ευπάθειας:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Ευπάθεια** , κάντε κλικ στο **Άνοιγμα** .

Σημαντικό
Για να ενημερώνεστε αυτόματα σχετικά με τις ευπάθειες του συστήματος ή της εφαρμογής, κρατήστε την επιλογή **Vulnerability** ενεργοποιημένη.

3. Μεταβείτε στην καρτέλα **Ρυθμίσεις** .
4. Επιλέξτε τις ευπάθειες του συστήματος που θέλετε να ελέγχονται τακτικά, χρησιμοποιώντας τους αντίστοιχους διακόπτες.

Windows updates
Ελέγξτε αν το λειτουργικό σας σύστημα των Windows έχει τις πιο πρόσφατες κρίσιμες ενημερώσεις ασφαλείας από τη Microsoft.

Ανανεώσεις Εφαρμογών
Ελέγξτε αν εφαρμογές που είναι εγκατεστημένες στο σύστημά σας είναι οι πιο πρόσφατες. Ληγμένες εφαρμογές μπορούν να αξιοποιηθούν από κακόβουλο λογισμικό, κάνοντας τον υπολογιστή σας ευάλωτο σε εξωτερικές επιθέσεις.

Κωδικοί πρόσβασης
Ελέγξτε αν οι κωδικοί πρόσβασης των λογαριασμών των Windows και των routers που υπάρχουν στο σύστημα είναι εύκολο να τους μαντέψει κανείς ή όχι. Ο ορισμός κωδικών πρόσβασης που είναι δύσκολο να τους μαντέψει κάποιος (ισχυροί κωδικοί πρόσβασης) καθιστά πολύ δύσκολο για τους χάκερ να σπάσουν στο σύστημά σας. Ένας ισχυρός κωδικός πρόσβασης περιλαμβάνει κεφαλαία και πεζά γράμματα, αριθμούς και ειδικούς χαρακτήρες (όπως #, $ ή @).

Autoplay
Ελέγξτε την κατάσταση της λειτουργίας Windows Autorun. Το χαρακτηριστικό αυτό επιτρέπει στις εφαρμογές να ξεκινήσουν αυτόματα από CD, DVD, USB drives ή από άλλες εξωτερικές συσκευές.

Ορισμένοι τύποι κακόβουλου λογισμικού χρησιμοποιούν το Autorun για να εξαπλωθούν αυτόματα από αφαιρούμενα μέσα στον υπολογιστή. Γι' αυτό συνιστάται να απενεργοποιήσετε αυτό το χαρακτηριστικό των Windows.

Wi-Fi Security Advisor
Ελέγξτε αν το ασύρματο οικιακό δίκτυο που είστε συνδεδεμένοι είναι ασφαλές ή όχι, και αν έχει τρωτά σημεία. Επίσης, ελέγξτε αν

ο κωδικός πρόσβασης του οικιακού router είναι αρκετά ισχυρός και πώς μπορείτε να το κάνετε ασφαλέστερο.

Τα περισσότεροι απροστάτευτα ασύρματα δίκτυα δεν είναι ασφαλή, επιτρέποντας έτσι στα αδιάκριτα βλέμματα των χάκερ να έχουν πρόσβαση στις ιδιωτικές δραστηριότητες σας.

Σημείωση
Εάν απενεργοποιήσετε την παρακολούθηση μιας συγκεκριμένης ευπάθειας, θέματα που σχετίζονται με αυτή, δεν θα καταγράφονται στο παράθυρο Συμβάντα.

4.6.3. Wi-Fi Security Advisor

Ενώ βρίσκεστε εν κινήσει, εργάζεστε σε ένα καφέ, ή περιμένετε στο αεροδρόμιο, το να συνδεθείτε σε ένα δημόσιο ασύρματο δίκτυο για την πραγματοποίηση πληρωμών, τον έλεγχο e-mail ή λογαριασμών κοινωνικών δικτύων μπορεί να είναι η ταχύτερη λύση. Αλλά τα αδιάκριτα βλέμματα που προσπαθούν να χακάρουν τα προσωπικά σας δεδομένα μπορεί να παρακολουθούν πώς διαρρέει η πληροφορία μέσω του δικτύου.

Τα δεδομένα προσωπικού χαρακτήρα νοούνται οι κωδικοί πρόσβασης και τα ονόματα χρήστη που χρησιμοποιείτε για να αποκτήσετε πρόσβαση σε online λογαριασμούς σας, όπως μηνύματα ηλεκτρονικού ταχυδρομείου, τραπεζικούς λογαριασμούς, λογαριασμούς κοινωνικών μέσων μαζικής ενημέρωσης, αλλά και τα μηνύματα που στέλνετε.

Συνήθως, δημόσια ασύρματα δίκτυα είναι πιο πιθανό να είναι μη ασφαλή, δεδομένου ότι δεν απαιτούν κωδικό πρόσβασης κατά τη σύνδεση, και αν το κάνουν, ο κωδικός πρόσβασης θα μπορούσε να διατεθεί σε όποιον θέλει να συνδεθεί. Επιπλέον, μπορεί να είναι κακόβουλα ή honeypot δίκτυα, που αντιπροσωπεύουν ένα στόχο για τους εγκληματίες του κυβερνοχώρου.

Για να σας διασφαλίσουμε από τους κινδύνους των ανασφάλιστων ή μη κρυπτογραφημένα δημόσιων ασύρματων hotspots, το Bitdefender Wi-Fi Security Advisor αναλύει πόσο ασφαλές είναι το ασύρματο δίκτυο, και όταν είναι απαραίτητο, σας συνιστά να χρησιμοποιήσετε το Bitdefender VPN

Το Bitdefender Wi-Fi Security Advisor δίνει πληροφορίες σχετικά με:

- Οικιακά Wi-Fi δίκτυα
- Office Wi-Fi δίκτυα

- Δημόσια Wi-Fi δίκτυα

Ενεργοποίηση ή απενεργοποίηση των ειδοποιήσεων του Wi-Fi Security Advisor

Για να ενεργοποιήσετε ή να απενεργοποιήσετε τις ειδοποιήσεις Wi-Fi Security Advisor:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Ευπάθεια** , κάντε κλικ στο **Άνοιγμα** .
3. Μεταβείτε στο παράθυρο **Ρυθμίσεις** και ενεργοποιήστε ή απενεργοποιήστε την επιλογή **Wi-Fi Security Advisor** .

Διαμόρφωση οικιακού Wi-Fi δικτύου

Για να ξεκινήσετε τη ρύθμιση του οικιακού σας δικτύου:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Ευπάθεια** , κάντε κλικ στο **Άνοιγμα** .
3. Μεταβείτε στο παράθυρο **Wi-Fi Security Advisor** και κάντε κλικ στο **Home Wi-Fi** .
4. Στην καρτέλα **ΟΙΚΙΑΚΟ Wi-Fi**, κάντε κλικ στο **ΕΠΙΛΕΞΤΕ ΟΙΚΙΑΚΟ WI-FI**.

   Εμφανίζεται λίστα με τα ασύρματα δίκτυα που έχετε συνδεθεί μέχρι τώρα.
5. Επιλέξτε το οικιακό σας δίκτυο και, στη συνέχεια, κάντε κλικ στην επιλογή **SELECT**.

Εάν ένα οικιακό δίκτυο θεωρείται μη εξασφαλισμένο ή μη ασφαλή, προτάσεις διαμόρφωσης για να βελτιώσει την ασφάλεια του εμφανίζονται.

Για να αφαιρέσετε το ασύρματο δίκτυο που έχετε θέσει ως οικιακό δίκτυο, κάντε κλικ στο κουμπί **REMOVE**.

Για να προσθέσετε ένα νέο ασύρματο δίκτυο ως οικιακό, κάντε κλικ στο κουμπί **Επιλέξτε νέο οικιακό wi-fi**.

Διαμόρφωση δικτύου Office Wi-Fi

Για να ξεκινήσετε τη διαμόρφωση του office δικτύου:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.

2. Στο παράθυρο **Ευπάθεια** , κάντε κλικ στο **Άνοιγμα** .
3. Μεταβείτε στο παράθυρο **Wi-Fi Security Advisor** , κάντε κλικ στο **Office Wi-Fi** .
4. Στην καρτέλα **Office Wi-Fi**, κάντε κλικ στο **ΕΠΙΛΕΞΤΕ OFFICE WI-FI**.

   Εμφανίζεται λίστα με τα ασύρματα δίκτυα που έχετε συνδεθεί μέχρι τώρα.
5. Επιλέξτε το εταιρικό σας δίκτυο και στη συνέχεια κάντε κλικ στο κουμπί **ΕΠΙΛΟΓΗ**.

Εάν ένα εταιρικό δίκτυο θεωρείται μη ασφαλές, εμφανίζονται συστάσεις διαμόρφωσης για τη βελτίωση της ασφάλειάς του.

Για να καταργήσετε το ασύρματο δίκτυο που έχετε ορίσει ως εταιρικό δίκτυο, κάντε κλικ στο κουμπί **ΔΙΑΓΡΑΦΗ**.

Για να προσθέσετε ένα νέο ασύρματο δίκτυο ως εταιρκό, κάντε κλικ στην επιλογή **Επιλογή νέου εταιρικού wi-fi**.

Δημόσιο Wi-Fi

Όταν συνδέεστε με ένα ακάλυπτο ή ανασφαλή ασύρματο δίκτυο, το προφίλ Δημόσιο Wi-Fi είναι ενεργοποιημένο. Ενώ τρέχει σε αυτό το προφίλ, το Bitdefender Total Security έχει ρυθμιστεί για να ολοκληρώσει αυτόματα τις ακόλουθες ρυθμίσεις του προγράμματος:

- Το Advanced Threat Defense είναι ενεργοποιημένο
- Το Bitdefender Firewall είναι ενεργοποιημένο και οι ακόλουθες ρυθμίσεις εφαρμόζονται στον wireless adapter σας:
  - Stealth mode - ON
  - Τύπος Δικτύου – Δημόσιο
- Οι ακόλουθες ρυθμίσεις από την Online Threat Prevention είναι ενεργοποιημένες:
  - Κρυπτογραφημένη σάρωση Web
  - Προστασία κατά της απάτης
  - Προστασία από phishing

- Ένα κουμπί που ανοίγει το Bitdefender Safepay™ είναι διαθέσιμο. Στην περίπτωση αυτή, η προστασία Hotspot για μη ασφαλή δίκτυα είναι ενεργοποιημένη από προεπιλογή.

Έλεγχος πληροφοριών σχετικά με τα δίκτυα Wi-Fi

Για να ελέγξετε τις πληροφορίες σχετικά με τα ασύρματα δίκτυα με τα οποία συνήθως συνδέεστε:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Ευπάθεια** , κάντε κλικ στο **Άνοιγμα** .
3. Μεταβείτε στο παράθυρο **Wi-Fi Security Advisor** .
4. Ανάλογα με τις πληροφορίες που χρειάζεστε, επιλέξτε μία από τις τρεις καρτέλες, **Οικιακό Wi- Fi**, **Εταιρικό Wi- Fi** ή **Δημόσιο Wi-Fi**.
5. Κάντε κλικ στο **View details** δίπλα από το δίκτυο για το οποίο θέλετε να βρείτε περισσότερες πληροφορίες.

Υπάρχουν τρεις τύποι ασύρματων δικτύων που φιλτράρονται από τη σπουδαιότητά τους, κάθε τύπος υποδεικνύεται από ένα συγκεκριμένο εικονίδιο:

Wi-Fi is unsafe - δείχνει ότι το επίπεδο ασφαλείας του δικτύου είναι χαμηλό. Αυτό σημαίνει ότι υπάρχει υψηλός κίνδυνος αν το χρησιμοποιήσετε, και δεν συνιστάται να κάνετε πληρωμές ή να ελέγξετε τους τραπεζικούς λογαριασμούς χωρίς επιπλέον προστασία. Σε τέτοιες περιπτώσεις, σας προτείνουμε να χρησιμοποιήσετε το Bitdefender Safepay™ με ενεργοποιημένη την προστασία Hotspot για μη ασφαλή δίκτυα.

Wi-Fi is unsafe - δείχνει ότι το επίπεδο ασφαλείας του δικτύου είναι μέτριο. Αυτό σημαίνει ότι υπάρχει υψηλός κίνδυνος αν το χρησιμοποιήσετε, και δεν συνιστάται να κάνετε πληρωμές ή να ελέγξετε τους τραπεζικούς λογαριασμούς χωρίς επιπλέον προστασία. Σε τέτοιες περιπτώσεις, σας προτείνουμε να χρησιμοποιήσετε το Bitdefender Safepay™ με ενεργοποιημένη την προστασία Hotspot για μη ασφαλή δίκτυα.

Wi-Fi is secure - δείχνει ότι το δίκτυο που χρησιμοποιείτε είναι ασφαλές. Σε αυτήν την περίπτωση, μπορείτε να χρησιμοποιήσετε ευαίσθητα δεδομένα για την πραγματοποίηση online εργασιών.

Επιλέγοντας τον σύνδεσμο **ΛΕΠΤΟΜΕΡΕΙΕΣ** στην περιοχή του κάθε δικτύου, εμφανίζονται οι ακόλουθες λεπτομέρειες:

- **Ασφαλές** - εδώ μπορείτε να δείτε εάν το επιλεγμένο δίκτυο είναι ασφαλές ή όχι. Μη κρυπτογραφημένα δίκτυα μπορούν να αφήσουν εκτεθειμένα τα δεδομένα που χρησιμοποιείτε.
- **Encryption type** - εδώ μπορείτε να δείτε τον τύπο κρυπτογράφησης που χρησιμοποιείται από το επιλεγμένο δίκτυο. Ορισμένοι τύποι κρυπτογράφησης μπορεί να μην είναι ασφαλής. Ως εκ τούτου, σας συνιστούμε να ελέγξετε τις πληροφορίες σχετικά με το εμφανιζόμενο τύπο κρυπτογράφησης για να βεβαιωθείτε ότι είστε προστατευμένοι κατά την πλοήγηση στο διαδίκτυο.
- **Channel/Frequency** - εδώ μπορείτε να δείτε τη συχνότητα του καναλιού που χρησιμοποιείται από το επιλεγμένο δίκτυο.
- **Password strength** - εδώ μπορείτε να δείτε πόσο ισχυρός είναι ο κωδικός πρόσβασης. Σημειώστε ότι τα δίκτυα που έχουν θέσει αδύναμους κωδικούς πρόσβασης αποτελούν στόχο για τους εγκληματίες του κυβερνοχώρου.
- **Type of sign in** - εδώ μπορείτε να δείτε εάν το επιλεγμένο δίκτυο προστατεύεται χρησιμοποιώντας έναν κωδικό πρόσβασης ή όχι. Συνιστάται ιδιαίτερα να συνδέεστε μόνο σε δίκτυα που έχουν ισχυρούς κωδικούς πρόσβασης.
- **Authentication type** - εδώ μπορείτε να δείτε τον τύπο ελέγχου ταυτότητας που χρησιμοποιείται από το επιλεγμένο δίκτυο.

4.7. ΒΙΝΤΕΟ & ΠΡΟΣΤΑΣΙΑ ΗΧΟΥ

Όλο και περισσότερες απειλές σχεδιάζονται για να αποκτήσουν πρόσβαση σε ενσωματωμένες κάμερες και μικρόφωνα. Για να αποτρέψετε την μη εξουσιοδοτημένη πρόσβαση στην κάμερά σας και να σας ενημερώσουμε ποιες αναξιόπιστες εφαρμογές έχουν πρόσβαση στο μικρόφωνο της συσκευής σας και πότε, το Bitdefender Βίντεο amp; Ήχο περιλαμβάνει:

- ΠΡΟΣΤΑΣΙΑ ΓΙΑ Webcam
- ΕΛΕΓΧΟΣ ΜΙΚΡΟΦΩΝΟΥ

4.7.1. ΠΡΟΣΤΑΣΙΑ ΓΙΑ Webcam

Το ότι οι χάκερ μπορούν να πάρουν τον έλεγχο την κάμερας σας για να σας κατασκοπεύσουν δεν είναι πλέον κάτι καινούριο και οι λύσεις για την προστασία σας, όπως η ανάκληση των προνομίων της εφαρμογής ή η

απενεργοποίηση της ενσωματωμένης κάμερας της συσκευής δεν είναι πολύ πρακτικές. Για να αποτρέψετε περαιτέρω προσπάθειες πρόσβασης στο ιδιωτικό σας απόρρητο, η Bitdefender Webcam προστασία παρακολουθεί μόνιμα τις εφαρμογές που προσπαθούν να αποκτήσουν πρόσβαση στην κάμερά σας και αποκλείει εκείνες που δεν εχουν οριστεί ως αξιόπιστες.

Ως μέτρο ασφάλειας, θα ενημερώνεστε κάθε φορά που μια μη αξιόπιστη εφαρμογή θα προσπαθήσει να αποκτήσει πρόσβαση στην κάμερά σας.

Ενεργοποίηση ή απενεργοποίηση της προστασίας της Webcam

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ΒΙΝΤΕΟ & ΠΡΟΣΤΑΣΙΑ ΗΧΟΥ**, κάντε κλικ στην επιλογή **Ρυθμίσεις**.
3. Τώρα μεταβείτε στο παράθυρο **Ρυθμίσεις** και ενεργοποιήστε ή απενεργοποιήστε τον αντίστοιχο διακόπτη.

Ρύθμιση Webcam Προστασίας

Μπορείτε να ορίσετε ποιοι κανόνες θα πρέπει να εφαρμόζονται όταν μια εφαρμογή προσπαθεί να αποκτήσει πρόσβαση στην κάμερά σας ακολουθώντας τα παρακάτω βήματα:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ΒΙΝΤΕΟ & ΠΡΟΣΤΑΣΙΑ ΗΧΟΥ**, κάντε κλικ στην επιλογή **Ρυθμίσεις**.
3. Μεταβείτε στην καρτέλα **Ρυθμίσεις** .

Διαθέσιμες επιλογές:

Κανόνες αποκλεισμού εφαρμογών

- **Αποκλεισμός κάθε πρόσβασης στην κάμερα web** - καμία εφαρμογή δεν θα επιτρέπεται να αποκτήσει πρόσβαση στην κάμερά σας.
- **Αποκλεισμός πρόσβασης των browsers στην κάμερα web** - Δεν επιτρέπεται σε κανένα πρόγραμμα περιήγησης εκτός από τον Internet Explorer και το Microsoft Edge να έχουν πρόσβαση στην κάμερά σας. Λόγω της διαδικασίας των εφαρμογών των Windows Store για εκτέλεση σε μια ενιαία διαδικασία, ο Internet Explorer και το Microsoft Edge δεν μπορούν να ανιχνευθούν από το Bitdefender ως browsers και ως εκ τούτου εξαιρούνται από αυτήν τη ρύθμιση.

- **Ορίστε δικαιώματα χρήσης με βάση την επιλογή της κοινότητας** - Εάν η πλειοψηφία των χρηστών του Bitdefender θεωρεί ότι μια δημοφιλής εφαρμογή είναι αβλαβής, τότε η πρόσβασή της στην κάμερα θα ρυθμιστεί αυτόματα σε Επιτρέψτε. Εάν μια δημοφιλής εφαρμογή θεωρείται επικίνδυνη από τους πολλούς, τότε η πρόσβασή της θα οριστεί αυτόματα στο Αποκλεισμός.

  Θα ενημερώνεστε κάθε φορά που μία από τις εγκατεστημένες εφαρμογές σας θα παραμείνει αποκλεισμένη από την πλειοψηφία των χρηστών του Bitdefender.

Ειδοποιήσεις

- **Ειδοποίηση όταν οι επιτρεπόμενες εφαρμογές συνδέονται με την κάμερα web** - θα ενημερώνεστε κάθε φορά που μια επιτρεπόμενη εφαρμογή θα έχει πρόσβαση στην κάμερα web.

Προσθήκη εφαρμογών στη λίστα Προστασίας Webcam

Οι εφαρμογές που προσπαθούν να συνδεθούν στην κάμερά σας ανιχνεύονται αυτόματα και ανάλογα με τη συμπεριφορά τους και την επιλογή της κοινότητας, η πρόσβασή τους επιτρέπεται ή απορρίπτεται. Παρόλα αυτά, μπορείτε να ξεκινήσετε χειροκίνητα τη διαμόρφωση με δική σας πρωτοβουλία ακολουθώντας τα εξής βήματα:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ΒΙΝΤΕΟ & ΠΡΟΣΤΑΣΙΑ ΗΧΟΥ**, κάντε κλικ στην επιλογή **Ρυθμίσεις**.
3. Μεταβείτε στο παράθυρο **Webcam Protection** .
4. Κάντε κλικ στο παράθυρο **Προσθήκη εφαρμογής** .
5. Κάντε κλικ στον σύνδεσμο που θέλετε:
   - **Από το Windows Store** - εμφανίζεται μια λίστα με τις εφαρμογές του Windows Store που εντοπίστηκαν. Ενεργοποιήστε τους διακόπτες δίπλα στις εφαρμογές που θέλετε να προσθέσετε στη λίστα.
   - **Από τις εφαρμογές σας** - μεταβείτε στο αρχείο .exe που θέλετε να προσθέσετε στη λίστα και, στη συνέχεια, κάντε κλικ στο **OK** .

Για να δείτε τι έχουν επιλέξει οι άλλοι Bitdefender χρήστες για την επιλεγμένη εφαρμογή, κάντε κλικ στο εικονίδιο.

Οι εφαρμογές που θα ζητήσουν πρόσβαση στην κάμερά σας μαζί με την ώρα της τελευταίας δραστηριότητας θα εμφανιστούν σε αυτό το παράθυρο.

Θα ειδοποιηθείτε κάθε φορά που μία από τις επιτρεπόμενες εφαρμογές έχει αποκλειστεί από τους χρήστες του Bitdefender.

Για να διακόψετε την πρόσβαση μιας εφαρμογής που προστέθηκε στην κάμερά σας, κάντε κλικ στο εικονίδιο . Το εικονίδιο μεταβαίνει σε , πράγμα που σημαίνει ότι η επιλεγμένη εφαρμογή δεν θα έχει πρόσβαση στην κάμερά σας.

4.7.2. ΕΛΕΓΧΟΣ ΜΙΚΡΟΦΩΝΟΥ

Οι Rogue εφαρμογές μπορούν να έχουν πρόσβαση στο ενσωματωμένο μικρόφωνο σιωπηλά ή στο παρασκήνιο χωρίς τη συγκατάθεσή σας. Για να σας ενημερώνουμε για πιθανές απειλές, Bitdefender Microphone monitor θα σας ειδοποιεί για τέτοια γεγονότα. Με αυτόν τον τρόπο, καμία εφαρμογή δεν θα μπορεί να αποκτήσει πρόσβαση στο μικρόφωνό σας χωρίς να το γνωρίζετε.

Ενεργοποίηση ή απενεργοποίηση του Microphone monitor

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ΒΙΝΤΕΟ & ΠΡΟΣΤΑΣΙΑ ΗΧΟΥ**, κάντε κλικ στην επιλογή **Ρυθμίσεις**.
3. Επιλέξτε το παράθυρο **Ρυθμίσεις** .
4. Στο παράθυρο **Ρυθμίσεις** , ενεργοποιήστε ή απενεργοποιήστε το διακόπτη **παρακολούθηση μικροφώνου** .

Ρύθμιση ειδοποιήσεων για το Microphone monitor

Για να ρυθμίσετε τις ειδοποιήσεις που θα εμφανίζονται όταν οι εφαρμογές θα προσπαθούν να αποκτήσουν πρόσβαση στο μικρόφωνό σας, ακολουθήστε τα εξής βήματα:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ΒΙΝΤΕΟ & ΠΡΟΣΤΑΣΙΑ ΗΧΟΥ**, κάντε κλικ στην επιλογή **Ρυθμίσεις**.

3. Μεταβείτε στο παράθυρο **Ρυθμίσεις** .

Ειδοποιήσεις

- **Ειδοποίησε με όταν μια εφαρμογή προσπαθεί να αποκτήσει πρόσβαση στο μικρόφωνο**
- **Ειδοποίησέ με όταν τα προγράμματα περιήγησης έχουν πρόσβαση στο μικρόφωνο**
- **Ειδοποίησέ με όταν οι μη αξιόπιστες εφαρμογές έχουν πρόσβαση στο μικρόφωνο**
- **Προβολή ειδοποιήσεων με βάση του Bitdefender με βάση τις επιλογές χρηστών**

Προσθήκη εφαρμογών στη λίστα του Microphone monitor

Οι εφαρμογές που θα προσπαθήσουν να συνδεθούν στο μικρόφωνο θα ανιχνευθούν αυτόματα και θα προστεθούν στη λίστα ειδοποιήσεων. Ωστόσο, μπορείτε να ρυθμίσετε τις ρυθμίσεις χειροκίνητα, εάν πρέπει να εμφανιστεί μια ειδοποίηση ή όχι, ακολουθώντας τα εξής βήματα:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ΒΙΝΤΕΟ & ΠΡΟΣΤΑΣΙΑ ΗΧΟΥ**, κάντε κλικ στην επιλογή **Ρυθμίσεις**.
3. Μεταβείτε στο παράθυρο **Προστασία ήχου** .
4. Κάντε κλικ στο παράθυρο **Προσθήκη εφαρμογής** .
5. Κάντε κλικ στον σύνδεσμο που θέλετε:
   - **Από το Windows Store** - εμφανίζεται μια λίστα με τις εφαρμογές του Windows Store που εντοπίστηκαν. Ενεργοποιήστε τους διακόπτες δίπλα στις εφαρμογές που θέλετε να προσθέσετε στη λίστα.
   - **Από τις εφαρμογές σας** - μεταβείτε στο αρχείο .exe που θέλετε να προσθέσετε στη λίστα και, στη συνέχεια, κάντε κλικ στο **OK** .

Για να δείτε τι έχουν επιλέξει οι άλλοι Bitdefender χρήστες για την επιλεγμένη εφαρμογή, κάντε κλικ στο εικονίδιο.

Οι εφαρμογές που θα ζητήσουν πρόσβαση στην κάμερά σας μαζί με την ώρα της τελευταίας δραστηριότητας θα εμφανιστούν σε αυτό το παράθυρο.

Για να σταματήσετε να λαμβάνετε ειδοποιήσεις σχετικά με τη δραστηριότητα μιας εφαρμογής που προστέθηκε, κάντε κλικ στο εικονίδιο . Το εικονίδιο μεταβαίνει σε , πράγμα που σημαίνει ότι δεν θα εμφανίζεται καμία Bitdefender ειδοποίηση όταν η επιλεγμένη εφαρμογή προσπαθήσει να αποκτήσει πρόσβαση στο μικρόφωνό σας.

4.8. Αποκατάσταση από Ransomware

Bitdefender Ransomware Αποκατάσταση υποστηρίζει τα αρχεία σας, όπως έγγραφα, εικόνες, βίντεο ή μουσική, και σας εξασφαλίζει ότι προστατεύονται από ζημιά ή απώλεια σε περίπτωση κρυπτογράφησης ransomware. Κάθε φορά που ανιχνεύεται επίθεση ransomware, Bitdefender θα αποκλείσει όλες τις διαδικασίες που εμπλέκονται στην επίθεση και θα ξεκινήσει την διαδικασία αποκατάστασης. Με αυτόν τον τρόπο, θα μπορείτε να ανακτήσετε το περιεχόμενο ολόκληρων των αρχείων σας χωρίς να πληρώσετε για οποιαδήποτε ζητούμενη αμοιβή.

Ενεργοποίηση ή απενεργοποίηση της Ransomware προστασίας

Για να ενεργοποιήσετε ή να απενεργοποιήσετε την Ανάκτηση του Ransomware:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο **RANSOMWARE ΑΝΑΚΤΗΣΗ** , ενεργοποιήστε ή απενεργοποιήστε το διακόπτη.

Σημείωση
Για να διασφαλίσετε ότι τα αρχεία σας προστατεύονται από τα ransomware, σας συνιστούμε να έχετε ενεργοποιημένη την Αποκατάσταση του Ransomware.

Ενεργοποίηση ή απενεργοποίηση της αυτόματης επαναφοράς

Η Αυτόματη Επαναφορά διασφαλίζει ότι τα αρχεία σας θα αποκατασταθούν αυτόματα σε περίπτωση κρυπτογράφησης ransomware.

Για να ενεργοποιήσετε ή να απενεργοποιήσετε την αυτόματη επαναφορά:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην οθόνη **ΑΝΑΚΤΗΣΗ RANSOMWARE** , επιλέξτε **Διαχείριση**.
3. Στο παράθυρο Ρυθμίσεις, ενεργοποιήστε ή απενεργοποιήστε το διακόπτη **Αυτόματη επαναφορά** .

Προβολή αρχείων που επαναφέρθηκαν αυτόματα

Όταν είναι ενεργοποιημένη η επιλογή **Αυτόματη επαναφορά** , το Bitdefender θα επαναφέρει αυτόματα τα αρχεία που κρυπτογραφήθηκαν από ransomware. Δια του παρόντος, μπορείτε να απολαύσετε μια εμπειρία χωρίς ανησυχίες γνωρίζοντας ότι τα αρχεία σας είναι ασφαλή.

Για να δείτε τα αρχεία που επαναφέρθηκαν αυτόματα:

1. Πατήστε **Ειδοποιήσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Στο **Όλα** καρτέλα, επιλέξτε την ειδοποίηση σχετικά με την πιο πρόσφατη συμπεριφορά αντιμετώπισης ransomware κα στην συνέχεια, κάντε κλικ **Επανάκτηση Αρχείων**.

   Εμφανίζεται η λίστα των αρχείων που έχουν επανακτηθεί. Εδώ μπορείτε επίσης να δείτε την τοποθεσία όπου έχουν ανακτηθεί τα αρχεία σας.

Επαναφορά κρυπτογραφημένων αρχείων χειροκίνητα

Σε περίπτωση που πρέπει να επαναφέρετε χειροκίνητα κρυπτογραφημένα από ransomware αρχεία, ακολουθήστε τα εξής βήματα:

1. Πατήστε **Ειδοποιήσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **Όλα** , επιλέξτε την ειδοποίηση σχετικά με την τελευταία ανίχνευση συμπεριφοράς ransomware και στην συνέχεια κάντε κλικ **Κρυπτογραφημένα αρχεία** .
3. Εμφανίζεται η λίστα με τα κρυπτογραφημένα αρχεία.

   Κάντε κλικ στο **Ανάκτηση αρχείων** για να συνεχίσετε.
4. Σε περίπτωση αποτυχίας ολόκληρου ή μέρους της διαδικασίας αποκατάστασης, πρέπει εσείς να επιλέξετε την θέση αποθήκευσης των αποκρυπτογραφημένων αρχείων. Κάντε κλικ στο **Επαναφορά τοποθεσίας** και, στη συνέχεια, επιλέξτε μια τοποθεσία στον υπολογιστή σας.
5. Εμφανίζεται ένα παράθυρο επιβεβαίωσης.

Κάντε κλικ στο **Τέλος** για να τερματίσετε τη διαδικασία επαναφοράς.

Αρχεία με τις ακόλουθες καταλήξεις μπορούν να αποκατασταθούν σε περίπτωση κρυπτογράφησης:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

Προσθήκη εφαρμογών στις εξαιρέσεις

Μπορείτε να ορίσετε κανόνες εξαίρεσης για αξιόπιστες εφαρμογές, έτσι ώστε η λειτουργία Αποκατάστασης από Ransowmare να μην τις αποκλείει εάν εκτελούν ενέργειες παρόμοιες με ransomware συμπεριφορά.

Για να προσθέσετε εφαρμογές στη λίστα εξαιρέσεων από Αποκατάσταση από Ransomware :

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην οθόνη **ΑΝΑΚΤΗΣΗ RANSOMWARE** , επιλέξτε **Διαχείριση**.
3. Μεταβείτε στο παράθυρο **Εξαιρέσεις** και κάντε κλικ στο **+ Προσθήκη εξαίρεσης** .

4.9. Προστασία των κωδικών σας με το Διαχειριστή Κωδικών Ασφαλείας

Χρησιμοποιούμε τις συσκευές μας για αγορές στο διαδίκτυο ή για πληρωμή των λογαριασμών μας, για σύνδεση σε πλατφόρμες κοινωνικών μέσων ή σύνδεση με εφαρμογές άμεσων μηνυμάτων.

Αλλά, όπως όλοι γνωρίζουν, δεν είναι πάντα εύκολο να θυμόμαστε τον κωδικό πρόσβασης!

Και αν δεν είμαστε προσεκτικοί κατά την πλοήγηση στο διαδίκτυο, οι προσωπικές μας πληροφορίες: όπως η διεύθυνση e-mail μας, η ταυτότητα άμεσων μηνυμάτων μας ή τα στοιχεία της πιστωτικής μας κάρτας μπορεί να τεθούν σε κίνδυνο.

Το να φυλάξετε τους κωδικούς πρόσβασής σας ή τα προσωπικά σας δεδομένα σε ένα φύλλο χαρτί ή στον υπολογιστή μπορεί να είναι επικίνδυνο, επειδή μπορεί να τα ανακαλύψουν και να χρησιμοποιηθούν από τους ανθρώπους που θέλουν να κλέψουν και να χρησιμοποιήσουν αυτές τις πληροφορίες . Και το να θυμάστε κάθε κωδικό πρόσβασης που έχετε ορίσει για τους ηλεκτρονικούς λογαριασμούς σας ή για τις αγαπημένες σας ιστοσελίδες δεν είναι ένα εύκολο.

Ως εκ τούτου, υπάρχει τρόπος για να βεβαιωθούμε πως θα βρούμε τους κωδικούς μας όταν θα τους χρειαστούμε; Και μπορούμε να είμαστε ήσυχοι ότι οι μυστικοί κωδικοί πρόσβασης μας είναι πάντα ασφαλείς;

Ο Διαχειριστής Κωδικών Ασφαλείας σας βοηθά να παρακολουθείτε τους κωδικούς πρόσβασής σας, προστατεύει την ιδιωτικότητα σας και παρέχει μια ασφαλή εμπειρία περιήγησης.

Χρησιμοποιώντας ένα ενιαίο βασικό κωδικό πρόσβασης για τους κωδικούς σας, ο Διαχειριστής Κωδικών Ασφαλείας καθιστά εύκολο για εσάς να κρατήσετε τους κωδικούς πρόσβασής σας ασφαλείς σε ένα Wallet.

Να προσφέρει την καλύτερη προστασία για τις online δραστηριότητές σας, ο Διαχειριστής Κωδικών Ασφαλείας είναι ενσωματωμένος με το Bitdefender Safepay™ και παρέχει μια ενοποιημένη λύση κατά των διάφορων τρόπων με τους οποίους τα προσωπικά σας δεδομένα μπορεί να τεθούν σε κίνδυνο.

Ο Διαχειριστής Κωδικών Ασφαλείας προστατεύει τις ακόλουθες προσωπικές πληροφορίες:

- Οι προσωπικές πληροφορίες όπως η διεύθυνση e-mail ή ο αριθμός τηλεφώνου
- Κωδικοί πρόσβασης για τις ιστοσελίδες
- Πληροφορίες Τραπεζικού λογαριασμού ή αριθμό πιστωτικής κάρτας
- Δεδομένα πρόσβασης στους λογαριασμούς e-mail
- Κωδικοί για τις εφαρμογές
- Κωδικούς πρόσβασης για τα δίκτυα Wi-Fi

Δημιουργήστε μια νέα βάση δεδομένων Wallet

Το Bitdefender Wallet είναι το μέρος όπου μπορείτε να αποθηκεύσετε τα προσωπικά σας δεδομένα. Για ευκολότερη περιήγηση στο διαδίκτυο,

χρειάζεται να δημιουργήσετε μια βάση δεδομένων για το Wallet με τα ακόλουθα βήματα:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **PASSWORD MANAGER**, πατήστε **Ρυθμίσεις**.
3. Στο παράθυρο **Τα πορτοφόλια** , κάντε κλικ στο **Προσθήκη πορτοφολιού** .
4. Κάντε κλικ στο **Δημιουργία νέου** .
5. Πληκτρολογήστε τις απαιτούμενες πληροφορίες στα αντίστοιχα πεδία.
   - Όνομα Πορτοφολιού - πληκτρολογήστε ένα μοναδικό όνομα για τη βάση δεδομένων του Πορτοφολιού σας.
   - Βασικός Κωδικός Πρόσβασης - πληκτρολογήστε έναν κωδικό πρόσβασης για το Wallet σας.
   - Υπόδειξη - Πληκτρολογήστε μια υπόδειξη για να θυμάστε τον κωδικό πρόσβασης.
6. Κάντε κλικ στο **Συνέχεια**.
7. Σε αυτό το βήμα μπορείτε να επιλέξετε να αποθηκεύσετε τις πληροφορίες σας στο cloud, ενεργοποιώντας το διακόπτη δίπλα στο **Συγχρονισμός σε όλες τις συσκευές μου** . Επιλέξτε την επιθυμητή επιλογή, στη συνέχεια κάντε κλικ στο **Συνέχεια**.
8. Επιλέξτε το πρόγραμμα περιήγησης από το οποίο θέλετε να εισάγετε τους κωδικούς.
9. Κάντε κλικ στο **Τέλος**.

Εισαγωγή μιας υπάρχουσας βάσης δεδομένων

Για να εισάγετε μία βάση δεδομένων του Wallet που έχετε αποδηκεύσει τοπικά:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **PASSWORD MANAGER**, πατήστε **Ρυθμίσεις**.
3. Στο παράθυρο **Τα πορτοφόλια** , κάντε κλικ στο **Προσθήκη πορτοφολιού** .
4. Κάντε κλικ στο **Εισαγωγή υπάρχουσας βάσης δεδομένων** .

5. Περιηγηθείτε στην τοποθεσία της συσκευής σας όπου αποθηκεύσατε τη βάση δεδομένων του πορτοφολιού και επιλέξτε την.
6. Κάντε κλικ στο **Open** (άνοιγμα)
7. Δώστε ένα όνομα στο Wallet και εισάγετε τον κωδικό που είχατε δώσει όταν είχατε φτιάξει τη βάση για πρώτη φορά.
8. Επιλέξτε **ΕΙΣΑΓΩΓΗ**.
9. Επιλέξτε τις εφαρμογές από τις οποίες θα θέλατε το wallet να εισάγει τα διαπιστευτήρια και στη συνέχεια επιλέξτε **ΤΕΛΟΣ**.

Εξαγωγή της βάσης Δεδομένων Wallet

Για την εξαγωγή δεδομένων απο το Wallet σας:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **PASSWORD MANAGER**, πατήστε **Ρυθμίσεις**.
3. Μεταβείτε στο παράθυρο **Τα πορτοφόλια μου** .
4. Επιλέξτε το ••• εικονίδιο στο επιθυμητό wallet, και στη συνέχεια επιλέξτε **ΕΞΑΓΩΓΗ**.
5. Περιηγηθείτε στην τοποθεσία της συσκευής σας όπου θέλετε να αποθηκεύσετε τη βάση δεδομένων του πορτοφολιού και, στη συνέχεια, επιλέξτε ένα όνομα για αυτήν.
6. Κάντε κλικ στο **Αποθήκευση**.

Σημείωση

Το Wallet πρέπει να ανοίξει προκειμένου η επιλογή **ΕΞΑΓΩΓΗ** να είναι διαθέσιμη.
Εάν το πορτοφόλι που πρέπει να εξαγάγετε είναι κλειδωμένο, κάντε κλικ στο **Ενεργοποίηση πορτοφολιού** και, στη συνέχεια, πληκτρολογήστε τον κωδικό πρόσβασης που εκχωρήθηκε όταν δημιουργήθηκε στην πρώτη θέση.

Συγχρονίστε τα wallets σας στο cloud

Για να ενεργοποιήσετε ή να απενεργοποιήσετε το συγχρονισμό των wallets:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **PASSWORD MANAGER**, πατήστε **Ρυθμίσεις**.

3. Μεταβείτε στο παράθυρο **Τα πορτοφόλια μου** .
4. Επιλέξτε το ••• εικονίδιο στο επιθυμητό wallet, και στη συνέχεια επιλέξτε **ΡΥΘΜΙΣΕΙΣ**.
5. Επιλέξτε την επιθυμητή επιλογή στο παράθυρο που εμφανίζεται, στη συνέχεια κάντε κλικ στο **Αποθήκευση**.

Σημείωση
Το Wallet πρέπει να ανοίξει προκειμένου η επιλογή **ΕΞΑΓΩΓΗ** να είναι διαθέσιμη.
Εάν το wallet που θέλετε να συγχρονίσετε είναι κλειδωμένο, επιλέξτε το κουμπί **ΕΝΕΡΓΟΠΟΙΗΣΗ WALLET**, και στη συνέχεια εισάγετε τον κωδικό που είχατε δώσει όταν το είχατε δημιουργήσει.

Διαχειριστείτε τους κωδικούς Wallet

Για να διαχειριστείτε τους κωδικούς σας:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **PASSWORD MANAGER**, πατήστε **Ρυθμίσεις**.
3. Μεταβείτε στο παράθυρο **Τα πορτοφόλια μου** .
4. Επιλέξτε την επιθυμητή βάση δεδομένων του Πορτοφολιού και, στη συνέχεια, κάντε κλικ στο **Ενεργοποίηση πορτοφολιού** .
5. Πληκτρολογήστε τον κωδικό πρόσβασης που απαιτείται και στη συνέχεια κάντε κλικ στο **OK**.

Εμφανίζεται ένα νέο παράθυρο. Επιλέξτε την κατηγορία που επιθυμείτε από το πάνω μέρος του παραθύρου:

- Ταυτότητα
- Ιστοσελίδες
- Online banking
- Emails
- Εφαρμογές
- Δίκτυα Wi-Fi

Προσθήκη/επεξεργασία των κωδικών

- Για να προσθέσετε ένα νέο κωδικό πρόσβασης, επιλέξτε την επιθυμητή κατηγορία από την κορυφή, κάντε κλικ στην επιλογή **+ Προσθήκη στοιχείου**, εισάγετε τις πληροφορίες στα αντίστοιχα πεδία και κάντε κλικ στο κουμπί Αποθήκευση.
- Για να επεξεργαστείτε μια καταχώριση από τον πίνακα, επιλέξτε την και κάντε κλικ στο κουμπί **Επεξεργασία** που βρίσκεται στη δεξιά πλευρά.
- Για να αφαιρέσετε μια εισαγωγή, επιλέξτε **ΔΙΑΓΡΑΦΗ**.

Ενεργοποίηση ή απενεργοποίηση της προστασίας του Διαχειριστή Κωδικών Ασφαλείας

Για να ενεργοποιήσετε ή απενεργοποιήσετε την προστασία του Password Manager:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **PASSWORD MANAGER**, επιλέξτε on ή off τον διακόπτη.

Διαχείριση ρυθμίσεων Διαχειριστή Κωδικών Ασφαλείας

Για να ρυθμίσετε τον κύριο κωδικό πρόσβασης αναλυτικά:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **PASSWORD MANAGER**, πατήστε **Ρυθμίσεις**.
3. Μεταβείτε στο παράθυρο **Ρυθμίσεις** .

Στην ενότητα **Ρυθμίσεις ασφαλείας** , είναι διαθέσιμες οι ακόλουθες επιλογές:

- **Να ερωτηθώ για το βασικό μου τον κωδικό όταν συνδέομαι στον υπολογιστή μου** - Θα σας ζητηθεί να εισάγετε τον βασικό σας κωδικό όταν συνδέεστε στον υπολογιστή.
- **Να ερωτηθώ για το βασικό μου τον κωδικό όταν ανοίγω τα προγράμματα πλοήγησης και τις εφαρμογές** - Θα σας ζητηθεί να εισάγετε τον βασικό σας κωδικό όταν ανοίγετε ένα πρόγραμμα πλοήγησης ή μια εφαρμογή.

- **Μην με ρωτάτε για τον κύριο κωδικό πρόσβασής μου** - δεν θα σας ζητηθεί να εισαγάγετε τον κύριο κωδικό πρόσβασης όταν έχετε πρόσβαση στη συσκευή, σε ένα πρόγραμμα περιήγησης ή σε μια εφαρμογή.
- **Αυτόματο κλείδωμα του Wallet όταν αφήνω το PC μου αφύλακτο** - Θα σας ζητηθεί να εισάγετε το βασικό σας κωδικό όταν επιστρέψετε στον υπολογιστή σας μετά από 15 λεπτά.

Σημαντικό

Βεβαιωθείτε ότι θυμάστε τον βασικό κωδικό πρόσβασής σας ή κρατήστε ένα αρχείο αυτού σε ασφαλές μέρος. Εάν ξεχάσετε τον κωδικό πρόσβασης, θα πρέπει να εγκαταστήσετε ξανά το πρόγραμμα ή να επικοινωνήσετε με το Bitdefender για υποστήριξη.

Βελτιώστε την εμπειρία σας

Για να επιλέξετε τα προγράμματα πλοήγησης ή τις εφαρμογές στις οποίες θέλετε να ενσωματώσετε το Διαχειριστή Κωδικών Ασφαλείας:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **PASSWORD MANAGER**, πατήστε **Ρυθμίσεις**.
3. Επιλέξτε το παράθυρο **Ρυθμίσεις** .

   Ενεργοποιήστε το διακόπτη δίπλα σε μια εφαρμογή για να χρησιμοποιήσετε το Password Manager και να βελτιώσετε την εμπειρία σας:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Διαμόρφωση του Autofill

Η λειτουργία Αυτόματης Συμπλήρωσης καθιστά εύκολο για εσάς να συνδεθείτε με τις αγαπημένες σας ιστοσελίδες ή να συνδεθείτε με τους online λογαριασμούς σας. Την πρώτη φορά που θα εισάγετε τα στοιχεία σύνδεσής σας και τις προσωπικές πληροφορίες στο πρόγραμμα πλοήγησής σας, αυτόματα σώζονται στο Wallet.

Για να διαμορφώσετε τις ρυθμίσεις **Autofill**.

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **PASSWORD MANAGER**, πατήστε **Ρυθμίσεις**.
3. Στο παράθυρο **Ρυθμίσεις** , μεταβείτε στην καρτέλα **Ρυθμίσεις αυτόματης συμπλήρωσης** .
4. Ρυθμίστε τις εξής επιλογές:
   - **Ρυθμίστε το πώς ο Διαχειριστής Κωδικών Ασφαλείας ασφαλίζει τους κωδικούς σας**:
     - **Αποθήκευση των κωδικών αυτόματα στο Wallet** - οι κωδικοί σύνδεσης και άλλες αναγνωρίσιμες πληροφορίες όπως τα προσωπικά και τα στοιχεία της πιστωτικής σας κάρτας αποθηκεύονται αυτόματα και ενημερώνονται μέσα στο Wallet.
     - **Να γίνεταιη ερώτηση κάθε φορά** - θα σας ζητείται κάθε φορά, αν θέλετε να προσθέσετε τα διαπιστευτήριά σας στο πορτοφόλι.
     - **Να μην αποθηκευτεί, Θα ενημερώσω τις πληροφορίες χειροκίνητα** - τα διαπιστευτήρια μπορούν να προστεθούν μόνο με χειροκίνητα στο πορτοφόλι.
   - **Αυτόματη συμπλήρωση διαπιστευτηρίων σύνδεσης**:
     - **Αυτόματη Συμπλήρωση των κωδικών σας κάθε φορά** - οι κωδικοί σας εισάγονται αυτόματα στο πρόγραμμα περιήγησης.
   - **Φόρμες αυτόματης συμπλήρωσης**:
     - **Προτείνεται αυτόματη συμπλήρωσει των στοιχείων μου όταν επισκέπτομαι μια σελίδα με φόρμα συμπλήρωσης** - ένα αναδυόμενο παράθυρο θα εμφανίζεται κάθε φορά που το Bitdefender ανιχνεύει ότι θέλετε να εκτελέσετε μια ηλεκτρονική πληρωμή ή μια εγγραφή.

Διαχειριστείτε τις πληροφορίες του Διαχειριστή Κωδικών Ασφαλείας από τον browser σας

Μπορείτε να διαχειριστείτε εύκολα το Διαχειριστή Κωδικών Ασφαλείας κατευθείαν από τον browser σας, για να έχετε όλα τα σημαντικά στοιχεία στη διάθεσή σας. Το Bitdefender Wallet add-on υποστηρίζεται από τα παρακάτω προγράμματα περιήγησης: Google Chrome, Internet Explorer και τον Mozilla Firefox, και επίσης μπορεί να ενσωματωθεί με το Safepay.

Για να αποκτήσετε πρόσβαση στην επέκταση του Bitdefender Wallet, ανοίξτε το πρόγραμμα περιήγησης, επιτρέψτε στο add-on να εγκατασταθεί και κάντε κλικ στο εικονίδιο στη γραμμή εργαλείων.

Η επέκταση Bitdefender Wallet περιέχει τις ακόλουθες επιλογές:

- Ανοιγμα Πορτοφολιού - ανοίγει το πορτοφόλι.
- Κλείδωμα Πορτοφολιού - κλειδώνει το πορτοφόλι.
- Ιστοσελίδες - ανοίγει ένα υπομενού με όλα τα logins στις ιστοσελίδες των οποίων οι συνδέσεις αποθηκεύονται στο Wallet. Κάντε κλικ στο**Προσθήκη ιστοσελίδας** για να προσθέσετε νέες ιστοσελίδες στη λίστα.
- Συμπληρώστε φόρμες - ανοίγει ένα υπομενού που περιέχει τις πληροφορίες που έχετε προσθέσει για μια συγκεκριμένη κατηγορία. Από εδώ μπορείτε να προσθέσετε νέα δεδομένα στο Wallet σας.
- Password Generator - σας δίνει τη δυνατότητα να δημιουργήσετε τυχαίους κωδικούς πρόσβασης που μπορείτε να χρησιμοποιήσετε για νέους ή υπάρχοντες λογαριασμούς. Κάντε κλικ στο **Εμφάνιση σύνθετων ρυθμίσεων** να προσαρμόσετε την πολυπλοκότητα του κωδικού πρόσβασης.
- Ρυθμίσεις - ανοίγει το παράθυρο ρυθμίσεων του Διαχειριστή Κωδικών Ασφαλείας.
- Αναφορά ζητήματος - αναφέρετε οποιοδήποτε ζήτημα που αντιμετωπίζετε με τον Bitdefender Διαχειριστή Κωδικών Ασφαλείας.

4.10. Anti-tracker

Πολλοί ιστότοποι που επισκέπτεστε χρησιμοποιούν trackers για τη συλλογή πληροφοριών σχετικά με τη συμπεριφορά σας, είτε για να τις μοιραστεί με εταιρείες τρίτων είτε για να προβάλλει διαφημίσεις που είναι πιο συναφείς για εσάς. Με αυτόν τον τρόπο, οι ιδιοκτήτες ιστότοπων κερδίζουν χρήματα για να σας παρέχουν δωρεάν περιεχόμενο ή να συνεχίσουν να λειτουργούν. Εκτός από τη συλλογή πληροφοριών, οι trackers μπορούν να επιβραδύνουν την εμπειρία περιήγησης ή να χρησιμοποιήσουν το bandwidth σας.

Με την επέκταση ενεργοποιημένη του Bitdefender Anti-Tracker στο πρόγραμμα περιήγησης ιστού, αποφεύγετε να σας παρακολουθούν, ώστε

τα δεδομένα σας να παραμένουν ιδιωτικά κατά την περιήγηση στο διαδίκτυο και να επιταχύνετε τον χρόνο που χρειάζεται να φορτώσουν οι ιστότοποι.

Η επέκταση του Bitdefender είναι συμβατή με τα ακόλουθα προγράμματα περιήγησης ιστού:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

Οι trackers που ανιχνεύουμε ομαδοποιούνται στις παρακάτω κατηγορίες:

- **Διαφήμιση** - χρησιμοποιείται για την ανάλυση της επισκεψιμότητας των ιστότοπων, της συμπεριφοράς των χρηστών ή των επισκεπτών.
- **Αλληλεπίδραση Πελατών** - χρησιμοποιείται για τη μέτρηση της αλληλεπίδρασης του χρήστη με διαφορετικές φόρμες εισόδου, όπως η συνομιλία ή η υποστήριξη.
- **Απαραίτητο** - χρησιμοποιείται για την παρακολούθηση σημαντικών λειτουργιών ιστοσελίδας.
- **Ανάλυση Ιστοστελίδας** - χρησιμοποιείται για τη συλλογή δεδομένων σχετικά με τη χρήση της ιστοσελίδας.
- **Κοινωνικά Δίκτυα** - χρησιμοποιείται για την παρακολούθηση του κοινωνικού κοινού, της δραστηριότητας και της εμπλοκής του χρήστη με διαφορετικές πλατφόρμες κοινωνικών μέσων.

Περιβάλλον Anti-tracker

Όταν είναι ενεργοποιημένη η επέκταση Bitdefender Anti-tracker, εμφανίζεται το εικονίδιο δίπλα στη γραμμή αναζήτησης στο πρόγραμμα περιήγησής σας. Κάθε φορά που επισκέπτεστε έναν ιστότοπο, μπορεί να παρατηρηθεί ένας μετρητής στο εικονίδιο, αναφερόμενος στους εντοπισμένους και αποκλεισμένους trackers. Για να δείτε περισσότερες λεπτομέρειες σχετικά με τους αποκλεισμένους trackers, κάντε κλικ στο εικονίδιο για να ανοίξετε το περιβάλλον. Εκτός από τον αποκλεισμό του αριθμού των trackers , μπορείτε να δείτε τον χρόνο που απαιτείται για τη φόρτωση της σελίδας και τις κατηγορίες στις οποίες ανήκουν οι εντοπισμένοι trackers. Για να προβάλετε τη λίστα με τους ιστότοπους που παρακολουθούν, κάντε κλικ στην κατηγορία που θέλετε.

Για να απενεργοποιήσετε το Bitdefender από το να μπλοκάρει τους trackers στον ιστότοπο που επισκέπτεστε αυτήν τη στιγμή, κάντε κλικ στην επιλογή **Παύση προστασίας σε αυτόν τον ιστότοπο**. Αυτή η ρύθμιση ισχύει μόνο εφόσον έχετε ανοιχτό τον ιστότοπο και θα επανέλθει στην αρχική κατάσταση όταν κλείσετε τον ιστότοπο.

Για να επιτρέψετε σε trackers από συγκεκριμένη κατηγορία να παρακολουθούν τη δραστηριότητά σας, κάντε κλικ στην επιθυμητή δραστηριότητα και, στη συνέχεια, κάντε κλικ στο αντίστοιχο κουμπί. Αν αλλάξετε γνώμη, κάντε ξανά κλικ στο ίδιο κουμπί.

Απενεργοποιώντας το Bitdefender Anti-tracker

Για να ενεργοποιήσετε το Bitdefender Anti-tracker:

- Από τον πλοηγό σας:
  1. Ανοίξτε τον browser σας.
  2. Επιλέξτε το εικονίδιο δίπλα στη γραμμή διευθύνσεων του browser σας.
  3. Κάντε κλικ στο εικονίδιο στην επάνω δεξιά πλευρά της οθόνης.
  4. Χρησιμοποιήστε τον αντίστοιχο διακόπτη για το απενεργοποιήσετε.

     Το Bitdefender εικονίδιο γίνεται γκρι.
- Από το περιβάλλον του Bitdefender:
  1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
  2. Στο παράθυρο **ANTI-TRACKER**, κάντε κλικ στο κουμπί **Ρυθμίσεις**.
  3. Δίπλα στο browser για το οποίο θέλετε να απενεργοποιήσετε την επέκταση, απενεργοποιήστε τον αντίστοιχο διακόπτη.

Επιτρέποντας την παρακολούθηση ενός ιστότοπου

Εάν θέλετε να παρακολουθείστε την ώρα που επισκέπτεστε έναν συγκεκριμένο ιστότοπο, μπορείτε να προσθέσετε τη διεύθυνσή του στις εξαιρέσεις ως εξής:

1. Ανοίξτε τον browser σας.
2. Κάντε κλικ στο κουμπί δίπλα στη γραμμή αναζήτησης.

3. Κάντε κλικ στο εικονίδιο στην επάνω δεξιά πλευρά της οθόνης.
4. Εάν βρίσκεστε στον ιστότοπο που θέλετε να προσθέσετε σε εξαιρέσεις, κάντε κλικ στην επιλογή **Προσθήκη τρέχοντος ιστότοπου στη λίστα** .

   Εάν θέλετε να προσθέσετε έναν άλλο ιστότοπο, πληκτρολογήστε τη διεύθυνσή του στο αντίστοιχο πεδίο και, στη συνέχεια, κάντε κλικ στο κουμπί .

4.11. VPN

Η εφαρμογή VPN μπορεί να εγκατασταθεί από το προϊόν σας Bitdefender προϊόν και να χρησιμοποιηθεί κάθε φορά που θέλετε να προσθέσετε ένα επιπλέον επίπεδο προστασίας στη σύνδεσή σας. Το VPN χρησιμεύει ως σήραγγα μεταξύ της συσκευής σας και του δικτύου που συνδέετε για να εξασφαλίζετε τη σύνδεσή σας, κρυπτογραφώντας τα δεδομένα χρησιμοποιώντας κρυπτογράφηση τραπεζικής ποιότητας και αποκρύπτοντας τη διεύθυνση IP όπου κι αν βρίσκεστε. Η επισκεψιμότητά σας μεταφέρεται μέσω ενός ξεχωριστού διακομιστή. καθιστώντας έτσι τη συσκευή σας σχεδόν αδύνατη να ταυτοποιηθεί μέσω των μυριάδων άλλων συσκευών που χρησιμοποιούν τις υπηρεσίες μας. Επιπλέον, ενώ είστε συνδεδεμένοι στο διαδίκτυο μέσω του Bitdefender VPN, μπορείτε να αποκτήσετε πρόσβαση σε περιεχόμενο που συνήθως περιορίζεται σε συγκεκριμένες περιοχές.

Σημείωση

Ορισμένες χώρες ασκούν λογοκρισία στο Διαδίκτυο και ως εκ τούτου η χρήση των VPN στην επικράτειά τους έχει απαγορευτεί από το νόμο. Για να αποφύγετε νομικές συνέπειες, μπορεί να εμφανιστεί ένα προειδοποιητικό μήνυμα όταν επιχειρήσετε να χρησιμοποιήσετε την εφαρμογή Bitdefender VPN για πρώτη φορά. Συνεχίζοντας τη χρήση της εφαρμογής, επιβεβαιώνετε ότι γνωρίζετε τους ισχύοντες κανονισμούς των χωρών και τους κινδύνους στους οποίους ενδέχεται να εκτεθείτε.

Εγκατάσταση VPN

Το VPN μπορεί να εγκατασταθεί από το Bitdefender περιβάλλον σας ως εξής:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο **VPN** παράθυρο, επιλέξτε **Εγκατάσταση VPN**.

3. το παράθυρο με την περιγραφή της εφαρμογής VPN, διαβάστε τη **Συμφωνία συνδρομής**, και στη συνέχεια, κάντε κλικ στην επιλογή**ΕΓΚΑΤΑΣΤΑΣΗ BITDEFENDER VPN**.

   Περιμένετε λίγα λεπτά μέχρι να γίνει λήψη και εγκατάσταση των αρχείων.

   Εάν εντοπιστεί άλλη εφαρμογή VPN, σας συνιστούμε να την απεγκαταστήσετε. Έχοντας εγκαταστήσει πολλές λύσεις VPN, μπορεί να αντιμετωπίσετε επιβράδυνση του συστήματος ή άλλα προβλήματα λειτουργικότητας.

4. Κάντε κλικ στο κουμπί **ΕΝΕΡΓΟΠΟΙΗΣΗ BITDEFENDER VPN** για να ολοκληρώσετε τη διαδικασία εγκατάστασης.

Σημείωση

Το Bitdefender VPN απαιτεί να εγκατασταθεί το Net Framework 4.5.2 ή νεότερο. Σε περίπτωση που δεν έχετε εγκαταστήσει αυτό το πακέτο, εμφανίζεται ένα παράθυρο ειδοποίησης. Κάντε κλικ στο **Εγκατάσταση. Net Framework** για να μεταφερθείτε σε μια σελίδα από την οποία μπορείτε να κατεβάσετε τη νεότερη έκδοση αυτού του λογισμικού.

Ανοίγοντας το VPN

Για να αποκτήσετε πρόσβαση στην κύρια πλατφόρμα του Bitdefender VPN, χρησιμοποιήστε μία από τις ακόλουθες μεθόδους:

- Από την περιοχή ειδοποιήσεων
  1. Κάντε δεξί κλικ στο εικονίδιο στο system tray και, στη συνέχεια, κάντε κλικ στο **Εμφάνιση**.
- Από το περιβάλλον του Bitdefender:
  1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
  2. Στο παράθυρο **VPN**, πατήστε **Άνοιγμα VPN**.

VPN interface

Το παράθυρο του VPN εμφανίζει την κατάσταση της εφαρμογής, συνδεδεμένη ή αποσυνδεδεμένη. Η τοποθεσία του server για χρήστες με δωρεάν έκδοση ορίζεται αυτόματα από το Bitdefender στον πιο κατάλληλο server, ενώ οι premium χρήστες έχουν τη δυνατότητα να αλλάξουν τη θέση του διακομιστή με την οποία επιθυμούν να συνδεθούν. Για περισσότερες

πληροφορίες σχετικά με αυτή τη λειτουργία, παρακαλούμε ανατρέξτε στο “Συνδρομές” (p. 159).

Για να συνδέσετε ή να αποσυνδέσετε, απλά κάντε κλικ στην κατάσταση που εμφανίζεται στο επάνω μέρος της οθόνης ή κάντε δεξί κλικ στο εικονίδιο της γραμμής συστήματος. Το εικονίδιο της γραμμής συστήματος εμφανίζει ένα πράσινο σημάδι ελέγχου όταν το VPN είναι συνδεδεμένο και ένα κόκκινο σημάδι ελέγχου όταν αποσυνδεθεί το VPN.

Κατά τη σύνδεση, ο χρόνος που έχει παρέλθει και η χρήση του bandwidth εμφανίζονται στο κάτω μέρος του interface.

Για να δείτε πλήρως την περιοχή **Μενού** , κάντε κλικ στο εικονίδιο στην επάνω αριστερή πλευρά. Εδώ έχετε τις εξής επιλογές:

- **Ο λογαριασμός μου** - εμφανίζονται λεπτομέρειες σχετικά με τον Bitdefender λογαριασμό σας και τη συνδρομή VPN. Κάντε κλικ στην επιλογή **Αλλαγή λογαριασμού** , εάν θέλετε να συνδεθείτε με άλλον λογαριασμό.

  Κάντε κλικ στο **Προσθήκη εδώ** για να προσθέσετε έναν κωδικό ενεργοποίησης για το Bitdefender Premium VPN.

- **Ρυθμίσεις** – ανάλογα με τις ανάγκες σας, μπορείτε να προσαρμόσετε τη συμπεριφορά του προϊόντος σας. Οι Ρυθμίσεις ομαδοποιούνται σε δύο κατηγορίες:

  - **Γενικά**
    - Ειδοποιήσεις
    - Εκκίνηση - επιλέξτε αν θα εκτελείται το Bitdefender VPN κατά την εκκίνηση ή όχι
    - Αναφορές προϊόντων - υποβάλετε ανώνυμες αναφορές προϊόντων για να μας βοηθήσετε να βελτιώσουμε την εμπειρία σας
    - Σκοτεινή λειτουργία
    - Γλώσσα
  - **Για προχωρημένους**
    - Internet Kill-Switch - αυτή η λειτουργία αναστέλλει προσωρινά όλη την κίνηση στο Διαδίκτυο εάν η σύνδεση VPN πέσει κατά λάθος. Μόλις συνδεθείτε ξανά, η σύνδεση VPN θα αποκατασταθεί.

- Αυτόματη σύνδεση - Συνδέστε το Bitdefender VPN αυτόματα όταν έχετε πρόσβαση σε ένα δημόσιο / μη ασφαλές δίκτυο Wi-Fi ή όταν ξεκινά μια εφαρμογή κοινής χρήσης αρχείων peer-to-peer

- **Υποστήριξη** - μπορείτε να αποκτήσετε πρόσβαση στην πλατφόρμα του Κέντρου υποστήριξης από όπου μπορείτε να διαβάσετε ένα χρήσιμο άρθρο σχετικά με τον τρόπο χρήσης του VPN Bitdefender ή να μας στείλετε σχόλια.

- **Σχετικά με** - Εμφανίζονται πληροφορίες σχετικά με την εγκατεστημένη έκδοση.

Συνδρομές

Το Bitdefender VPN προσφέρει δωρεάν μια ημερήσια quota κίνησης 200 MB ανά συσκευή για να εξασφαλίσει τη σύνδεσή σας κάθε φορά που χρειάζεστε και σας συνδέει αυτόματα με τη βέλτιστη τοποθεσία του server.

Για να έχετε απεριόριστη κίνηση και απεριόριστη πρόσβαση στο περιεχόμενο σε όλο τον κόσμο επιλέγοντας μια τοποθεσία διακομιστή σύμφωνα με τη βούλησή σας, αναβαθμίστε την έκδοση Premium.

Μπορείτε να πραγματοποιήσετε αναβάθμιση στην έκδοση Bitdefender Premium VPN ανά πάσα στιγμή κάνοντας κλικ στο κουμπί **Αναβάθμιση** που είναι διαθέσιμο στη διεπαφή του προϊόντος.

Η συνδρομή Bitdefender Premium VPN είναι ανεξάρτητη από τη Bitdefender Total Security συνδρομή , πράγμα που σημαίνει ότι θα μπορείτε να το χρησιμοποιήσετε για ολόκληρη τη διαθεσιμότητα, ανεξάρτητα από την κατάσταση της συνδρομής κατά των ιών. Σε περίπτωση που λήξει η συνδρομή Bitdefender Premium VPN, αλλά το προϊόν για το Bitdefender Total Security εξακολουθεί να είναι ενεργό, θα επανέλθετε στην ελεύθερη έκδοση.

Το Bitdefender [VPN] είναι προϊόν πολλαπλής πλατφόρμας, διαθέσιμο σε Bitdefender προϊόντα συμβατά με Windows, mac OS, Android και iOS. Μόλις αναβαθμίσετε στην premium έκδοση, να είστε σε θέση να χρησιμοποιήσετε τη συνδρομή σας σε όλα τα προϊόντα, υπό την προϋπόθεση ότι θα συνδεθείτε με τον ίδιο Bitdefender λογαριασμό.

4.12. Ασφάλεια Safepay για online συναλλαγές

Ο υπολογιστής έχει σχεδόν γίνει το κύριο εργαλείο για ψώνια και τραπεζικές συναλλαγές. Πληρωμή λογαριασμών, μεταφορά χρημάτων, η

αγορά σχεδόν οποιουδήποτε προϊόντος μπορείτε να φανταστείτε, δεν ήταν ποτέ πιο εύκολη και γρήγορη.

Αυτό περιλαμβάνει την αποστολή προσωπικών πληροφοριών, δεδομένα λογαριασμών και πιστωτικής κάρτας, κωδικούς πρόσβασης και άλλα είδη των προσωπικών πληροφοριών μέσω του Διαδικτύου, με άλλα λόγια, ακριβώς το είδος πληροφοριών το οποίο οι εγκληματίες του κυβερνοχώρου ενδιαφέρονται πολύ να αξιοποιήσουν. Οι χάκερς είναι αμείλικτοι στις προσπάθειές τους να κλέψουν την πληροφορία αυτή, δεν μπορείτε ποτέ να είστε πάρα πολύ προσεκτικοί σχετικά με την ασφάλεια των ηλεκτρονικών συναλλαγών.

Το Bitdefender Safepay™ είναι πρώτα από όλα ένα προστατευμένο πρόγραμμα πλοήγησης, ένα κλειστό περιβάλλον το οποίο έχει σχεδιαστεί για να κρατήσει τις online συναλλαγές σας, το e-shopping σας και κάθε άλλου είδους online συναλλαγής σας, προσωπική και ασφαλή.

Για την βέλτιστη προστασία των προσωπικών δεδομένων σας, ο Bitdefender Διαχειριστής Κωδικών Ασφαλείας έχει ενταχθεί στο Bitdefender Safepay™ για να εξασφαλίσει τους κωδικούς σας κάθε φορά που εσείς θέλετε να αποκτήσετε πρόσβαση σε έναν ιδιωτικό διαδικτυακό χώρο. Για περισσότερες πληροφορίες, ανατρέξτε στην "*Προστασία των κωδικών σας με το Διαχειριστή Κωδικών Ασφαλείας*" (p. 145).

Το Bitdefender Safepay™ προσφέρει τις ακόλουθες δυνατότητες:

- Εμποδίζει την πρόσβαση στην επιφάνεια εργασίας σας και οποιαδήποτε απόπειρα λήψης στιγμιότυπων(snapshots) της οθόνης σας.
- Προστατεύει τους μυστικούς κωδικούς πρόσβασης σας κατά την περιήγηση στο διαδίκτυο με το Διαχειριστή Κωδικών Ασφαλείας.
- Συνοδεύεται με ένα εικονικό πληκτρολόγιο το οποίο, όταν χρησιμοποιείται, καθιστά αδύνατο για τους χάκερς να διαβάσουν τις πληκτρολογήσεις σας.
- Είναι εντελώς ανεξάρτητο από άλλα προγράμματα πλοήγησης σας.
- Έρχεται με ενσωματωμένη προστασία hotspot για χρήση όταν η συσκευή σας είναι συνδεδεμένη σε μη ασφαλή δίκτυα Wi-Fi.
- Υποστηρίζει σελιδοδείκτες και σας επιτρέπει να περιηγηθείτε στις αγαπημένες σας ιστοσελίδες τραπεζικών/αγορών σας.
- Δεν περιορίζεται σε τραπεζικές συναλλαγές και e-shopping. Κάθε ιστοσελίδα μπορεί να ανοίξει σε Bitdefender Safepay™.

Χρησιμοποιώντας το Bitdefender Safepay™

Από προεπιλογή, το Bitdefender εντοπίζει όταν πλοηγείστε σε έναν ιστότοπο τραπεζικών συναλλαγών ή σε ηλεκτρονικό κατάστημα σε οποιοδήποτε πρόγραμμα περιήγησης στη συσκευή σας και σας ζητά να το ξεκινήσετε στο Bitdefender Safepay™.

Για να αποκτήσετε πρόσβαση στην κύρια πλατφόρμα του Bitdefender Safepay™, χρησιμοποιήστε μία από τις ακόλουθες μεθόδους:

- Από τη διεπαφή Bitdefender:
  1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
  2. Στο παράθυρο **Safepay**, πατήστε **Ρυθμίσεις**.
  3. Στο παράθυρο **Safepay** , κάντε κλικ στο **Εκκίνηση Safepay** .
- Από τα Windows:
  - Στα **Windows 7**:
    1. Κάντε κλικ στην **Έναρξη** και οδηγηθείτε στο **Όλα τα προγράμματα**.
    2. Κάντε κλικ στο **Bitdefender**.
    3. Κάντε κλικ στο **Bitdefender Safepay™**.
  - Στα **Windows 8 και στα Windows 8.1**:

    Εντοπίστε το Bitdefender Safepay™ από το μενού έναρξης των Windows (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Bitdefender Safepay" απευθείας στο μενού Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιο.
  - Στα **Windows 10**:

    Πληκτρολογήστε "Bitdefender Safepay™" στο πλαίσιο αναζήτησης από τη γραμμή εργασιών και κάντε κλικ στο εικονίδιο του.

Αν έχετε συνηθίσει σε προγράμματα πλοήγησης, δεν θα έχετε κανένα πρόβλημα με τη χρήση του Bitdefender Safepay™ - φαίνεται και συμπεριφέρεται όπως ένα κανονικό πρόγραμμα πλοήγησης:

- εισάγετε στην γραμμή διευθύνσεων, διευθύνσεις URL στις οποίες θέλετε να μεταβείτε.
- προσθέστε καρτέλες για να επισκεφθείτε διάφορες ιστοσελίδες στο Bitdefender Safepay™ κάνοντας κλικ στο + .

- περιηγηθείτε πίσω και εμπρός και ανανεώστε τις σελίδες χρησιμοποιώντας το ← → ↻ αντίστοιχα.
- Μπείτε στοBitdefender Safepay™ Ρυθμίσεις κάνοντας κλικ ••• και επιλέγοντας **Ρυθμίσεις**.
- προστατέψτε τους κωδικούς πρόσβασης σας με το Διαχειριστή Κωδικών Ασφαλείας κάνοντας κλικ στο .
- διαχείριση των σελιδοδεικτών κάνοντας κλικ στο ☆ δίπλα από την μπάρα διευθύνσεων.
- άνοιγμα του εικονικού πληκτρολογίου κάνοντας κλικ στο .
- αυξήσετε ή να μειώσετε το μέγεθος του προγράμματος πλοήγησης πατώντας ταυτόχρονα το **Ctrl** και τα πλήκτρα **+/-** στο αριθμητικό πληκτρολόγιο.
- δείτε πληροφορίες σχετικά με το προϊόν Bitdefender κάνοντας κλικ στο ••• και επιλέγοντας **Σχετικά**.
- εκτυπώστε σημαντικές πληροφορίες κάνοντας κλικ ••• και επιλέγοντας **Εκτύπωση** .

Σημείωση
Για εναλλαγή μεταξύ της επιφάνειας Bitdefender Safepay™ και Windows desktop, πατήστε τα πλήκτρα **Alt+Tab**, ή κάντε κλικ στην επιλογή **Μεταφορά στο Desktop** στην επάνω αριστερή πλευρά του παραθύρου.

Διαμόρφωση ρυθμίσεων

Κάντε κλικ ••• και επιλέξτε **Ρυθμίσεις** για να ρυθμίσετε το Bitdefender Safepay™:

Εφαρμογή κανόνων Bitdefender Safepay για πρόσβαση σε domains
Οι ιστοσελίδες που έχετε προσθέσει στους Σελιδοδείκτες με ενεργοποιημένη την επιλογή **Αυτόματη ανοιχτό στο Safepay** θα

εμφανιστούν εδώ. Αν θέλετε να σταματήσετε το αυτόματα με το Bitdefender Safepay ™ για έναν ιστότοπο από τη λίστα, κάντε κλικ στο × δίπλα στην καταχώρηση που θέλετε από τη στήλη **Κατάργηση** .

Αποκλεισμός pop- ups

Μπορείτε να επιλέξετε να αποκλείσετε τα αναδυόμενα παράθυρα κάνοντας κλικ στον αντίστοιχο διακόπτη.

Μπορείτε επίσης να δημιουργήσετε μια λίστα των δικτυακών τόπων από τους οποίους επιτρέπετε τα pop- ups. Ο κατάλογος θα πρέπει να περιλαμβάνει μόνο τις ιστοσελίδες που εμπιστεύεστε πλήρως.

Για να προσθέσετε μια ιστοσελίδα στην λίστα, συμπληρώστε την διεύθυνση της στο αντίστοιχο πεδίο και κάντε κλικ στο κουμπί **Προσθήκη Domain**.

Για να καταργήσετε μια ιστοσελίδα από τη λίστα, επιλέξτε το X που αντιστοιχεί στην επιθυμητή καταχώρηση.

Manage Plugins

Μπορείτε να επιλέξετε αν θέλετε να ενεργοποιήσετε ή να απενεργοποιήσετε συγκεκριμένες προσθήκες στο Bitdefender Safepay™.

Διαχείριση πιστοποιητικών

Μπορείτε να εισάγετε πιστοποιητικά από το σύστημά σας σε ένα κατάστημα πιστοποιητικών.

Κάντε κλικ στο **ΕΙΣΑΓΩΓΗ** και ακολουθήστε τον οδηγό για να χρησιμοποιήσετε τα πιστοποιητικά στο Bitdefender Safepay ™.

Χρησιμοποιήστε Εικονικό Πληκτρολόγιο

Το εικονικό πληκτρολόγιο εμφανίζεται αυτόματα όταν επιλέγεται ένα πεδίο κωδικού πρόσβασης.

Χρησιμοποιήστε τον αντίστοιχο διακόπτη για να ενεργοποιήσετε ή να απενεργοποιήσετε τη λειτουργία.

Εκτύπωση επιβεβαίωσης

Ενεργοποιήστε την επιλογή αν θα θέλατε να επιβεβαιώνετε για να ξεκινά η διαδικασία εκτύπωσης.

Διαχείριση σελιδοδεικτών

Εάν έχετε απενεργοποιήσει την αυτόματη ανίχνευση ορισμένων ή όλων των δικτυακών τόπων το Bitdefender απλά δεν θα ανιχνεύσει συγκεκριμένες ιστοσελίδες, μπορείτε να προσθέσετε σελιδοδείκτες στο

Bitdefender Safepay ™, έτσι ώστε να μπορείτε εύκολα να ξεκινήσετε τις αγαπημένες σας ιστοσελίδες στο μέλλον.

Ακολουθήστε τα παρακάτω βήματα για να προσθέσετε μια διεύθυνση URL σε Bitdefender Safepay ™ σελιδοδείκτες:

1. Κάντε κλικ στο ••• και επιλέξτε **Σελιδοδείκτες** για να ανοίξετε τη σελίδα σελιδοδεικτών.

   Σημείωση
   Η σελίδα σελιδοδεικτών ανοίγει από προεπιλογή όταν ξεκινάτε το Bitdefender Safepay ™.

2. Κάντε κλικ στο **+** κουμπί για να προσθέσετε ένα νέο σελιδοδείκτη.
3. Εισάγετε τη διεύθυνση URL και τον τίτλο του σελιδοδείκτη και πατήστε **ΔΗΜΙΟΥΡΓΙΑ**. Επιλέξτε το **Αυτόματο άνοιγμα με Safepay** αν θέλετε το σελιδοδείκτη να ανοίγει με το Bitdefender Safepay™ κάθε φορά που τον ανοίγετε. Η διεύθυνση URL προστίθεται επίσης στη λίστα Domains στην Ρυθμίσεις .

Απενεργοποίηση των ειδοποιήσεων Safepay

Όταν εντοπιστεί ένα τραπεζικό site, το Bitdefender προϊόν έχει ρυθμιστεί για να σας ειδοποιεί μέσω pop-up παραθύρου.

Για να απενεργοποίησετε τις ενημερώσεις Safepay

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Safepay**, πατήστε **Ρυθμίσεις**.
3. Στο παράθυρο **Ρυθμίσεις** , απενεργοποιήστε το διακόπτη δίπλα στις **Ειδοποιήσεις Safepay** .

Χρήση VPN με Safepay

Για να πραγματοποιήσετε ηλεκτρονικές πληρωμές σε ασφαλές περιβάλλον ενώ είστε συνδεδεμένοι σε μη ασφαλή δίκτυα, το Bitdefender προϊόν έχει ρυθμιστεί για αυτόματη εκκίνηση της εφαρμογής VPN με το Safepay.

Για να σταματήσετε να χρησιμοποιείτε την εφαρμογή VPN μαζί με το Safepay:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.

2. Στο παράθυρο **Safepay**, πατήστε **Ρυθμίσεις**.
3. Στο παράθυρο **Ρυθμίσεις** , ενεργοποιήστε το διακόπτη δίπλα στο **Χρήση VPN με Safepay** .

4.13. Γονικός Έλεγχος

Bitdefender Γονικός Σύμβουλος σας επιτρέπει να διαχειρίζεστε και να προστατεύετε τις δραστηριότητες του παιδιού σας στο διαδίκτυο. Μόλις διαμορφώσετε το Bitdefender Γονικό Σύμβουλο, μπορείτε εύκολα να μάθετε τι κάνουν τα παιδιά σας στις συσκευές που χρησιμοποιούν και που βρίσκονταν τις τελευταίες 24 ώρες. Επιπλέον, για να σας βοηθήσει να γνωρίζετε καλύτερα τι κάνουν τα παιδιά σας, το χαρακτηριστικό σας παρέχει στατιστικά στοιχεία σχετικά με τις δραστηριότητες και τα ενδιαφέροντά τους.

Στη συνδρομή σας στο Bitdefender έχετε συμπεριλάβει τις ακόλουθες λειτουργίες:

- Στις συσκευές Windows, macOS και Android:
  - Αποκλεισμός ακατάλληλων ιστοσελίδων.
  - Αποκλείστε εφαρμογές όπως παιχνίδια, συνομιλία, προγράμματα κοινής χρήσης αρχείων ή άλλα.
  - Αποκλείστε τη χρήση της παρακολουθούμενης συσκευής.
  - Αποκλείστε την πρόσβαση στο διαδίκτυο για συγκεκριμένες χρονικές περιόδους (όπως όταν είναι ώρα για μαθήματα).
  - Ορίστε χρονικούς περιορισμούς για τη χρήση των συσκευών.
  - Δείτε τον μέσο χρόνο που αφιερώνουν τα παιδιά σας σε μια συσκευή.
  - Δείτε μια αναφορά με τις εφαρμογές που χρησιμοποιήθηκαν στη συσκευή που έγινε η παρακολούθηση τις τελευταίες 30 ημέρες.
  - Ορίστε ελεγχόμενες περιοχές.
  - Βρείτε τη θέση του παιδιού σας στο Android.
- Στις συσκευές με iOS:
  - Αποκλείστε τις εισερχόμενες κλήσεις από τη λίστα επαφών.
  - Ορίστε ελεγχόμενες περιοχές.
  - Βρείτε τη θέση της iOS συσκευής του παιδιού σας.

Για να ελέγξετε τις ηλεκτρονικές δραστηριότητες των παιδιών σας, να διαχειριστείτε τις συσκευές που χρησιμοποιούν τα παιδιά σας ή να αλλάξετε τις ρυθμίσεις στον Γονικό Σύμβουλο, πρέπει να έχετε πρόσβαση στο λογαριασμό σας στο Bitdefender.

Υπάρχουν δύο δυνατότητες πρόσβασης στο λογαριασμό σας στο Bitdefender, είτε από ένα πρόγραμμα περιήγησης ιστού, πηγαίνοντας στο https://central.bitdefender.com, είτε από την εφαρμογή Bitdefender Central, η οποία μπορεί να εγκατασταθεί σε συσκευές με Android ή iOS.

Για να εγκαταστήσετε την Bitdefender Centralεφαρμογή στις συσκευές σας:

- **Σε Android** - αναζητήστε Bitdefender Central στο Google Play και στη συνέχεια κατεβάστε και εγκαταστήστε την εφαρμογή. Ακολουθήστε τα απαιτούμενα βήματα για να ολοκληρώσετε την εγκατάσταση.
- **Σε iOS** - αναζητήστε Bitdefender Central στο App Store και στη συνέχεια κάντε λήψη και εγκατάσταση της εφαρμογής. Ακολουθήστε τα απαιτούμενα βήματα για να ολοκληρώσετε την εγκατάσταση.

Σημείωση
Σε αυτό το υλικό παρέχονται οι επιλογές και οι οδηγίες που διατίθενται στην πλατφόρμα web.

4.13.1. Πρόσβαση στον Γονικό Έλεγχο - Τα παιδιά μου

Μόλις έχετε πρόσβαση στην ενότητα γονικού ελέγχου, το **παράθυρο Τα παιδιά μου** είναι διαθέσιμο. Εδώ μπορείτε να ξεκινήσετε τη δημιουργία προφίλ για τα παιδιά σας και αργότερα να τα δείτε και να τα επεξεργαστείτε. Μόλις δημιουργηθούν, τα προφίλ εμφανίζονται ως κάρτες προφίλ, επιτρέποντάς σας να τα διαχειριστείτε γρήγορα και να ελέγξετε τις καταστάσεις τους με μια ματιά.

Μόλις δημιουργήσετε ένα προφίλ, μπορείτε να αρχίσετε να προσαρμόζετε πιο λεπτομερείς ρυθμίσεις για την παρακολούθηση και τον έλεγχο της πρόσβασης στο Internet και σε ειδικές εφαρμογές για τα παιδιά σας.

Μπορείτε να αποκτήσετε πρόσβαση στις ρυθμίσεις γονικού ελέγχου από το Bitdefender Central σε οποιονδήποτε υπολογιστή ή φορητή συσκευή συνδεδεμένη στο Διαδίκτυο.

Εισέλθετε στο Bitdefender λογαριασμό:

- Σε οποιαδήποτε συσκευή με πρόσβαση στο Διαδίκτυο:

1. Πρόσβαση στο Bitdefender Central.
2. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Επιλέξτε τον πίνακα **Γονικός Σύμβουλος**.
4. Στο παράθυρο που εμφανίζεται, μπορείτε να διαχειριστείτε και να διαμορφώσετε τα προφίλ γονικού ελέγχου για κάθε συσκευή.

- Από το Bitdefender περιβάλλον σας:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Στο **ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ** , κάντε κλικ **Ρύθμιση**.

   Θα μεταφερθείτε στην ιστοσελίδα του Bitdefender λογαριασμού. Βεβαιωθείτε ότι έχετε συνδεθεί με τους κωδικούς σας.
3. Επιλέξτε την δυνατότητα **Γονικός Έλεγχος**.
4. Στο παράθυρο που εμφανίζεται, μπορείτε να διαχειριστείτε και να διαμορφώσετε τα προφίλ γονικού ελέγχου για κάθε συσκευή.

Σημείωση
Βεβαιωθείτε ότι έχετε συνδεθεί στη συσκευή με λογαριασμό διαχειριστή. Μόνο οι χρήστες με δικαιώματα διαχειριστή συστήματος (διαχειριστές του συστήματος) μπορούν να έχουν πρόσβαση και να διαμορφώσουν τον Γονικό Έλεγχο.

4.13.2. Δημιουργήστε προφίλ για τα παιδιά σας

Για να ξεκινήσετε την παρακολούθηση των δραστηριοτήτων των παιδιών σας στο διαδίκτυο, πρέπει να ρυθμίσετε τα προφίλ και να εγκαταστήσετε την εφαρμογή Bitdefender Γονικός Σύμβουλος στις συσκευές που χρησιμοποιούν.

Για να δημιουργήσετε ένα προφίλ παιδιού:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε τον πίνακα Γονικός Σύμβουλος.
3. Κάντε κλικ στο **ΠΡΟΣΘΗΚΗ ΠΡΟΦΙΛ ΠΑΙΔΙΟΥ** στο παράθυρο **Τα παιδιά μου** .
4. Ορίστε συγκεκριμένες πληροφορίες, όπως όνομα, ημερομηνία γέννησης ή φύλο. Για να προσθέσετε μια εικόνα στο προφίλ του παιδιού σας, κάντε

κλικ στο εικονίδιο στην κάτω δεξιά γωνία **Εικόνα προφίλ**. Κάντε κλικ στο **ΑΠΟΘΗΚΕΥΣΗ** για να συνεχίσετε.

Με βάση τα πρότυπα ανάπτυξης των παιδιών, τον καθορισμό της ηλικίας του παιδιού φορτώνονται οι αυτόματα προδιαγραφές που θεωρούνται κατάλληλες για την κατηγορία της ηλικίας του.

5. Κάντε κλικ **ΑΣ ΠΡΟΣΘΕΣΟΥΜΕ ΜΙΑ ΣΥΣΚΕΥΗ**
6. Εάν η συσκευή του παιδιού σας έχει ήδη εγκατεστημένο Bitdefender προϊόν , επιλέξτε τη συσκευή του από τη διαθέσιμη λίστα και στη συνέχεια επιλέξτε τον λογαριασμό που θέλετε να παρακολουθήσετε. Κάντε κλικ στο **ΑΝΤΙΣΤΟΙΧΙΣΗ**.

   Εάν το παιδί δεν έχει εγκατεστημένο το Bitdefender προϊόν στη συσκευή που χρησιμοποιεί, κάντε κλικ στην επιλογή **Εγκατάσταση σε μια νέα συσκευή** και στη συνέχεια, κάντε κλικ στο κουμπί **ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΛΗΨΗΣ**. Πληκτρολογήστε μια διεύθυνση email στο αντίστοιχο πεδίο και κάντε κλικ στο **Αποστολή email** . Λάβετε υπόψη ότι ο παραγόμενος σύνδεσμος λήψης ισχύει μόνο για τις επόμενες 24 ώρες. Εάν λήξει ο σύνδεσμος, θα πρέπει να δημιουργήσετε ένα νέο, ακολουθώντας τα ίδια βήματα.

   Στη συσκευή που θέλετε να εγκαταστήσετε το Bitdefender, ελέγξτε τον email λογαριασμό που πληκτρολογήσατε και στη συνέχεια κάντε κλικ στο αντίστοιχο κουμπί λήψης.

Σημαντικό

Σε συσκευές που βασίζονται σε Windows και macOS και δεν έχουν εγκατεστημένο προϊόν Bitdefender, θα εγκατασταθεί το πρόγραμμα παρακολούθησης γονικού ελέγχου Bitdefender και θα μπορείτε να παρακολουθείτε τις δραστηριότητες των παιδιών στο διαδίκτυο.
Στις συσκευές Android και iOS, θα γίνει λήψη και εγκατάστασης της εφαρμογής Bitdefender Parental Control.

Για να αντιστοιχίσετε άλλες συσκευές, κάντε κλικ στο **ΠΡΟΣΘΗΚΗ ΣΥΣΚΕΥΗΣ** δίπλα στο προφίλ του παιδιού. Ακολουθήστε τις οδηγίες από το βήμα 6 που παρέχονται σε αυτό το κεφάλαιο.

Εγκατάσταση της εφαρμογής Bitdefender Γονικός Σύμβουλος σε συσκευές Android και iOS

Για να παρακολουθήσετε τις δραστηριότητες των παιδιών σας σε συσκευές Android ή iOS, πρέπει να εγκαταστήσετε την ειδική εφαρμογή Γονικού

Συμβούλου και στη συνέχεια, να συνδέσετε τις συσκευές τους με το λογαριασμό σας στο Bitdefender. Ανάλογα με τις συσκευές που έχουν τα παιδιά σας, ακολουθήστε τα εξής βήματα:

- Σε **Android**:

1. Μεταβείτε στο Google Play Store, αναζητήστε το Bitdefender Parental Control και στη συνέχεια, πατήστε την επιλογή εγκατάστασης.
2. Πατήστε **ΑΠΟΔΟΧΗ** όταν σας ζητηθεί να επιτρέψετε δικαιώματα. Το Bitdefender χρειάζεται άδεια για να σας ενημερώνει για τη δραστηριότητα του παιδιού σας και εάν δεν γίνει αποδεκτή, η εφαρμογή δεν θα εγκατασταθεί.
3. Εκκινήστε την εφαρμογή Γονικός Σύμβουλος.
4. Ένας οδηγός εισαγωγής που περιέχει λεπτομέρειες σχετικά με τις λειτουργίες του προϊόντος εμφανίζεται την πρώτη φορά που ανοίγετε την εφαρμογή. Επιλέξτε **Επόμενο** για να συνεχίσετε με τις οδηγίες, ή **Παράλειψη περιήγησης** για να κλείσετε τον οδηγό.
5. Για να συνεχίσετε με την εγκατάσταση, το Bitdefender χρειάζεται την έγκρισή σας για τη συλλογή προσωπικών δεδομένων που ανήκουν στο παιδί σας, το οποίο θα χρησιμοποιείται μόνο για να σας παρέχει πληροφορίες σχετικά με τη δραστηριότητα του παιδιού σας. Για περισσότερες λεπτομέρειες, πατήστε **Πολιτική απορρήτου**. Πατώντας **ΣΥΝΕΧΕΙΑ** συμφωνείτε να συλλέξετε προσωπικά δεδομένα από τη συσκευή.
6. Συνδεθείτε στο υπάρχοντα λογαριασμό σας Bitdefender. Αν δεν έχετε Bitdefender λογαριασμό, επιλέξτε να δημιουργήσετε ένα νέο λογαριασμό χρησιμοποιώντας την αντίστοιχη επιλογή. Εναλλακτικά, μπορείτε να συνδεθείτε χρησιμοποιώντας έναν Facebook, Google ή Microsoft λογαριασμό.
7. Πατήστε **ΕΝΕΡΓΟΠΟΙΗΣΗ** για να μεταφερθείτε στην οθόνη από όπου μπορείτε να ενεργοποιήσετε την επιλογή Προσβασιμότητα για την εφαρμογή. Ακολουθήστε τις οδηγίες στην οθόνη για να ρυθμίσετε σωστά την εφαρμογή.
8. Επιλέξτε **ΕΠΕΤΡΕΨΕ** για να γίνει ανακατεύθυνση στην οθόνη από όπου μπορείτε να ενεργοποιήσετε την επιλογή Ενεργοποίηση πρόσβασης για την εφαρμογή. Ακολουθήστε τις οδηγίες στην οθόνη για να ρυθμίσετε σωστά την εφαρμογή.

9. Επιλέξτε **ΕΝΕΡΓΟΠΟΙΗΣΗ** για να γίνει ανακατεύθυνση στην οθόνη από όπου μπορείτε να ενεργοποιήσετε την επιλογή δικαιωμάτων ενεργοποίησης διαχειριστή συσκευής για την εφαρμογή. Ακολουθήστε τις οδηγίες στην οθόνη για να ρυθμίσετε σωστά την εφαρμογή.

   Αυτό θα αποτρέψει το παιδί σας από την απεγκατάσταση του Γονικού Συμβούλου.

10. Κάντε κλικ στο **ΕΠΙΛΟΓΗ** και, στη συνέχεια, εκχωρήστε όλα τα απαιτούμενα δικαιώματα.

11. Αντιστοιχίστε την συσκευή με το προφίλ του παιδιού σας.

- Σε **iOS**:

1. Μεταβείτε στο App Store, αναζητήστε το Bitdefender Parental Control και στη συνέχεια, πατήστε την επιλογή εγκατάστασης.

2. Για να συνεχίσετε με την εγκατάσταση, το Bitdefender χρειάζεται την έγκρισή σας για τη συλλογή προσωπικών δεδομένων που ανήκουν στο παιδί σας, το οποίο θα χρησιμοποιείται μόνο για να σας παρέχει πληροφορίες σχετικά με τη δραστηριότητα του παιδιού σας. Για περισσότερες λεπτομέρειες, πατήστε **Πολιτική απορρήτου**. Πατώντας **Συνέχεια**, συμφωνείτε στη συλλογή προσωπικών δεδομένων από τη συσκευή.

3. Συνδεθείτε στο υπάρχοντα λογαριασμό σας Bitdefender. Αν δεν έχετε Bitdefender λογαριασμό, επιλέξτε να δημιουργήσετε ένα νέο λογαριασμό χρησιμοποιώντας την αντίστοιχη επιλογή. Εναλλακτικά, μπορείτε να συνδεθείτε χρησιμοποιώντας έναν Facebook, Google ή Microsoft λογαριασμό.

4. Σας ζητείται να δώσετε πρόσβαση σε όλα τα απαιτούμενα δικαιώματα που απαιτούνται για την εφαρμογή. Επιλέξτε **Επέτρεψε**.

5. Επιστρέψτε την πρόσβαση στη θέση της συσκευής σας έτσι ώστε το Bitdefender να μπορεί να το εντοπίσει.

6. Επιστρέψτε στην εφαρμογή να στείλει ειδοποιήσεις. Για να διαχειριστείτε τις ειδοποιήσεις του Bitdefender, μεταβείτε στην περιοχή Ρυθμίσεις > Ειδοποιήσεις >Parental.

7. Για να μπορέσετε να παρακολουθήσετε τις επαφές του παιδιού σας, θα πρέπει να ενεργοποιήσετε το **Κλείδωμα κλήσεων & Ταυτοποίηση**. Ακολουθήστε τα απαιτούμενα βήματα ώστε να μπορείτε να

χρησιμοποιήσετε το Bitdefender Γονικό Σύμβουλο για να περιορίσετε τις εισερχόμενες τηλεφωνικές κλήσεις.

8. Αντιστοιχίστε την συσκευή με το προφίλ του παιδιού σας.

Παρακολουθήστε τις δραστηριότητες των παιδιών σας στο διαδίκτυο

Ο Bitdefender Γονικός Σύμβουλος σας βοηθά να παρακολουθείτε τι κάνουν τα παιδιά σας online. Με αυτόν τον τρόπο, μπορείτε πάντα να μάθετε με ακρίβεια σε ποιες δραστηριότητες εμπλέκονταν, ενώ ξόδευαν χρόνο στις αντιστοιχισμένες συσκευές που έχουν.

Ανάλογα με τις ρυθμίσεις που κάνετε, το Bitdefender σας παρέχει αναφορές που μπορεί να περιέχουν λεπτομερείς πληροφορίες για κάθε συμβάν, όπως:

- Η κατάσταση του συμβάντος
- Η σοβαρότητα της ειδοποίησης.
- Το όνομα της συσκευής.
- Η ημερομηνία και η ώρα που συνέβη το γεγονός.

Για να παρακολουθήσετε την κίνηση στο διαδίκτυο, τις εφαρμογές που έχετε πρόσβαση ή τις ηλεκτρονικές δραστηριότητες για τα παιδιά σας:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε τον πίνακα Γονικός Σύμβουλος.
3. Επιλέξτε ένα παιδικό προφίλ.

   Στο κύριο παράθυρο **Δραστηριότητα** μπορείτε να δείτε τις πληροφορίες που σας ενδιαφέρουν.

Διαμόρφωση ρυθμίσεων Αναφορών

Από προεπιλογή, όταν είναι ενεργοποιημένος ο Γονικός Έλεγχος, οι δραστηριότητες των παιδιών σας καταγράφονται.

Για να λαμβάνετε ειδοποιήσεις μέσω email σχετικά με τις online δραστηριότητες των παιδιών σας:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε τον πίνακα Γονικός Σύμβουλος.

3. Κάντε κλικ στο **ΡΥΘΜΙΣΕΙΣ ΑΝΑΦΟΡΏΝ**.
4. Ενεργοποιήστε τον αντίστοιχο διακόπτη για να λαμβάνετε αναφορές δραστηριότητας.
5. Εισάγετε τη διεύθυνση e-mail στην οποία θα στέλνονται οι ειδοποιήσεις.
6. Προσαρμόστε τη συχνότητα επιλέγοντας: καθημερινά, εβδομαδιαία ή μηνιαία και, στη συνέχεια, κάντε κλικ στο **ΑΠΟΘΉΚΕΥΣΗ**.

Μπορείτε επίσης να επιλέξετε να λαμβάνετε ειδοποιήσεις στον Bitdefender λογαριασμό σας στις ακόλουθες περιπτώσεις:

- Κάθε φορά που τα παιδιά σας προσπαθούν να αποκτήσουν πρόσβαση σε εφαρμογές που έχουν αποκλειστεί (σε Windows, macOS και Android).
- Κάθε φορά που τα παιδιά σας λαμβάνουν κλήσεις από αποκλεισμένους / άγνωστους αριθμούς τηλεφώνου (στο iOS).
- Κάθε φορά που τα παιδιά σας εγκαταλείπουν τις ασφαλείς περιοχές ή εισέρχονται σε απαγορευμένες περιοχές.
- Κάθε φορά που τα παιδιά σας κάνουν check-in ως ασφαλή.

Επεξεργασία ενός προφίλ

Για να επεξεργαστείτε ένα υπάρχον προφίλ:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε τον πίνακα **Γονικός Σύμβουλος**.
3. Κάντε κλικ στο **ΕΠΙΛΟΓΕΣ** στην επιθυμητή κάρτα προφίλ και, στη συνέχεια, επιλέξτε **Επεξεργασία προφίλ** .
4. Αφού προσαρμόσετε τις επιθυμητές ρυθμίσεις, επιλέξτε **ΑΠΟΘΗΚΕΥΣΗ**.

Διαγραφή ενός προφίλ

Για να διαγράψετε ένα υπάρχον προφίλ:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε τον πίνακα **Γονικός Σύμβουλος**.
3. Επιλέξτε το προφίλ παιδιού.
4. Κάντε κλικ στο κουμπί **ΕΠΙΛΟΓΕΣ** και, στη συνέχεια, επιλέξτε **Διαγραφή προφίλ** .
5. Επιβεβαιώστε την επιλογή σας.

4.13.3. Ρυθμίζοντας τα προφίλ του Γονικού Ελέγχου

ια να ξεκινήσετε να παρακολουθείτε το παιδί σας, θα πρέπει να οριστεί ένα προφίλ σε μια συσκευή που έχει εγκατεστημένο τον Bitdefender Γονικό Έλεγχο .

Μετά την προσθήκη ενός προφίλ για το παιδί σας, μπορείτε να προσαρμόσετε πιο λεπτομερείς ρυθμίσεις για την παρακολούθηση και τον έλεγχο της πρόσβασης στο Internet και σε ειδικές εφαρμογές.

Για να ξεκινήσετε τη διαμόρφωση ενός προφίλ, επιλέξτε την επιθυμητή κάρτα προφίλ και κάντε κλικ στο **ΕΠΙΛΟΓΕΣ** .

Κάντε κλικ σε μια καρτέλα για να διαμορφώσετε την αντίστοιχη λειτουργία Γονικού Συμβούλου για τη συσκευή:

- Screentime - εδώ μπορείτε να αποκλείσετε την πρόσβαση στις συσκευές που καθορίσατε στα προφίλ των παιδιών σας. Η πρόσβαση μπορεί να περιοριστεί σε ένα συγκεκριμένο χρονικό διάστημα και σε αθροιστικά ημερήσια όρια.
- Εφαρμογές - σας δίνει τη δυνατότητα να εμποδίσετε την πρόσβαση σε ορισμένες εφαρμογές, όπως παιχνίδια, λογισμικό ανταλλαγής μηνυμάτων, ταινίες, κ.λπ.
- Websites - σας επιτρέπει να ασφαλίσετε την πλοήγηση στο Διαδίκτυο.
- Τοποθεσία παιδιού - εδώ μπορείτε να ορίσετε τις τοποθεσίες που είναι ασφαλείς ή όχι για το παιδί σας.
- Επαφές τηλεφώνου - εδώ μπορείτε να δείτε τις επαφές στο τηλέφωνο του παιδιού σας.
- Προβολή συσκευών - εδώ μπορείτε να δείτε την κατάσταση των συσκευών που παρακολουθείτε, να αντιστοιχίσετε μια νέα συσκευή στο προφίλ του παιδιού σας ή να καταργήσετε μια εκχωρημένη συσκευή.

Δραστηριότητα

Το κύριο παράθυρο σας παρέχει λεπτομερείς πληροφορίες σχετικά με τις διαδικτυακές δραστηριότητες των παιδιών σας από τις τελευταίες 24 ώρες ή από τις τελευταίες 7 ημέρες, ανάλογα με την επιλογή σας, εντός και εκτός σπιτιού. Για να δείτε δραστηριότητες από τις προηγούμενες επτά ημέρες κάντε κλικ στο **Τελευταίες 7 ημέρες** .

Ανάλογα με τη δραστηριότητα, αυτό το παράθυρο μπορεί να περιλαμβάνει πληροφορίες σχετικά με:

- **Τοποθεσία για παιδιά** - εδώ μπορείτε να δείτε τις τοποθεσίες όπου βρίσκονταν τα παιδιά σας κατά τη διάρκεια της ημέρας.
- **Δραστηριότητα ιστότοπου** - εδώ μπορείτε να δείτε πληροφορίες σχετικά με τις κατηγορίες ιστότοπων που έχουν επισκεφτεί τα παιδιά σας. Κάντε κλικ στο σύνδεσμο **ΑΛΛΑΓΗ ΡΥΘΜΙΣΕΩΝ** για να επιτρέψετε ή να αρνηθείτε την πρόσβαση σε συγκεκριμένα ενδιαφέροντα.
- **Τελευταίες επαφές τηλεφώνου που προστέθηκαν** - εδώ μπορείτε να δείτε εάν έχουν προστεθεί νέες επαφές στις συσκευές του παιδιού σας. Κάντε κλικ στο σύνδεσμο **ΠΡΟΒΟΛΗ ΟΛΩΝ ΤΩΝ ΤΗΛΕΦΩΝΩΝ** για να επιλέξετε τις επαφές με τις οποίες τα παιδιά σας πρέπει να παραμένουν σε επαφή ή όχι.
- **Εφαρμογές** - εδώ μπορείτε να δείτε τις εφαρμογές που χρησιμοποιεί το παιδί σας. Κάντε κλικ στο σύνδεσμο **ΠΡΟΒΟΛΗ ΟΛΩΝ ΕΦΑΡΜΟΓΩΝ** για να αποκλείσετε ή να επιτρέψετε την πρόσβαση σε συγκεκριμένες εφαρμογές.
- **Χρόνος οθόνης** - εδώ μπορείτε να δείτε το χρόνο που αφιερώνεται στο διαδίκτυο σε όλες τις συσκευές που έχουν εκχωρηθεί στα παιδιά σας. Κάντε κλικ στο **ΠΡΟΒΟΛΗ ΧΡΟΝΟΥ ΟΘΟΝΗΣ** για πρόσβαση στο παράθυρο **Ώρα οθόνης** .

Εφαρμογές

Το παράθυρο Εφαρμογές σας επιτρέπει να αποκλείσετε την εκτέλεση εφαρμογών σε Windows, macOS, Android και iOS συσκευές. Παιχνίδια, μέσα ενημέρωσης και λογισμικό ανταλλαγής μηνυμάτων, καθώς και άλλες κατηγορίες λογισμικού μπορούν να αποκλειστούν με αυτό τον τρόπο.

Εδώ μπορείτε επίσης να προβάλλετε τις πρώτες 30 ημέρες εφαρμογών που χρησιμοποιεί το παιδί σας μαζί με το χρόνο που δαπανά σας για τη χρήση τους. Η πληροφορία σχετικά με το χρόνο που δαπανάται για τη χρήση εφαρμογών μπορεί να ανακτηθεί μόνο από συσκευές Windows, macOS και Android.

Για να ρυθμίσετε τη Διαχείριση Εφαρμογών ενός συγκεκριμένου λογαριασμού χρήστη:

1. Εμφανίζεται μια λίστα με τις διαθέσιμες συσκευές.

Επιλέξτε την κάρτα με την συσκευή της οποίας θέλετε να περιορίσετε την πρόσβαση της σε εφαρμογές.

2. Κάντε κλικ **Διαχείριση των εφαρμογών που χρησιμοποιούνται από ...** .

   Εμφανίζεται μια λίστα με τις εγκατεστημένες εφαρμογές.

3. Επιλέξτε **Αποκλεισμός** δίπλα στις εφαρμογές που θέλετε να σταματήσει να χρησιμοποιεί το παιδί σας.

4. Κάντε κλικ στο **ΑΠΟΘΗΚΕΥΣΗ** για να εφαρμόσετε τις ρυθμίσεις.

Μπορείτε να διακόψετε την παρακολούθηση των εγκατεστημένων εφαρμογών απενεργοποιώντας την επιλογή **Παρακολούθηση εφαρμογών** στην επάνω δεξιά γωνία του παραθύρου.

Websites

Το παράθυρο Ιστοσελίδες σάς βοηθά να αποκλείσετε websites με ακατάλληλο περιεχόμενο σε συσκευές με Windows, MacOS και Android. Ιστοσελίδες που φιλοξενούν βίντεο, παιχνίδια, media και λογισμικό ανταλλαγής μηνυμάτων, καθώς και άλλες κατηγορίες αρνητικού περιεχομένου μπορεί να αποκλειστούν με αυτό τον τρόπο.

Η λειτουργία μπορεί να ενεργοποιηθεί ή να απενεργοποιηθεί χρησιμοποιώντας τον αντίστοιχο διακόπτη.

Ανάλογα με την ηλικία που ορίζετε για τα παιδιά σας, ο κατάλογος Ενδιαφέροντα έρχεται από προεπιλογή με μια λίστα ενεργοποιημένων κατηγοριών . Για να επιτρέψετε ή να αρνηθείτε την πρόσβαση σε μια συγκεκριμένη κατηγορία, κάντε κλικ σε αυτή.

Το εικονίδιο που εμφανίζεται υποδεικνύει ότι το παιδί σας δεν θα έχει πρόσβαση στο περιεχόμενο που σχετίζεται με την συγκεκριμένη κατηγορία.

Αποδοχή ή αποκλεισμός μιας ιστοσελίδας

Για να επιτρέψετε ή να περιορίσετε την πρόσβαση σε ορισμένες ιστοσελίδες, θα πρέπει να τις προσθέσετε στη λίστα Εξαιρέσεις, ως εξής:

1. Κάντε κλικ στο κουμπί **ΔΙΑΧΕΙΡΙΣΗ**.

2. Πληκτρολογήστε την ιστοσελίδα που θέλετε να επιτρέψετε στο αντίστοιχο πεδίο.

3. Επιλέξτε **Αποδοχή** ή **Άρνηση**.
4. Κάντε κλικ στο εικονίδιο **+** για να αποθηκεύσετε τις αλλαγές.

Σημείωση
Οι περιορισμοί πρόσβασης στους ιστότοπους μπορούν να ρυθμιστούν μόνο για συσκευές Windows, Android και macOS που έχουν προστεθεί στο προφίλ του παιδιού σας.

Τηλεφωνικές επαφές

Το παράθυρο "Επαφές τηλεφώνου" σας δίνει τη δυνατότητα να δείτε τις επαφές στο τηλέφωνο του παιδιού σας.

Η δυνατότητα είναι διαθέσιμη σε συσκευές iOS και Android.

Τοποθεσία παιδιού

Δείτε την τρέχουσα θέση της συσκευής στο Google Maps. Η τοποθεσία ανανεώνεται κάθε 5 δευτερόλεπτα, ώστε να μπορείτε να παρακολουθείτε αν είναι σε κίνηση.

Η ακρίβεια της τοποθεσίας εξαρτάται από το πόσο το Bitdefender είναι σε θέση να την προσδιορίσει:

- Εάν το GPS είναι ενεργοποιημένο στη συσκευή, η θέση του μπορεί να εντοπιστεί με προσέγγιση μερικών μέτρων για όσο διάστημα είναι στο εύρος των δορυφόρων GPS (π.χ. δεν είναι μέσα σε ένα κτίριο).
- Αν η συσκευή είναι σε εσωτερικό χώρο, η θέση του μπορεί να προσδιοριστεί με προσέγγιση δεκάδων μέτρων εάν το Wi-Fi είναι ενεργοποιημένο και υπάρχουν διαθέσιμα ασύρματα δίκτυα σε κοντινή απόσταση.
- Σε αντίθετη περίπτωση, η θέση θα προσδιορίζεται με τη χρήση μόνο των πληροφοριών από το δίκτυο κινητής τηλεφωνίας, το οποίο μπορεί να προσφέρει ακρίβεια όχι καλύτερη από αρκετές εκατοντάδες μέτρα.

Διαμόρφωση τοποθεσίας & Ασφαλές Check-in

Για να είστε σίγουροι ότι το παιδί σας πηγαίνει σε ορισμένες τοποθεσίες, μπορείτε να κάνετε μια λίστα με ασφαλή και μη ασφαλή μέρη. Κάθε φορά που μπαίνει μόνος του σε μια προκαθορισμένη περιοχή, θα εμφανιστεί μια ειδοποίηση στην εφαρμογή του γονικού συμβούλου, ζητώντας να επιβεβαιωθεί ότι είναι ασφαλής. Πατώντας το πλήκτρο **ΕΦΤΑΣΑ ΜΕ**

ΑΣΦΑΛΕΙΑ ενημερώνεστε μέσω ειδοποίησης στο Bitdefender λογαριασμό σας ότι έχει επιτευχθεί ο τελικός προορισμός.

Σε περίπτωση που δεν έχει δοθεί επιβεβαίωση από το παιδί σας, εξακολουθείτε να βλέπετε το ιστορικό της τοποθεσίας του καθ 'όλη τη διάρκεια της ημέρας ελέγχοντας το προφίλ του στον Bitdefender λογαριασμό σας.

Για να ρυθμίσετε μια τοποθεσία:

1. Στη διεπαφή γονικού ελέγχου, αποκτήστε πρόσβαση στο προφίλ του παιδιού σας, κάντε κλικ στο **ΕΠΙΛΟΓΕΣ** και επιλέξτε το παράθυρο **Τοποθεσία παιδιού** .
2. Κάντε κλικ στο **Συσκευές** .
3. Κάντε κλικ στη συσκευή που θέλετε να διαμορφώσετε.
4. Στο παράθυρο **Περιοχές**, κάντε κλικ στο κουμπί **ΠΡΟΣΘΗΚΗ ΠΕΡΙΟΧΗΣ**.
5. Επιλέξτε το είδος της τοποθεσίας, **SAFE** ή **RESTRICTED**.
6. Πληκτρολογήστε ένα έγκυρο όνομα για την περιοχή όπου το παιδί σας έχει δικαίωμα πρόσβασης ή όχι.
7. Ορίστε το εύρος που πρέπει να εφαρμοσθεί για την παρακολούθηση από τη γραμμή ολίσθησης **Ακτίνα**.
8. Κάντε κλικ στο **ΠΡΟΣΘΗΚΗ ΠΕΡΙΟΧΗΣ** για να αποθηκεύσετε τις ρυθμίσεις σας. Δέχεστε την ερώτηση αν τα παιδιά σας πρόκειται να ταξιδέψουν μόνα τους ή όχι. Επιβεβαιώστε με Ναι ή Όχι.

Σημείωση

Ο εντοπισμός θέσης μπορεί να χρησιμοποιηθεί για την παρακολούθηση συσκευών Android και iOS που έχουν εγκαταστήσει την εφαρμογή Bitdefender Γονικό Σύμβουλο.

Screentime

Στο παράθυρο Screentime ενημερώνεστε για το χρόνο που αφιερώνεται στις εκχωρημένες συσκευές την τρέχουσα ημέρα, τον χρόνο που απομένει από το ημερήσιο όριο που έχετε ορίσει και την κατάσταση του επιλεγμένου προφίλ, ενεργό ή σε παύση. Από αυτό το παράθυρο μπορείτε επίσης να ορίσετε χρονικούς περιορισμούς για διαφορετικές ώρες της ημέρας, όπως η ώρα ύπνου, η εργασία ή ιδιωτικά μαθήματα.

Χρονικοί περιορισμοί

Για να ξεκινήσετε τη ρύθμιση των χρονικών περιορισμών:

1. Κάντε κλικ στο **ΕΠΙΛΟΓΕΣ** και επιλέξτε **Screentime** .
2. Στην περιοχή **Προγραμματισμένα** , κάντε κλικ στο **ΠΡΟΣΘΗΚΗ ΠΡΟΓΡΑΜΜΑΤΟΣ** .
3. Δώστε ένα όνομα στο πρόγραμμα που θέλετε να ορίσετε (για παράδειγμα, ώρα ύπνου, εργασία στο σπίτι, μαθήματα τένις κ.λπ.).
4. Ορίστε το χρονικό πλαίσιο και τις ημέρες κατά τις οποίες πρέπει να εφαρμόζονται οι περιορισμοί και, στη συνέχεια, κάντε κλικ στο **ΠΡΟΣΘΗΚΗ ΠΡΟΓΡΑΜΜΑΤΟΣ** για να αποθηκεύσετε τις ρυθμίσεις.

Για να επεξεργαστείτε έναν περιορισμό που έχετε ορίσει, μεταβείτε στην ενότητα Προγράμματα, επισημάνετε τον περιορισμό που θέλετε να επεξεργαστείτε και κάντε κλικ στο κουμπί **Επεξεργασία** .

Για να διαγράψετε έναν περιορισμό, μεταβείτε στο παράθυρο Ώρα οθόνης, δείξτε τον περιορισμό που θέλετε να επεξεργαστείτε, κάντε κλικ στο **Επεξεργασία** και, στη συνέχεια, επιλέξτε **ΔΙΑΓΡΑΦΗ ΠΡΟΓΡΑΜΜΑΤΟΣ** .

Ημερήσιο όριο

Το ημερήσιο όριο χρήσης μπορεί να εφαρμοστεί σε Windows, MacOS και Android συσκευές. Εάν ρυθμίσετε το προφίλ που πρόκειται να τεθεί σε παύση μόλις επιτευχθεί το όριο, τότε αυτή η ρύθμιση θα ισχύει για όλες τις συσκευές που έχουν εκχωρηθεί, ανεξάρτητα από το αν πρόκειται για Windows, macOS, Android ή iOS.

Για να ρυθμίσετε την όριο καθημερινής χρήσης:

1. Κάντε κλικ στο **ΕΠΙΛΟΓΕΣ** και επιλέξτε **ΡΥΘΜΙΣΗ ΗΜΕΡΗΣΙΩΝ ΧΡΟΝΙΚΌΝ ΟΡΙΩΝ** .
2. Ορίστε την ώρα και τις ημέρες κατά τις οποίες πρέπει να εφαρμόζονται οι περιορισμοί και, στη συνέχεια, κάντε κλικ στο **ΑΠΟΘΗΚΕΥΣΗ ΑΛΛΑΓΩΝ** για να αποθηκεύσετε τις ρυθμίσεις.

4.14. Κατά της κλοπής συσκευής (Anti-Theft)

Κλοπή φορητού υπολογιστή είναι ένα μείζον θέμα που επηρεάζει άτομα όσο και οργανώσεις. Ακόμη περισσότερο και από την απώλεια του ίδιου

του υλικού, τα στοιχεία που χάνονται με αυτό μπορεί να προκαλέσουν σημαντικές ζημίες, τόσο σε οικονομικό όσο και συναισθηματικό επίπεδο.

Ωστόσο, λίγοι άνθρωποι παίρνουν τα κατάλληλα μέτρα για να εξασφαλίσουν σημαντικά προσωπικά, επιχειρηματικά και οικονομικά δεδομένα τους σε περίπτωση κλοπής ή απώλειας.

Το Bitdefender Anti-Theft σας βοηθά να είστε καλύτερα προετοιμασμένοι για ένα τέτοιο ενδεχόμενο, επιτρέποντάς σας να εντοπίσετε απομακρυσμένα ή να κλειδώσετε τον υπολογιστή σας, ακόμα και να εξαλείψετε όλα τα δεδομένα από αυτόν, σε περίπτωση που αποχωριστείτε τον υπολογιστή σας παρά τη θέλησή σας.

Για να χρησιμοποιήσετε τις λειτουργίες Anti-Theft, οι ακόλουθες προϋποθέσεις πρέπει να πληρούνται:

- Οι εντολές μπορούν να σταλούν μόνο από το Bitdefender λογαριασμό.
- Ο υπολογιστής πρέπει να είναι συνδεδεμένος με το Διαδίκτυο για να λάβει τις εντολές.

Οι λειτουργίες Anti-Theft λειτουργούν ως εξής:

Εντοπισμός

Δείτε την θέση της συσκευής σας στο Google Maps.

Η ακρίβεια της τοποθεσίας εξαρτάται από το πόσο το Bitdefender είναι σε θέση να την προσδιορίσει. Η τοποθεσία προσδιορίζεται με ακρίβεια δεκάδων μέτρων, εάν το Wi-Fi είναι ενεργοποιημένο στον υπολογιστή σας και υπάρχουν ασύρματα δίκτυα στο βεληνεκές του.

Εάν ο υπολογιστής είναι συνδεδεμένος σε ενσύρματο δίκτυο LAN χωρίς διαθεσιμότητα εύρεσης τοποθεσίας βάση του Wi-Fi, η τοποθεσία θα καθορίζεται με βάση τη διεύθυνση IP, η οποία είναι πολύ λιγότερο ακριβής.

Ειδοποίηση

Αποστολή απομακρυσμένης ειδοποίησης στη συσκευή.

Η λειτουργία είναι διαθέσιμη μόνο για κινητά.

ΚΛΕΙΔΩΜΑ

Κλειδώστε τον υπολογιστή σας και ορίστε έναν 4ψήφιο κωδικό PIN για το ξεκλείδωμα του. Όταν στέλνετε την εντολή **Lock**, ο υπολογιστής επανεκκινεί και η εκ νέου σύνδεση στα Windows είναι δυνατή μόνο μετά την εισαγωγή του PIN που έχετε ορίσει.

Αν θέλετε το Bitdefender να τραβήξει φωτογραφίες από αυτόν που προσπαθεί να αποκτήσετε πρόσβαση στο φορητό υπολογιστή σας, επιλέξτε την αντίστοιχη επιλογή. Οι στιγμιαίες φωτογραφίες έχουν ληφθεί χρησιμοποιώντας την μπροστινή κάμερα και εμφανίζονται μαζί σήμανση του χρόνου στο Anti-Theft ταμπλό. Αποθηκευτούν μόνο οι δύο πιο πρόσφατες φωτογραφίες.

Αυτή η ενέργεια είναι διαθέσιμη μόνο για τους φορητούς υπολογιστές που έχουν μπροστινή κάμερα.

Διαγραφή

Απαλοιφή όλων των δεδομένων από τον υπολογιστή σας. Όταν στέλνετε την εντολή **Wipe**, ο υπολογιστής επανεκκινεί και τα δεδομένα για όλα τα διαμερίσματα του σκληρού δίσκου διαγράφονται

Εμφάνιση IP

Εμφανίζει την τελευταία διεύθυνση IP για την επιλεγμένη συσκευή. Κάντε κλικ στο **SHOW IP** ώστε να είναι ορατή.

Το Anti-Theft ενεργοποιείται μετά την εγκατάσταση και μπορεί να προσεγγιστεί μόνο μέσω του Bitdefender λογαριασμού σας από οποιαδήποτε συσκευή που συνδέεται στο Διαδίκτυο, οπουδήποτε.

Χρησιμοποιώντας τις λειτουργίες Anti-Theft

Για να αποκτήσετε πρόσβαση στις λειτουργίες Anti-Theft, χρησιμοποιείστε μία από τις παρακάτω δυνατότητες:

- Από τη κεντρική διεπαφή του Bitdefender:

  1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
  2. Επιλέξτε **ΜΕΤΑΒΑΣΗ ΣΤΟ CENTRAL**.

     Θα ανακατευθυνθείτε στη σελίδα του Bitdefender Central. Βεβαιωθείτε ότι έχετε συνδεθεί με τους κωδικούς σας.
  3. Στο παράθυρο Bitdefender Central που ανοίγει, κάντε κλικ στην καρτέλα της συσκευής που επιθυμείτε και στη συνέχεια επιλέξτε το **Anti-Theft**.

- Σε οποιαδήποτε συσκευή με πρόσβαση στο Διαδίκτυο:

  1. Ανοίξτε ένα παράθυρο πλοήγησης και πηγαίνετε στο: https://central.bitdefender.com.

2. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Επιλέξτε το **Οι συσκευές μου**.
4. Κάντε κλικ στην επιθυμητή κάρτα της συσκευής, στη συνέχεια, επιλέξτε **Anti-Theft**.
5. Επιλέξτε την λειτουργία που θέλετε να χρησιμοποιήσετε

   Το **Show IP** - εμφανίζει την τελευταία διεύθυνση IP της συσκευής σας.
   Εντοπισμός - εμφανίζει την τοποθεσία της συσκευής σας στο Google Maps.
   Ειδοποίηση - στέλνει μια ειδοποίηση στη συσκευή.
   Lock - κλειδώστε την συσκευή σας και ορίστε ένα κωδικό PIN για το ξεκλείδωμα του.
   Wipe - διαγράψετε όλα τα δεδομένα από το φορητό σας.

   Σημαντικό
   Μετά από την απαλοιφή μιας συσκευής, όλες οι λειτουργίες Anti-Theft παύουν να λειτουργούν.

4.15. USB Immunizer

Η δυνατότητα Autorun ενσωματωμένη στα λειτουργικά συστήματα των Windows είναι ένα πολύ χρήσιμο εργαλείο που επιτρέπει στις συσκευές να εκτελούν αυτόματα ένα αρχείο από πολυμέσα που είναι συνδεδεμένα σε αυτό. Για παράδειγμα, η εγκατάσταση λογισμικού μπορεί να ξεκινήσει αυτόματα όταν τοποθετηθεί ένα CD στη μονάδα οπτικού δίσκου.

Δυστυχώς, αυτή η δυνατότητα μπορεί επίσης να χρησιμοποιηθεί από απειλές για αυτόματη εκκίνηση και διείσδυση της συσκευής σας από επανεγγράψιμα μέσα, όπως μονάδες flash USB και κάρτες μνήμης συνδεδεμένες μέσω συσκευών ανάγνωσης καρτών. Πολυάριθμες επιθέσεις έχουν δημιουργηθεί με βάση το Autorun, τα τελευταία χρόνια.

Με το USB Immunizer μπορείτε να αποτρέψετε οποιαδήποτε NTFS, FAT32 ή FAT διαμορφωμένη μονάδα flash από απειλές αυτόματης εκτέλεσης. Μόλις μια συσκευή USB εμβολιαστεί, οι απειλές δεν μπορούν πλέον να τη

διαμορφώσουν ώστε να εκτελούν μια συγκεκριμένη εφαρμογή όταν η συσκευή είναι συνδεδεμένη σε μια συσκευή με Windows.

Για την ανοσοποίηση μια συσκευή USB:

1. Συνδέστε τη μονάδα flash στη συσκευή σας.
2. Περιηγηθείτε στη συσκευή σας για να εντοπίσετε την αφαιρούμενη συσκευή αποθήκευσης και κάντε δεξί κλικ στο εικονίδιο της.
3. Στο αναδυόμενο μενού, δείξτε στο **Bitdefender** και επιλέξτε **Immunize αυτό το δίσκο**.

Σημείωση

Αν η μονάδα έχει ήδη γίνει immunized, το μήνυμα **Η συσκευή USB προστατεύεται από τα autorun malware** θα εμφανιστεί αντί της επιλογής Immunize.

Για να αποτρέψετε την εκκίνηση απειλών από μη εξομοιωμένες συσκευές USB της συσκευής σας, απενεργοποιήστε τη λειτουργία αυτόματης εκτέλεσης πολυμέσων. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Χρήση της αυτόματης παρακολούθησης ευπάθειας"* (p. 131).

5. ΕΡΓΑΛΕΊΑ

5.1. Προφίλ

Οι καθημερινές δραστηριότητες εργασίας, όπως παρακολουθώντας ταινίες ή παίζοντας παιχνίδια μπορεί να προκαλέσουν επιβράδυνση του συστήματος, ειδικά αν εκτελούνται ταυτόχρονα με τις διαδικασίες ενημέρωσης των Windows και τις εργασίες συντήρησης. Με το Bitdefender, μπορείτε τώρα να επιλέξετε και να εφαρμόσετε το προτιμώμενο προφίλ σας, το οποίο κάνει προσαρμογές του συστήματος που είναι κατάλληλες για την αύξηση της απόδοσης των συγκεκριμένων εγκατεστημένων εφαρμογών.

Το Bitdefender παρέχει τα ακόλουθα προφίλ:

- Προφίλ Εργασίας
- Προφίλ Ταινιών
- Προφίλ Παιχνιδιών
- Προφίλ Δημόσιο Wi-Fi
- Προφίλ Battery Mode

Αν αποφασίσετε να μην χρησιμοποιήσετε τα **Προφίλ**, ένα προεπιλεγμένο προφίλ που ονομάζεται **Τυπικό** είναι ενεργοποιημένο και δεν φέρνει καμία βελτιστοποίηση στο σύστημά σας.

Σύμφωνα με τη δραστηριότητά σας, οι ακόλουθες ρυθμίσεις του προϊόντος εφαρμόζονται όταν ενεργοποιούνται τα προφίλ Εργασία, Ταινία και Παιχνίδι.

- Όλες οι ειδοποιήσεις του Bitdefender και τα αναδυόμενα παράθυρα είναι απενεργοποιημένα.
- Η Αυτόματη Ενημέρωση είναι απενεργοποιημένη.
- Οι προγραμματισμένες σαρώσεις αναβλήθηκαν.
- Η ενότητα Antispam είναι ενεργοποιημένη.
- Ο Σύμβουλος Αναζήτησης είναι απενεργοποιημένος.
- Οι ειδοποιήσεις ειδικών προσφορών είναι απενεργοποιημένες.

Σύμφωνα με τη δραστηριότητά σας, οι ακόλουθες ρυθμίσεις του προϊόντος εφαρμόζονται όταν ενεργοποιούνται τα προφίλ Εργασία, Ταινία και Παιχνίδι.

- Οι Αυτόματες ενημερώσεις των Windows αναβλήθηκαν.
- Οι ειδοποιήσεις των Windows και τα αναδυόμενα παράθυρα είναι απενεργοποιημένα.
- Τα περιττά προγράμματα στο παρασκήνιο αναστέλλονται.
- Τα οπτικά εφέ έχουν προσαρμοστεί για τη βέλτιστη απόδοση.
- Οι εργασίες συντήρησης έχουν αναβληθεί.
- Οι ρυθμίσεις της παροχής ενέργειας έχουν προσαρμοστεί.

Ενώ τρέχει στο προφίλ Δημόσιο Wi-Fi, το Bitdefender Total Security έχει ρυθμιστεί για να ολοκληρώσει αυτόματα τις ακόλουθες ρυθμίσεις του προγράμματος:

- Το Advanced Threat Defense είναι ενεργοποιημένο
- Το Bitdefender Firewall είναι ενεργοποιημένο και οι ακόλουθες ρυθμίσεις εφαρμόζονται στον wireless adapter σας:
  - Stealth mode - ON
  - Τύπος Δικτύου – Δημόσιο
- Οι ακόλουθες ρυθμίσεις από την Online Threat Prevention είναι ενεργοποιημένες:
  - Κρυπτογραφημένη σάρωση Web
  - Προστασία κατά της απάτης
  - Προστασία από phishing

5.1.1. Προφίλ Εργασίας

Εκτελώντας πολλαπλά καθήκοντα στο χώρο εργασίας, όπως αποστολή e-mails, επικοινωνώντας μέσω βίντεο με απομακρυσμένους συναδέλφους σας ή εργασία με εφαρμογές σχεδιασμού μπορεί να επηρεάσουν την απόδοση του συστήματός σας. Το Προφίλ Εργασίας έχει σχεδιαστεί για να σας βοηθήσει να βελτιώσετε την αποδοτικότητα της εργασίας σας, απενεργοποιώντας κάποιες υπηρεσίες του παρασκηνίου σας και εργασίες συντήρησης.

Διαμόρφωση Προφίλ Εργασίας

Για να ρυθμίσετε τις ενέργειες που πρέπει να ληφθούν, ενώ είστε στο Προφίλ Εργασία:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **Προφίλ** , κάντε κλικ στο **Ρυθμίσεις** .
3. Κάντε κλικ στο κουμπί **CONFIGURE** στο χώρο του προφίλ εργασία.
4. Διαλέξτε τις ρυθμίσεις του συστήματος που θα εφαρμοστούν επιλέγοντας τις παρακάτω επιλογές:
   - Ενισχύει την απόδοση σε εφαρμογές εργασίας
   - Βελτιστοποιεί τις ρυθμίσεις του προϊόντος για το προφίλ εργασίας
   - Αναβάλει προγράμματα στο παρασκήνιο και τις εργασίες συντήρησης
   - Αναβάλει τις Αυτόματες ενημερώσεις των Windows
5. Κάντε κλικ στο **Αποθήκευση** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

Χειροκίνητη προσθήκη εφαρμογών στη λίστα του Προφίλ Εργασίας

Εάν το Bitdefender δεν εισέρχεται αυτόματα στο Προφίλ Εργασίας όταν ξεκινήσει μια συγκεκριμένη εφαρμογή εργασίας, μπορείτε να προσθέσετε χειροκίνητα την εφαρμογή στη **Λίστα Εφαρμογών Εργασίας**.

Για να προσθέσετε χειροκίνητα τις εφαρμογές στη Λίστα Εφαρμογών στο Προφίλ Εργασίας:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **Προφίλ** , κάντε κλικ στο **Ρυθμίσεις** .
3. Κάντε κλικ στο κουμπί **CONFIGURE** στο χώρο του προφίλ εργασία.
4. Στο παράθυρο **Ρυθμίσεις προφίλ εργασίας**, πατήστε**Λίστα Εφαρμογών**.
5. Κάντε κλικ στο **ΠΡΟΣΘΗΚΗ**.

   Εμφανίζεται ένα νέο παράθυρο. Περιηγηθείτε στο εκτελέσιμο αρχείο της εφαρμογής, επιλέξτε το και κάντε κλικ στο **OK** για να το προσθέσετε στη λίστα.

5.1.2. Προφίλ Ταινιών

Για την εμφάνιση υψηλής ποιότητας βίντεο, όπως ταινίες υψηλής ευκρίνειας, απαιτούνται σημαντικοί πόροι του συστήματος. Το Προφίλ Ταινιών προσαρμόζει τις ρυθμίσεις του συστήματος και του προϊόντος ώστε να μπορείτε να απολαύσετε μια συνεχή και ομαλή εμπειρία ταινιών.

Διαμόρφωση Προφίλ Ταινιών

Για να ρυθμίσετε τις ενέργειες που πρέπει να ληφθούν, ενώ είστε στο Προφίλ Ταινιών:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **Προφίλ** , κάντε κλικ στο **Ρυθμίσεις** .
3. Κάντε κλικ στο κουμπί **CONFIGURE** στο χώρο του προφίλ Ταινία.
4. Διαλέξτε τις ρυθμίσεις του συστήματος που θα εφαρμοστούν επιλέγοντας τις παρακάτω επιλογές:
   - Ενισχύει την απόδοση των προγραμμάτων αναπαραγωγής βίντεο
   - Βελτιστοποιεί τις ρυθμίσεις του προϊόντος για το προφίλ Ταινίες
   - Αναβάλει προγράμματα στο παρασκήνιο και τις εργασίες συντήρησης
   - Αναβάλει τις Αυτόματες ενημερώσεις των Windows
   - Προσαρμόζει τις ρυθμίσεις παροχής ενέργειας για Ταινίες
5. Κάντε κλικ στο **Αποθήκευση** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

Χειροκίνητη προσθήκη προγραμμάτων αναπαραγωγής βίντεο για την λίστα Προφίλ Ταινιών

Εάν το Bitdefender δεν εισέρχεται αυτόματα στο Προφίλ Ταινιών όταν ξεκινήσετε μια συγκεκριμένη εφαρμογή αναπαραγωγής βίντεο, μπορείτε να προσθέσετε χειροκίνητα την εφαρμογή στη **Λίστα Προγραμμάτων Αναπαραγωγής**.

Για να προσθέσετε χειροκίνητα προγράμματα αναπαραγωγής βίντεο στη λίστα Προγράμματα Αναπαραγωγής στο Προφίλ Ταινιών:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.

2. Στην καρτέλα **Προφίλ** , κάντε κλικ στο **Ρυθμίσεις** .
3. Κάντε κλικ στο κουμπί **CONFIGURE** στο χώρο του προφίλ Ταινία.
4. Στο παράθυρο **Ρυθμίσεις Προφίλ Ταινιών**, πατήστε **Λίστα Players**.
5. Κάντε κλικ στο **ΠΡΟΣΘΗΚΗ**.

   Εμφανίζεται ένα νέο παράθυρο. Περιηγηθείτε στο εκτελέσιμο αρχείο της εφαρμογής, επιλέξτε το και κάντε κλικ στο **OK** για να το προσθέσετε στη λίστα.

5.1.3. Προφίλ Παιχνιδιών

Η απόλαυση μιας αδιάλειπτης εμπειρίας παιχνιδιού έχει να κάνει με τη μείωση διακοπών συστήματος και την μείωση επιβράδυνση αυτού. Με τη χρήση συστημάτων αναγνώρισης μαζί με μια λίστα γνωστών παιχνιδιών, το Bitdefender μπορεί να ανιχνεύσει αυτόματα τη λειτουργία παιχνιδιού και να βελτιστοποιήσει τους πόρους του συστήματος σας έτσι ώστε να μπορείτε να απολαύσετε το διάλειμμα του παιχνιδιού σας.

Διαμόρφωση Προφίλ Παιχνιδιών

Για να ρυθμίσετε τις ενέργειες που πρέπει να ληφθούν, ενώ είστε στο Προφίλ Παιχνίδι:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **Προφίλ** , κάντε κλικ στο **Ρυθμίσεις** .
3. Κάντε κλικ στο κουμπί **Διαμόρφωση** από την περιοχή προφίλ παιχνιδιού.
4. Διαλέξτε τις ρυθμίσεις του συστήματος που θα εφαρμοστούν επιλέγοντας τις παρακάτω επιλογές:
   - Ενισχύει την απόδοση σε παιχνίδια
   - Βελτιστοποίηση ρυθμίσεων προϊόντος για Προφίλ Παιχνίδι
   - Αναβάλει προγράμματα στο παρασκήνιο και τις εργασίες συντήρησης
   - Αναβάλει τις Αυτόματες ενημερώσεις των Windows
   - Προσαρμογή ρυθμίσεων παροχής ενέργειας για παιχνίδια
5. Κάντε κλικ στο **Αποθήκευση** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

Χειροκίνητη προσθήκη παιχνιδιών στη λίστα Παιχνιδιών

Εάν το Bitdefender δεν εισέρχεται αυτόματα στο Προφίλ Παιχνιδιών όταν ξεκινήσετε ένα συγκεκριμένο παιχνίδι ή μία εφαρμογή, μπορείτε να προσθέσετε χειροκίνητα την εφαρμογή στη **Λίστα Παιχνιδιών**.

Για να προσθέσετε χειροκίνητα παιχνίδια στη λίστα Παιχνιδιών στο Προφίλ Παιχνιδιών:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **Προφίλ** , κάντε κλικ στο **Ρυθμίσεις** .
3. Κάντε κλικ στο κουμπί **CONFIGURE** στο χώρο του προφίλ Παιχνίδι.
4. Στο παράθυρο **Ρυθμίσεις Προφίλ Παιχνιδιών**, πατήστε **Λίστα παιχνιδιών**.
5. Κάντε κλικ στο **ΠΡΟΣΘΗΚΗ**.

   Εμφανίζεται ένα νέο παράθυρο. Περιηγηθείτε στο εκτελέσιμο αρχείο του παιχνιδιού, επιλέξτε το και κάντε κλικ στο **OK** για να το προσθέσετε στη λίστα.

5.1.4. Προφίλ Δημόσιο Wi-Fi

Αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, πληκτρολογήσει ευαίσθητων δεδομένων ή online αγορές, ενώ συνδέεστε με μη ασφαλή ασύρματα δίκτυα μπορούν να εκθέσουν τα προσωπικά σας δεδομένα σε κίνδυνο. Το προφίλ Δημόσιο Wi-Fi προσαρμόζει τις ρυθμίσεις του προϊόντος για να σας δώσει τη δυνατότητα να κάνετε τις πληρωμές σε online σύνδεση και να χρησιμοποιείτε ευαίσθητες πληροφορίες σε ένα προστατευμένο περιβάλλον.

Διαμόρφωση του προφίλ Δημόσιο Wifi

Για να ρυθμίσετε το Bitdefender για να εφαρμόζει τις ρυθμίσεις του προϊόντος, ενώ συνδέεστε με ένα μη ασφαλές ασύρματο δίκτυο:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **Προφίλ** , κάντε κλικ στο **Ρυθμίσεις** .
3. Κάντε κλικ στο κουμπί **CONFIGURE** στο χώρο του προφίλ Δημόσιο Wi-Fi.

4. Αφήστε το **Προσαρμόζει τις ρυθμίσεις του προϊόντος για την ενίσχυση της προστασίας όταν είναι συνδεδεμένο σε ένα ανασφαλή δημόσιο Wi-Fi δίκτυο** ενεργοποιημένο.
5. Κάντε κλικ στο **Αποθήκευση**.

5.1.5. Προφίλ Battery Mode

Το προφίλ λειτουργία με μπαταρία είναι ειδικά σχεδιασμένο για χρήστες φορητού υπολογιστη και tablet. Ο σκοπός του είναι η ελαχιστοποίηση τόσο του συστήματος οσο και του Bitdefender σχετικά με τις επιπτώσεις στην κατανάλωση ενέργειας όταν το επίπεδο φόρτισης της μπαταρίας είναι χαμηλότερο από ό,τι επιλέξετε.

Διαμόρφωση Λειτουργίας με Μπαταρία

Για να διαμορφώσετε το προφίλ Λειτουργία με μπαταρία:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **Προφίλ** , κάντε κλικ στο **Ρυθμίσεις** .
3. Κάντε κλικ στο κουμπί **Διαμόρφωση** από την περιοχή προφίλ λειτουργίας μπαταρίας.
4. Διαλέξτε τις ρυθμίσεις του συστήματος που θα εφαρμοστούν επιλέγοντας τις παρακάτω επιλογές:
   - Βελτιστοποίηση των ρυθμίσεων του προϊόντος για τη Λειτουργία Μπαταρίας.
   - Αναβάλει προγράμματα στο παρασκήνιο και τις εργασίες συντήρησης.
   - Αναβάλει τις Αυτόματες ενημερώσεις των Windows.
   - Προσαρμογή ρυθμίσεων για λειτουργία μπαταρίας.
   - Απενεργοποιεί τις εξωτερικές συσκευές και τις θύρες δικτύου.
5. Κάντε κλικ στο **Αποθήκευση** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

Πληκτρολογήστε μια έγκυρη τιμή στο πλαίσιο ή επιλέξτε με το βέλος για να καθορίσετε πότε το σύστημα θα πρέπει να αρχίσει να λειτουργεί σε κατάσταση Battery mode. Από προεπιλογή, η λειτουργία ενεργοποιείται όταν το επίπεδο φόρτισης της μπαταρίας πέσει κάτω από το 30%.

Οι ακόλουθες ρυθμίσεις εφαρμόζονται όταν το Bitdefender βρίσκεται σε προφίλ λειτουργίας με μπαταρία:

- Η Αυτόματη Ενημέρωση του Bitdefender αναβλήθηκε.
- Οι προγραμματισμένες σαρώσεις αναβλήθηκαν.

Το Bitdefender ανιχνεύει όταν ο φορητός υπολιγιστής σας αλλάξει σε τροφοδοσία μέσω μπαταρίας και με βάση το επίπεδο φόρτισης της μπαταρίας εισέρχεται αυτόματα σε λειτουργία μπαταρίας. Παρομοίως, το Bitdefender εξέρχεται αυτόματα από τη Λειτουργία της Μπαταρίας όταν ανιχνεύει ο φορητός υπολογιστής δεν τροφοδοτείται πλέον με μπαταρία.

5.1.6. Βελτιστοποίηση σε πραγματικό χρόνο

Το Real-Time Optimization του Bitdefender είναι ένα plugin που βελτιώνει σιωπηλά στο παρασκήνιο την απόδοση του συστήματός σας, βεβαιώνοντας ότι δεν διακόπτεστε ενώ βρίσκεστε σε profile mode. Ανάλογα με το φορτίο της CPU, το plugin παρακολουθεί όλες τις διαδικασίες, με έμφαση σε εκείνες που λαμβάνουν ένα υψηλότερο φορτίο, για να τις προσαρμόσει στις ανάγκες σας.

Για να ενεργοποιήσετε ή να απενεργοποιήσετε την βελτιστοποίηση σε πραγματικό χρόνο:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Στην καρτέλα **Προφίλ** , κάντε κλικ στο **Ρυθμίσεις** .
3. Πραγματοποιήστε κύλιση προς τα κάτω μέχρι να δείτε την επιλογή βελτιστοποίησης πραγματικού χρόνου και, στη συνέχεια, χρησιμοποιήστε τον αντίστοιχο διακόπτη για να την ενεργοποιήσετε ή να την απενεργοποιήσετε.

5.2. OneClick Optimizer

Ζητήματα όπως αστοχίες σκληρού δίσκου, εναπομείναντα αρχεία μητρώου και ιστορικό προγράμματος περιήγησης, ενδέχεται να επιβραδύνουν την εργασία σας, κάτι που μπορεί να σας ενοχλήσει. Όλα αυτά μπορούν τώρα να διορθωθούν με ένα μόνο κλικ.

OneClick Optimizer σας επιτρέπει να αναγνωρίσετε και να αφαιρέσετε άχρηστα αρχεία εκτελώντας ταυτόχρονα πολλαπλές εργασίες καθαρισμού.

Για να ξεκινήσετε τη διαδικασία OneClick Optimizer:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Κάντε κλικ στο κουμπί **Βελτιστοποίηση**.
   a. **Γίνεται Ανάλυση του**

      Περιμένετε το Bitdefender για να ολοκληρώσει την αναζήτηση για θέματα του συστήματος.

      - Καθαρισμός δίσκου - εντοπίζει περιττά μεγάλα αρχεία και φακέλους.
      - Η Registry Cleanup εντοπίζει άκυρες ή παλίες αναφορές στο μητρώο των Windows.
      - Η Privacy Cleanup - εντοπίζει τα προσωρινά αρχεία του Internet και τα cookies, καθώς και την προσωρινή μνήμη του προγράμματος περιήγησης.

      Εμφανίζεται ο αριθμός των θεμάτων που βρέθηκαν. Κάντε κλικ στο **View details** σύνδεσμο και επανεξετάσετε πριν προχωρήσετε με την διαδικασία καθαρισμού. Κάντε κλικ στο **Optimize** για να συνεχίσετε.

   b. **Βελτιστοποίηση**

      Περιμένετε το Bitdefender για να ολοκληρώσει τη βελτιστοποίηση του συστήματός σας.

   c. **Ζητήματα**

      Εδώ μπορείτε να δείτε το αποτέλεσμα της λειτουργίας.

      Εάν θέλετε ολοκληρωμένες πληροφορίες σχετικά με τη διαδικασία βελτιστοποίησης, κάντε κλικ στο κουμπί **Προβολή λεπτομερούς αναφοράς** .

5.3. ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

Μόνιμη διαγραφή αρχείων

Όταν διαγράφετε ένα αρχείο, δεν μπορείτε πλέον να έχετε πρόσβαση σε αυτό με τα συνήθη μέσα. Ωστόσο, το αρχείο εξακολουθεί να είναι αποθηκευμένο στο σκληρό δίσκο έως ότου να αντικατασταθεί κατά την αντιγραφή νέων αρχείων.

Το Bitdefender File Shredder σας βοηθά να διαγράψετε οριστικά τα δεδομένα αφαιρώντας τα από το σκληρό σας δίσκο.

Μπορείτε να τεμαχίσετε γρήγορα αρχεία ή φακέλους από τη συσκευή σας χρησιμοποιώντας το μενού με τα συμφραζόμενα των Windows ακολουθώντας αυτά τα βήματα:

1. Κάντε δεξί κλικ στο αρχείο ή στο φάκελο που θέλετε να διαγράψετε οριστικά.
2. Επιλέξτε το **Bitdefender** > **File Shredder** στο μενού επιλογών που εμφανίζεται.
3. Κάντε κλικ στο **Διαγραφή μόνιμα** και, στη συνέχεια, επιβεβαιώστε ότι θέλετε να συνεχίσετε τη διαδικασία.

   Περιμένετε να τελειώσει το Bitdefender την καταστροφή των αρχείων.
4. Τα αποτελέσματα εμφανίζονται. Κάντε κλικ στο **Τέλος** για έξοδο από τον οδηγό.

Εναλλακτικά, μπορείτε να καταστρέφετε αρχεία από την οθόνη του Bitdefender με τα ακόλουθα βήματα:

1. Πατήστε **Βοηθητικά προγράμματα** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **Προστασία δεδομένων** , κάντε κλικ στο **Τεμαχιστής αρχείων** .
3. Ακολουθήστε τον οδηγό File Shredder:

   a. Κάντε κλικ στο κουμπί **Προσθήκη φακέλων** για να προσθέσετε τα αρχεία ή τους φακέλους που θέλετε να καταργήσετε οριστικά.

      Εναλλακτικά, μπορείτε να σύρετε τα αρχεία ή τους φακέλους σε αυτό το παράθυρο.

   b. Κάντε κλικ στο **Διαγραφή μόνιμα** και, στη συνέχεια, επιβεβαιώστε ότι θέλετε να συνεχίσετε τη διαδικασία.

      Περιμένετε να τελειώσει το Bitdefender την καταστροφή των αρχείων.

   c. **Συγκεντρωτικά αποτελέσματα**

      Τα αποτελέσματα εμφανίζονται. Κάντε κλικ στο **Τέλος** για έξοδο από τον οδηγό.

6. ΑΝΤΙΜΕΤΏΠΙΣΗ ΠΡΟΒΛΗΜΆΤΩΝ

6.1. Επίλυση κοινών ζητημάτων

Το κεφάλαιο αυτό παρουσιάζει κάποια προβλήματα που μπορεί να αντιμετωπίσετε κατά τη χρήση του Bitdefender και σας παρέχει πιθανές λύσεις σε αυτά τα προβλήματα. Τα περισσότερα από αυτά τα προβλήματα μπορούν να επιλυθούν με την κατάλληλη διαμόρφωση των ρυθμίσεων του προϊόντος.

Εάν δεν μπορείτε να βρείτε το πρόβλημά σας εδώ, ή εάν οι λύσεις που παρουσιάζονται δεν το λύσουν, μπορείτε να επικοινωνήσετε με τους αντιπροσώπους τεχνικής υποστήριξης της Bitdefender, όπως παρουσιάζονται στο κεφάλαιο "*Ζητήσετε βοήθεια*" (p. 345).

6.1.1. Το σύστημα μου φαίνεται να είναι αργό

Συνήθως, μετά την εγκατάσταση ενός λογισμικού ασφαλείας, μπορεί να εμφανιστεί μια μικρή επιβράδυνση του συστήματος, το οποίο σε ένα βαθμό είναι φυσιολογικό.

Αν παρατηρήσετε μια σημαντική επιβράδυνση, το θέμα αυτό μπορεί να εμφανιστεί για τους εξής λόγους:

- **Το Bitdefender δεν είναι το μόνο πρόγραμμα ασφαλείας που είναι εγκατεστημένο στο σύστημα.**

  Το Bitdefender ανίχνευσε και αφαίρεσε τα προγράμματα ασφαλείας που βρέθηκαν κατά τη διάρκεια της εγκατάστασης. Συνιστάται να αφαιρέσετε οποιοδήποτε άλλο πρόγραμμα προστασίας από ιούς που μπορεί να χρησιμοποιούσατε πριν από την εγκατάσταση του Bitdefender. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Πώς μπορώ να καταργήσω τις άλλες λύσεις ασφάλειας;"* (p. 82).

- **Οι Ελάχιστες Απαιτήσεις του Συστήματος για την εκτέλεση του Bitdefender δεν πληρούνται.**

  Εάν το μηχάνημά σας δεν πληροί τις απαιτήσεις συστήματος, η συσκευή θα είναι αργή, ειδικά όταν εκτελούνται πολλές εφαρμογές ταυτόχρονα. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Απαιτήσεις συστήματος"* (p. 3).

- **Έχετε εγκαταστήσει εφαρμογές που δεν χρησιμοποιείτε** .

  Οποιαδήποτε συσκευή διαθέτει προγράμματα ή εφαρμογές που δεν χρησιμοποιείτε. Και πολλά ανεπιθύμητα προγράμματα που εκτελούνται στο παρασκήνιο πιάνουν χώρο στο δίσκο και τη μνήμη. Εάν δεν χρησιμοποιείτε ένα πρόγραμμα, απεγκαταστήστε το. Αυτό ισχύει επίσης και για οποιοδήποτε άλλο προ-εγκατεστημένο λογισμικό ή δοκιμαστική εφαρμογή που ξεχάσατε να αφαιρέσετε.

  Σημαντικό
  Αν υποπτεύεστε ένα πρόγραμμα ή μια εφαρμογή να είναι ένα ουσιαστικό μέρος του λειτουργικού σας συστήματος, μην το αφαιρέσετε και επικοινωνήστε με την Εξυπηρέτηση Πελατών του Bitdefender για βοήθεια.

- **Το σύστημά σας μπορεί να έχει προσβληθεί**.

  Η ταχύτητα του συστήματός σας και γενικά η συμπεριφορά του μπορεί επίσης να επηρεαστεί από κακόβουλο λογισμικό. Το λογισμικό υποκλοπής spyware, κακόβουλο λογισμικό, Trojans και adware επηρεάζει την απόδοση της συσκευής σας. Σιγουρευτείτε ότι σαρώνετε το σύστημά σας σε τακτά χρονικά διαστήματα, τουλάχιστον μία φορά την εβδομάδα. Συνιστάται να χρησιμοποιήσετε το Bitdefender System Scan, γιατί

σαρώνει για όλους τους τύπους κακόβουλου λογισμικού που απειλούν την ασφάλεια του συστήματός σας.

Για να ξεκινήσετε τη σάρωση του συστήματος:

1. a
   Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στο παράθυρο **Σάρωση** , κάντε κλικ στο **Εκτέλεση σάρωσης** δίπλα στο **Σάρωση συστήματος** .
4. Ακολουθήστε τα βήματα του οδηγού.

6.1.2. Η Σάρωση δεν ξεκινάει

Αυτού του είδους το ζήτημα μπορεί να έχει δύο κύριες αιτίες:

- **Μια προηγούμενη εγκατάσταση του Bitdefender η οποία δεν είχε αφαιρεθεί εντελώς ή μια ελαττωματική εγκατάσταση του Bitdefender**.

  Σε αυτήν την περίπτωση επανεγκαταστήστε το Bitdefender:

  - Στα **Windows 7**:
    1. Κάντε κλικ στο **Εναρξη**, πηγαίνετε στο **Πίνακας Ελέγχου** και κάντε διπλό κλικ στο **Προγράμματα και Δυνατότητες** .
    2. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
    3. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ** στο παράθυρο που εμφανίζεται.
    4. Περιμένετε την ολοκλήρωση της διαδικασίας επανεγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.
  - Στα **Windows 8 και στα Windows 8.1**:
    1. Από την οθόνη Έναρξης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Πίνακας Ελέγχου" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του.
    2. Κάντε κλικ στο **Κατάργηση εγκατάστασης προγράμματος** ή στο **Προγράμματα και δυνατότητες** .

3. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
4. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ** στο παράθυρο που εμφανίζεται.
5. Περιμένετε την ολοκλήρωση της διαδικασίας επανεγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

- Στα **Windows 10**:

1. Κάντε κλικ στο **Εκκίνηση**και στη συνέχεια, κάντε κλικ στην επιλογή Ρυθμίσεις.
2. Κάντε κλικ στο εικονίδιο **Σύστημα** στην περιοχή Ρυθμίσεις, στη συνέχεια, επιλέξτε **Εγκατεστημένες εφαρμογές**.
3. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
4. Κάντε κλικ στο **Απεγκατάσταση** ξανά για να επιβεβαιώσετε την επιλογή σας.
5. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ** στο παράθυρο που εμφανίζεται.
6. Περιμένετε την ολοκλήρωση της διαδικασίας επανεγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

Σημείωση

Ακολουθώντας αυτήν τη διαδικασία επανεγκατάστασης, οι προσαρμοσμένες ρυθμίσεις αποθηκεύονται και διατίθενται στο νέο εγκατεστημένο προϊόν. Άλλες ρυθμίσεις μπορεί να επανέλθουν στην προεπιλεγμένη διαμόρφωσή τους.

- **Το Bitdefender δεν είναι η μόνη λύση ασφαλείας που εγκατεστημένη στο σύστημά σας**.

Στην περίπτωση αυτή:

1. Αφαιρέστε την άλλη λύση ασφαλείας. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Πώς μπορώ να καταργήσω τις άλλες λύσεις ασφάλειας;"* (p. 82).
2. Επανεγκατάσταση του Bitdefender:

   - Στα **Windows 7**:

a. Κάντε κλικ στο **Εναρξη**, πηγαίνετε στο **Πίνακας Ελέγχου** και κάντε διπλό κλικ στο **Προγράμματα και Δυνατότητες** .

b. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.

c. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ** στο παράθυρο που εμφανίζεται.

d. Περιμένετε την ολοκλήρωση της διαδικασίας επανεγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

- Στα **Windows 8 και στα Windows 8.1**:

a. Από την οθόνη Έναρξης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Πίνακας Ελέγχου" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του.

b. Κάντε κλικ στο **Κατάργηση εγκατάστασης προγράμματος** ή στο **Προγράμματα και δυνατότητες** .

c. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.

d. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ** στο παράθυρο που εμφανίζεται.

e. Περιμένετε την ολοκλήρωση της διαδικασίας επανεγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

- Στα **Windows 10**:

a. Κάντε κλικ στο **Εκκίνηση**και στη συνέχεια, κάντε κλικ στην επιλογή Ρυθμίσεις.

b. Κάντε κλικ στο εικονίδιο **Σύστημα** στην περιοχή Ρυθμίσεις, στη συνέχεια, επιλέξτε **Εγκατεστημένες εφαρμογές**.

c. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.

d. Κάντε κλικ στο **Απεγκατάσταση** ξανά για να επιβεβαιώσετε την επιλογή σας.

e. Κάντε κλικ στο κουμπί **ΕΠΑΝΕΓΚΑΤΑΣΤΑΣΗ** στο παράθυρο που εμφανίζεται.

f. Περιμένετε την ολοκλήρωση της διαδικασίας επανεγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

Σημείωση
Ακολουθώντας αυτήν τη διαδικασία επανεγκατάστασης, οι προσαρμοσμένες ρυθμίσεις αποθηκεύονται και διατίθενται στο νέο εγκατεστημένο προϊόν. Άλλες ρυθμίσεις μπορεί να επανέλθουν στην προεπιλεγμένη διαμόρφωσή τους.

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήστε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα *"Ζητήσετε βοήθεια"* (p. 345).

6.1.3. Δεν μπορώ πλέον να χρησιμοποιήσω μια εφαρμογή

Αυτό το ζήτημα προκύπτει όταν προσπαθείτε να χρησιμοποιήσετε ένα πρόγραμμα το οποίο λειτουργούσε κανονικά πριν εγκαταστήσετε το Bitdefender.

Μετά την εγκατάσταση του Bitdefender ενδέχεται να αντιμετωπίσετε μία από αυτές τις καταστάσεις:

- Θα μπορούσατε να λάβετε ένα μήνυμα από το Bitdefender ότι το πρόγραμμα προσπαθεί να προβεί σε τροποποίηση του συστήματος.
- Θα μπορούσατε να λάβετε ένα μήνυμα λάθους από το πρόγραμμα που προσπαθείτε να χρησιμοποιήσετε.

Αυτό το status εμφανίζεται όταν το Advanced Threat Defense ανιχνεύει λανθασμένα κάποιες εφαρμογές ως κακόβουλες.

Το Advanced Threat Defense είναι μια λειτουργία του Bitdefender που παρακολουθεί συνεχώς τις εφαρμογές που τρέχουν στο σύστημά σας και αναφέρει εκείνα που ενδεχομένως έχουν κακόβουλη συμπεριφορά. Δεδομένου ότι αυτή η λειτουργία βασίζεται σε ένα heuristic σύστημα, μπορεί να υπάρξουν περιπτώσεις κατά τις οποίες οι νόμιμες εφαρμογές αναφέρονται από το Advanced Threat Defense.

Σε αυτήν την περίπτωση, μπορείτε να εξαιρέσετε την αντίστοιχη εφαρμογή από το να παρακολουθείται από το Advanced Threat Defense.

Για να προσθέσετε την εφαρμογή στη λίστα εξαιρέσεων:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.

2. Στην **ADVANCED THREAT DEFENSE** οθόνη, επιλέξτε **Άνοιγμα**.
3. Στο παράθυρο **Ρυθμίσεις** , κάντε κλικ στην επιλογή **Διαχείριση εξαιρέσεων** .
4. Κάντε κλικ στο **+ Προσθήκη εξαίρεσης** .
5. Εισαγάγετε τη διαδρομή του εκτελέσιμου που θέλετε εκτός από τη σάρωση στο αντίστοιχο πεδίο.

   Εναλλακτικά, μπορείτε να πλοηγηθείτε στο εκτελέσιμο κάνοντας κλικ στο κουμπί περιήγησης στη δεξιά πλευρά της διεπαφής, επιλέξτε το και κάντε κλικ στο **OK** .
6. Ενεργοποιήστε το διακόπτη δίπλα στο **Advanced Threat Defense** .
7. Κάντε κλικ στο **Αποθήκευση**.

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήστε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα "*Ζητήσετε βοήθεια*" (p. 345).

6.1.4. Τι να κάνετε όταν το Bitdefender αποκλείει έναν ιστότοπο, ένα domain, μια διεύθυνση IP ή μια εφαρμογή στο διαδίκτυο που είναι ασφαλής

Το Bitdefender προσφέρει μια ασφαλή εμπειρία περιήγησης στο Web φιλτράροντας όλες τις κινήσεις στο Δίκτυο και εμποδίζοντας κάθε κακόβουλο περιεχόμενο. Ωστόσο, είναι πιθανό το Bitdefender να θεωρήσει ότι μια ασφαλής σελίδα ή ηλεκτρονική αίτηση δεν είναι ασφαλή, γεγονός που θα προκαλέσει τον λανθασμένο αποκλεισμό της ιστοσελίδας από το Bitdefender HTTP traffic.

Σε περίπτωση που η ίδια σελίδα, το domain, η IP διεύθυνση ή μια online εφαρμογή αποκλειστεί, μπορείτε να τις προσθέσετε σε μια εγκεκριμένη λίστα (whitelist), ούτως ώστε να μην σαρώνεται από τις Bitdefender μηχανές, εξασφαλίζοντας έτσι μια ομαλή εμπειρία περιήγησης στο web.

Για να προσθέσετε μία website από τις **Εξαιρέσεις**:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ONLINE THREAT PREVENTION**, επιλέξτε **Ρυθμίσεις**.
3. Κάντε κλικ στο **Διαχείριση εξαιρέσεων** .
4. Κάντε κλικ στο **+ Προσθήκη εξαίρεσης** .

5. Πληκτρολογήστε στο αντίστοιχο πεδίο το όνομα του ιστότοπου, το όνομα του τομέα ή τη διεύθυνση IP που θέλετε να προσθέσετε στις εξαιρέσεις.
6. Κάντε κλικ στον διακόπτη δίπλα στο **Online Threat Prevention** .
7. Κάντε κλικ στο **Αποθήκευση** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

Μόνο οι ιστότοποι, domains, οι διευθύνσεις IP και οι εφαρμογές που εμπιστεύεστε πλήρως πρέπει να προστεθούν σε αυτήν τη λίστα. Αυτά θα εξαιρεθούν από τον έλεγχο από τις ακόλουθες μηχανές: απειλές, phishing και απάτη.

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήστε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα "*Ζητήσετε βοήθεια*" (p. 345).

6.1.5. Δεν μπορώ να συνδεθώ στο Διαδίκτυο

Μπορεί να παρατηρήσετε ότι ένα πρόγραμμα ή ένας περιηγητής ιστού δεν μπορεί πλέον να συνδεθεί με τις υπηρεσίες Internet ή δεν έχει πρόσβαση στο δίκτυο μετά την εγκατάσταση του Bitdefender.

Σε αυτή την περίπτωση, η καλύτερη λύση είναι να διαμορφώσετε Bitdefender να επιτρέπει αυτόματα συνδέσεις προς και από την αντίστοιχη εφαρμογή λογισμικού:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **FIREWALL**, πατήστε **Ρυθμίσεις**.
3. Στο παράθυρο **Κανόνες**, πατήστε **Προσθήκη κανόνα**.
4. Ένα νέο παράθυρο εμφανίζεται, όπου μπορείτε να προσθέσετε τις λεπτομέρειες. Βεβαιωθείτε ότι έχετε επιλέξει όλους τους διαθέσιμους τύπους δικτύου και στην ενότητα **Άδεια** επιλέξτε **Να επιτρέπεται**.

Κλείστε το Bitdefender, ανοίξτε την εφαρμογή λογισμικού και προσπαθήστε ξανά να συνδεθείτε στο Διαδίκτυο.

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήστε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα "*Ζητήσετε βοήθεια*" (p. 345).

6.1.6. Δεν μπορώ να αποκτήσω πρόσβαση σε μια συσκευή στο δίκτυό μου

Ανάλογα με το δίκτυο στο οποίο είστε συνδεδεμένοι, το τείχος προστασίας Bitdefender ενδέχεται να αποκλείσει τη σύνδεση μεταξύ του συστήματός σας και μιας άλλης συσκευής (όπως άλλος υπολογιστής ή εκτυπωτής). Ως αποτέλεσμα, δεν μπορείτε πλέον να μοιραστείτε ή να εκτυπώσετε αρχεία.

Σε αυτή την περίπτωση, η καλύτερη λύση είναι να ρυθμίσετε ως εξής το Bitdefender να επιτρέπει αυτόματα τις συνδέσεις προς και από την αντίστοιχη συσκευή:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **FIREWALL**, πατήστε **Ρυθμίσεις**.
3. Στο παράθυρο **Κανόνες**, πατήστε **Προσθήκη κανόνα**.
4. Ενεργοποιήστε την επιλογή **Εφαρμογή αυτού του κανόνα σε όλες τις εφαρμογές** .
5. Κάντε κλικ στο κουμπί **Σύνθετες ρυθμίσεις** .
6. Στο πλαίσιο **Προσαρμοσμένη απομακρυσμένη διεύθυνση** , πληκτρολογήστε τη διεύθυνση IP του υπολογιστή ή του εκτυπωτή στον οποίο θέλετε να έχετε απεριόριστη πρόσβαση.

Εάν εξακολουθείτε να μην μπορείτε να συνδεθείτε με τη συσκευή, το ζήτημα μπορεί να μην προκαλείται από το Bitdefender.

Ελέγξτε για άλλες πιθανές αιτίες, όπως οι ακόλουθες:

- Το τείχος προστασίας στην άλλη συσκευή ενδέχεται να αποκλείσει την κοινή χρήση αρχείων και εκτυπωτών με τον υπολογιστή σας.
  - Εάν χρησιμοποιείται το τείχος προστασίας των Windows, μπορεί να ρυθμιστεί ώστε να επιτρέπει κοινή χρήση αρχείων και εκτυπωτών ως εξής:
    - Στα **Windows 7**:
      1. Κάντε κλικ στο **Έναρξη**, μεταβείτε στον **Πίνακα Ελέγχου** και επιλέξτε **Σύστημα και Ασφάλεια**.
      2. Πηγαίνετε στο **Windows Firewall**, και κάντε κλικ στο **Allow a program through Windows Firewall**.

3. Επιλέξτε το **Κοινή χρήση αρχείων και εκτυπωτών** Κουτί επιλογής.

- Στα **Windows 8 και στα Windows 8.1**:

  1. Από την οθόνη Έναρξης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Πίνακας Ελέγχου" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του.
  2. Κάντε κλικ στο **Σύστημα και Ασφαλεία** , πηγαίνετε στο **Τείχος προστασίας των Windows** και επιλέξτε **Να επιτρέπεται μια εφαρμογή μέσω του Τείχους προστασίας των Windows**.
  3. Επιλέξτε το **Κοινή χρήση αρχείων και εκτυπωτών** κουτί επιλογής, και κάντε κλικ στο **OK**.

- Στα **Windows 10**:

  1. Πληκτρολογήστε "Allow an app through Windows Firewall" στο πλαίσιο αναζήτησης από τη γραμμή εργασιών και κάντε κλικ στο εικονίδιο του.
  2. Κάντε κλικ στο **Αλλαγή ρυθμίσεων** .
  3. Στη **Allowed apps and features** λίστα επιλέξτε το **File and Printer Sharing**, και κάντε κλικ στο **OK**.

- Αν χρησιμοποιείται άλλο firewall πρόγραμμα, ανατρέξτε στην τεκμηρίωση ή το αρχείο βοήθειας του.

- Γενικοί όροι που μπορούν να αποτρέψουν τη χρήση ή τη σύνδεση με τον κοινόχρηστο εκτυπωτή:

  - Μπορεί να χρειαστεί να συνδεθεί σε ένα λογαριασμό ως διαχειριστής των Windows για να αποκτήσετε πρόσβαση στον κοινόχρηστο εκτυπωτή.
  - Ορίζονται δικαιώματα για τον κοινόχρηστο εκτυπωτή ώστε να επιτρέπεται η πρόσβαση μόνο σε συγκεκριμένη συσκευή και χρήστες. Εάν μοιράζεστε τον εκτυπωτή σας, ελέγξτε τα δικαιώματα που έχουν οριστεί για τον εκτυπωτή για να δείτε εάν επιτρέπεται στον χρήστη η άλλη συσκευή να έχει πρόσβαση στον εκτυπωτή. Εάν προσπαθείτε να συνδεθείτε σε έναν κοινόχρηστο εκτυπωτή, επικοινωνήστε με τον χρήστη στην άλλη συσκευή εάν έχετε άδεια σύνδεσης με τον εκτυπωτή.

- Ο εκτυπωτής που είναι συνδεδεμένος στη συσκευή σας ή σε κάποιο άλλο δεν είναι κοινόχρηστος.
- Ο κοινόχρηστος εκτυπωτής δεν προστίθεται στη συσκευή.

Σημείωση
Για να μάθετε πώς να διαχειρίζεστε κοινή χρήση του εκτυπωτή (κοινή χρήση ενός εκτυπωτή, ρύθμιση ή κατάργηση δικαιωμάτων για έναν εκτυπωτή, σύνδεση σε έναν εκτυπωτή δικτύου ή σε έναν κοινόχρηστο εκτυπωτή), μεταβείτε στη Βοήθεια και υποστήριξη των Windows (στο μενού Έναρξη , κάντε κλικ στο **Βοήθεια και υποστήριξη**).

- Η πρόσβαση σε έναν εκτυπωτή δικτύου μπορεί να περιορίζεται μόνο σε συγκεκριμένες συσκευές ή χρήστες. Θα πρέπει να ελέγξετε με το διαχειριστή του δικτύου, ότι έχετε άδεια για να συνδεθείτε με αυτόν τον εκτυπωτή.

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήστε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα *"Ζητήσετε βοήθεια"* (p. 345).

6.1.7. Η σύνδεση μου στο Internet είναι αργή

Αυτή η κατάσταση μπορεί να εμφανιστεί μετά την εγκατάσταση του Bitdefender. Το θέμα θα μπορούσε να οφείλεται σε σφάλματα στην διαμόρφωση του Bitdefender firewall.

Για να αντιμετωπίσετε αυτή την κατάσταση:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **FIREWALL** , κάντε κλικ στον διακόπτη για να απενεργοποιήσετε τη λειτουργία.
3. Ελέγξτε αν η σύνδεσή σας στο Internet βελτιώνεται με το Bitdefender τείχος προστασίας απενεργοποιημένο.
   - Εάν εξακολουθείτε να έρχετε αργή σύνδεση με το Internet, το ζήτημα μπορεί να μην προκαλείται από το Bitdefender. Θα πρέπει να επικοινωνήσετε με ον πάροχο σύνδεσης Internet για να ελέγξει εάν η σύνδεση είναι λειτουργική από την πλευρά τους.

     Εάν λάβετε επιβεβαίωση από τον πάροχο υπηρεσιών Διαδικτύου σας ότι η σύνδεση είναι λειτουργική στο πλευρό τους και το πρόβλημα

συνεχίζει, επικοινωνήστε με το Bitdefender όπως περιγράφεται στην ενότητα *"Ζητήσετε βοήθεια"* (p. 345).

- Εάν η σύνδεση στο Internet βελτιώθηκε μετά την απενεργοποίηση του Bitdefender firewall:

  a. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.

  b. Στο παράθυρο **FIREWALL**, πατήστε **Ρυθμίσεις**.

  c. Μεταβείτε στην καρτέλα **Προσαρμογείς δικτύου** και ρυθμίστε τη σύνδεση στο διαδίκτυο στο **Home/Office** .

  d. Στην καρτέλα **Ρυθμίσεις** , απενεργοποιήστε την επιλογή **Προστασία σάρωσης θυρών** .

  Στην περιοχή **Stealth Mode** , κάντε κλικ στην επιλογή **Επεξεργασία συνδέσεων stealth** . Ενεργοποιήστε τη λειτουργία Stealth για τον προσαρμογέα δικτύου στον οποίο είστε συνδεδεμένοι.

  e. Κλείστε το Bitdefender, κάντε επανεκκίνηση του συστήματος και να ελέγξετε την ταχύτητα σύνδεσης στο Internet.

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήστε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα *"Ζητήσετε βοήθεια"* (p. 345).

6.1.8. Πώς να ενημερώσετε το Bitdefender σε μια αργή σύνδεση στο Internet

Αν έχετε μια αργή σύνδεση στο Διαδίκτυο (όπως dial-up), μπορεί να συμβούν σφάλματα κατά τη διάρκεια της διαδικασίας ενημέρωσης.

Για να διατηρήσετε το σύστημά σας ενημερωμένο με την πιο πρόσφατη Bitdefender βάση δεδομένων πληροφοριών απειλών:

1. Πατήστε **Ρυθμίσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Επιλέξτε την καρτέλα **Update**.
3. Απενεργοποιήστε το διακόπτη **Σιωπηλή αναβάθμιση** .
4. Την επόμενη φορά που θα είναι διαθέσιμη μια ενημέρωση, θα σας ζητηθεί να επιλέξετε την ενημέρωση που θέλετε να κατεβάσετε. Επιλέξτε μόνο την **Ενημέρωση υπογραφών** .
5. Το Bitdefender θα κατεβάσει και θα εγκαταστήσει μόνο τη βάση δεδομένων πληροφοριών απειλών.

6.1.9. Οι Υπηρεσίες του Bitdefender δεν ανταποκρίνονται

Αυτό το άρθρο σας βοηθά να αντιμετωπίσετε το σφάλμα **Οι υπηρεσίες του Bitdefender δεν ανταποκρίνονται**. Μπορεί να αντιμετωπίσετε αυτό το σφάλμα ως εξής:

- Το Bitdefender εικονίδιο στην περιοχή ειδοποιήσεων είναι γκρι και για να σας ενημερώσει ότι οι Bitdefender υπηρεσίες δεν ανταποκρίνεται.
- Το παράθυρο του Bitdefender υποδηλώνει ότι οι υπηρεσίες του Bitdefender δεν ανταποκρίνονται.

Το σφάλμα μπορεί να προκληθεί από μία από τις ακόλουθες συνθήκες:

- προσωρινά σφάλματα επικοινωνίας μεταξύ των υπηρεσιών του Bitdefender.
- ορισμένες από τις υπηρεσίες του Bitdefender έχουν σταματήσει.
- άλλες λύσεις ασφαλείας που εκτελούνται ταυτόχρονα στη συσκευή σας με το Bitdefender.

Για να αντιμετωπίσετε αυτό το σφάλμα, δοκιμάστε τις παρακάτω λύσεις:

1. Περιμένετε μερικά λεπτά και δείτε αν αλλάξει κάτι. Το σφάλμα μπορεί να είναι προσωρινό.
2. Επανεκκινήστε τη συσκευή και περιμένετε λίγα λεπτά μέχρι να φορτωθεί το Bitdefender. Ανοίξτε το Bitdefender για να δείτε εάν το πρόβλημα παραμένει. Η επανεκκίνηση της συσκευής λύνει συνήθως το πρόβλημα.
3. Ελέγξτε αν έχετε εγκαταστήσει κάποια άλλη λύση ασφάλειας που ενδέχεται να διακόψει την ομαλή λειτουργία του Bitdefender. Αν αυτή είναι η περίπτωση, σας συνιστούμε να καταργήσετε όλες τις άλλες λύσεις ασφάλειας και στη συνέχεια εγκαταστήστε ξανά το Bitdefender.

   Για περισσότερες πληροφορίες, ανατρέξτε στην *"Πώς μπορώ να καταργήσω τις άλλες λύσεις ασφάλειας;"* (p. 82).

Εάν το σφάλμα παραμένει, επικοινωνήστε με τους εκπροσώπους υποστήριξής μας για βοήθεια όπως περιγράφεται στην ενότητα *"Ζητήσετε βοήθεια"* (p. 345).

6.1.10. Το Antispam φίλτρο δεν λειτουργεί σωστά

Αυτό το άρθρο σας βοηθά να αντιμετωπίσετε τα ακόλουθα προβλήματα που αφορούν την Bitdefender Antispam λειτουργία φιλτραρίσματος :

- Ένας αριθμός νόμιμων μηνυμάτων e-mail επισημαίνονται ως [spam] (ανεπιθύμητα).
- Πολλά μηνύματα που είναι spam δεν φέρουν την κατάλληλη σήμανση από το φίλτρο antispam.
- Το antispam φίλτρο δεν ανιχνεύει κανένα μήνυμα spam.

Νόμιμα μηνύματα χαρακτηρίζονται ως [spam]

Τα νόμιμα μηνύματα χαρακτηρίζονται ως [spam] απλά επειδή φαίνονται σαν spam στο Bitdefender antispam φίλτρο. Κανονικά μπορείτε να λύσετε αυτό το πρόβλημα με την κατάλληλη διαμόρφωση του antispam φίλτρου.

Το Bitdefender προσθέτει αυτόματα τους δέκτες των μηνυμάτων e-ταχυδρομείου σας σε μια λίστα φίλων. Τα μηνύματα e-mail που λαμβάνετε από τις επαφές στη λίστα Φίλοι θεωρούνται ως νόμιμα. Δεν ελέγχονται από το φίλτρο antispam και, ως εκ τούτου, ποτέ δεν επισημαίνονται ως [spam] .

Η αυτόματη ρύθμιση παραμέτρων του στη λίστα Φίλων δεν εμποδίζει τα σφάλματα ανίχνευσης που μπορεί να συμβούν σε αυτές τις περιπτώσεις:

- Λαμβάνετε πολύ εμπορικό ταχυδρομείο ως συνέπεια της εγγραφής σας στους διάφορους ιστοχώρους Σε αυτή την περίπτωση, η λύση είναι να προσθέσετε τις διευθύνσεις ηλεκτρονικού ταχυδρομείου από τις οποίες μπορείτε να λάβετε τέτοια μηνύματα ηλεκτρονικού ταχυδρομείου στη λίστα Φίλων.
- Ένα σημαντικό τμήμα των νόμιμων mail σας είναι από τους ανθρώπους από τους οποίους δεν είχατε ποτέ πριν λάβει ηλεκτρονικό ταχυδρομείο, όπως πελάτες, δυνητικούς επιχειρηματικούς εταίρους και άλλους. Απαιτούνται άλλες λύσεις σε αυτή την περίπτωση.

  Εάν χρησιμοποιείτε μία από τις εφαρμογές ηλεκτρονικού ταχυδρομείου στις οποίες το Bitdefender ενσωματώνεται, υπόδειξη σφαλμάτων ανίχνευσης.

Σημείωση

Το Bitdefender ενσωματώνεται στις πιο συχνά χρησιμοποιούμενες εφαρμογές ηλεκτρονικού ταχυδρομείου μέσω της εύχρηστης γραμμής εργαλείων antispam. Για μια πλήρη λίστα των υποστηριζόμενων εφαρμογών ηλεκτρονικού ταχυδρομείου, παρακαλούμε ανατρέξτε στο *"Υποστηριζόμενοι πελάτες e-mail και πρωτόκολλα"* (p. 115).

Προσθήκη επαφών στη λίστα φίλων

Εάν χρησιμοποιείτε μία υποστηριζόμενη εφαρμογή ηλεκτρονικού ταχυδρομείου, μπορείτε εύκολα να προσθέσετε τους αποστολείς των νόμιμων μηνυμάτων στη λίστα φίλων. Ακολουθείστε αυτά τα βήματα:

1. Στην εφαρμογή ηλεκτρονικού ταχυδρομείου σας, επιλέξτε ένα μήνυμα ηλεκτρονικού ταχυδρομείου από τον αποστολέα που θέλετε να προσθέσετε στη λίστα φίλων.
2. Κάντε κλικ στο **Προσθήκη φίλων** πλήκτρο στην γραμμή εργαλείων antispam του Bitdefender.
3. Μπορεί να σας ζητηθεί να επικυρώσετε τις διευθύνσεις που προστίθενται στη λίστα Φίλων. Επιλέξτε **Να μην εμφανιστεί αυτό το μήνυμα ξανά** και κάντε κλικ στο **OK** .

Θα λαμβάνετε πάντα μηνύματα e-mail από την διεύθυνση αυτή ανεξάρτητα από το περιεχόμενο.

Εάν χρησιμοποιείτε κάποιο άλλο πρόγραμμα ηλεκτρονικού ταχυδρομείου, μπορείτε να προσθέσετε επαφές στη λίστα Φίλων από τη διεπαφή του Bitdefender Ακολουθείστε αυτά τα βήματα:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην ενότητα **ANTISPAM**, επιλέξτε **Διαχείριση φίλωνs**.

   Εμφανίζεται ένα παράθυρο διαμόρφωσης.
3. Πληκτρολογήστε τη διεύθυνση e-mail από την οποία θέλετε να λαμβάνετε πάντοτε τα μηνύματα ηλεκτρονικού ταχυδρομείου και στη συνέχεια κάντε κλικ στο **ΠΡΟΣΘΗΚΗ**. Μπορείτε να προσθέσετε όσες διευθύνσεις ηλεκτρονικού ταχυδρομείου θέλετε.
4. Κάντε κλικ στο **OK** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

Υπόδειξη σφαλμάτων ανίχνευσης

Εάν χρησιμοποιείτε μια υποστηριζόμενη εφαρμογή ηλεκτρονικού ταχυδρομείου, μπορείτε εύκολα να διορθώσετε το antispam φίλτρο (αναφέροντας ποια μηνύματα e-mail δεν θα έπρεπε να έχουν σημανθεί ως [spam]). Με αυτόν τον τρόπο συμβάλλει στη βελτίωση της αποτελεσματικότητας του φίλτρου antispam. Ακολουθείστε αυτά τα βήματα:

1. Ανοίξτε την εφαρμογή του ηλεκτρονικού ταχυδρομείου σας.
2. Πηγαίνετε στο φάκελο ανεπιθύμητης αλληλογραφίας όπου μετακινούνται τα μηνύματα spam.
3. Επιλέξτε το νόμιμο μήνυμα που εσφαλμένα χαρακτηρίστηκε ως [spam] από το Bitdefender.
4. Κάντε κλικ στο **Προσθήκη στους φίλους κουμπί** στην Bitdefender antispam γραμμή εργαλείων για να προσθέσετε τον αποστολέα στη λίστα Φίλων. Μπορεί να χρειαστεί να κάνετε κλικ στο κουμπί **OK** για να αποδεχτείτε. Θα λαμβάνετε πάντα μηνύματα e-mail από την διεύθυνση αυτή ανεξάρτητα από το περιεχόμενο.
5. Κάντε κλικ στο **Not Spam** κουμπί στην Bitdefender antispam μπάρας εργαλείων (συνήθως βρίσκεται στο πάνω μέρος του παραθύρου της εφαρμογής ηλεκτρονικού ταχυδρομείου). Το μήνυμα ηλεκτρονικού ταχυδρομείου θα μετακινηθεί στο φάκελο Εισερχόμενα.

Πολλά μηνύματα spam δεν ανιχνεύονται

Εάν λαμβάνετε πολλά μηνύματα spam που δεν έχουν επισημανθεί ως [spam] , θα πρέπει να ρυθμίσετε το Bitdefender antispam φίλτρο, έτσι ώστε να βελτιωθεί η αποτελεσματικότητά του.

Δοκιμάστε τις παρακάτω λύσεις:

1. Εάν χρησιμοποιείτε μία από τις εφαρμογές ηλεκτρονικού ταχυδρομείου στις οποίες το Bitdefender ενσωματώνεται, υπόδειξη μη ανιχνευθέντων spam μηνυμάτων.

Σημείωση

Το Bitdefender ενσωματώνεται στις πιο συχνά χρησιμοποιούμενες εφαρμογές ηλεκτρονικού ταχυδρομείου μέσω της εύχρηστης γραμμής εργαλείων antispam. Για μια πλήρη λίστα των υποστηριζόμενων

εφαρμογών ηλεκτρονικού ταχυδρομείου, παρακαλούμε ανατρέξτε στο *"Υποστηριζόμενοι πελάτες e-mail και πρωτόκολλα"* (p. 115).

2. Προσθήκη των Spammers (ανεπιθύμητων αποστολέων) στη λίστα αποστολέων spam Τα μηνύματα e-mail που ελήφθησαν από τις διευθύνσεις της λίστας Spammers επισημαίνονται αυτόματα ως [spam]..

Υπόδειξη μη ανιχνευθέντων spam μηνύματων

Εάν χρησιμοποιείτε μία υποστηριζόμενη εφαρμογή ηλεκτρονικού ταχυδρομείου, μπορείτε εύκολα να υποδείξετε ποιά e- mail θα έπρεπε να είχαν ανιχνευθεί ως spam. Με αυτόν τον τρόπο συμβάλλει στη βελτίωση της αποτελεσματικότητας του φίλτρου antispam. Ακολουθείστε αυτά τα βήματα:

1. Ανοίξτε την εφαρμογή του ηλεκτρονικού ταχυδρομείου σας.
2. Πηγαίνετε στο φάκελο Εισερχόμενα.
3. Επιλέξτε τα μη ανιχνευθέντα spam μηνύματα
4. Κάντε κλικ στο **Is Spam** κουμπί στην Bitdefender antispam μπάρα εργαλείων (συνήθως βρίσκεται στο πάνω μέρος του παραθύρου της εφαρμογής ηλεκτρονικού ταχυδρομείου). Αυτά σημειώνονται αμέσως ως [spam] και μεταφέρονται στο φάκελο ανεπιθύμητης αλληλογραφίας.

Προσθήκη των Spammers (ανεπιθύμητων αποστολέων) στη λίστα αποστολέων spam

Εάν χρησιμοποιείτε μία υποστηριζόμενη εφαρμογή ηλεκτρονικού ταχυδρομείου, μπορείτε εύκολα να προσθέσετε τους αποστολείς των ανεπιθύμητων μηνυμάτων στη λίστα Spammers. Ακολουθείστε αυτά τα βήματα:

1. Ανοίξτε την εφαρμογή του ηλεκτρονικού ταχυδρομείου σας.
2. Πηγαίνετε στο φάκελο ανεπιθύμητης αλληλογραφίας όπου μετακινούνται τα μηνύματα spam.
3. Επιλέξτε τα μηνύματα που έχουν επισημανθεί ως [spam] από το Bitdefender.
4. Κάντε κλικ στο **Προσθήκη Spammers** πλήκτρο στην γραμμή εργαλείων antispam του Bitdefender.

5. Μπορεί να σας ζητηθεί να επικυρώσετε τις διευθύνσεις που προστίθενται στη λίστα Spammers. Επιλέξτε **Να μην εμφανιστεί αυτό το μήνυμα ξανά** και κάντε κλικ στο **OK** .

Εάν χρησιμοποιείτε κάποιο άλλο πρόγραμμα ηλεκτρονικού ταχυδρομείου, μπορείτε να προσθέσετε χειροκίνητα ανεπιθύμητες επαφές στη λίστα Spammers από τη διεπαφή του Bitdefender Είναι βολικό να το κάνετε αυτό μόνο όταν έχετε λάβει πολλά μηνύματα spam από την ίδια διεύθυνση ηλεκτρονικού ταχυδρομείου. Ακολουθείστε αυτά τα βήματα:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στο παράθυρο **ANTISPAM**, πατήστε **Ρυθμίσεις**.
3. Μεταβείτε στο παράθυρο **Διαχείριση ανεπιθύμητων μηνυμάτων** .
4. Πληκτρολογήστε τη διεύθυνση ηλεκτρονικού ταχυδρομείου του spammer και στη συνέχεια κάντε κλικ στο **Προσθήκη** Μπορείτε να προσθέσετε όσες διευθύνσεις ηλεκτρονικού ταχυδρομείου θέλετε.
5. Κάντε κλικ στο **OK** για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

Το antispam φίλτρο δεν ανιχνεύει κανένα μήνυμα spam.

Εάν δεν υπάρχουν μηνύματα που να έχουν έχει επισημανθεί ως [spam] , μπορεί να υπάρχει πρόβλημα με το Bitdefender antispam φίλτρο. Πριν από την αντιμετώπιση αυτού του προβλήματος, βεβαιωθείτε ότι δεν προκαλείται από μία από τις ακόλουθες συνθήκες:

- Η Antispam προστασία μπορεί να έχει απενεργοποιηθεί. Για να επαληθεύσετε την κατάσταση antispam προστασίας, επιλέξτε **Προστασία** στο μενού πλοήγησης στο Bitdefender interface . Αναζητήστε το παράθυρο **Antispam** για να ελέγξετε αν είναι ενεργοποιημένη η λειτουργία.

  Αν το Antispam είναι απενεργοποιημένο, τότε αυτό προκαλεί το πρόβλημά σας. Κάντε κλικ στον αντίστοιχο διακόπτη για να ενεργοποιήσετε την antispam προστασία σας.

- Η Προστασία Antispam του Bitdefender είναι διαθέσιμη μόνο για τους πελάτες e-mail που είναι ρυθμισμένα ώστε να λαμβάνουν μηνύματα ηλεκτρονικού ταχυδρομείου μέσω του πρωτοκόλλου POP3. Αυτό σημαίνει τα εξής:

- - Μηνύματα e-mail μέσω των υπηρεσιών του διαδικτυακού ηλεκτρονικού ταχυδρομείου (όπως το Yahoo, το Gmail, το Hotmail ή άλλο) δεν φιλτράρονται για ενδεχόμενο spam από το Bitdefender.
- Εάν η εφαρμογή του ηλεκτρονικού ταχυδρομείου σας έχει ρυθμιστεί ώστε να λαμβάνει μηνύματα ηλεκτρονικού ταχυδρομείου χρησιμοποιώντας άλλο πρωτόκολλο από το POP3 (για παράδειγμα, IMAP4), τότε το Bitdefender antispam φίλτρο δεν τα ελέγχει για spam.

Σημείωση

Το POP3 είναι ένα από τα πιο ευρέως χρησιμοποιούμενα πρωτόκολλα για τη λήψη μηνυμάτων ηλεκτρονικού ταχυδρομείου από ένα διακομιστή αλληλογραφίας. Αν δεν ξέρετε το πρωτόκολλο που χρησιμοποιεί η εφαρμογή e-mail σας για να κάνετε λήψη μηνυμάτων e-mail, να ρωτήσετε το πρόσωπο που ρύθμισε την εφαρμογή e-mail σας.

- Το Bitdefender Total Security δεν σαρώνει κυκλοφορία Lotus Notes POP3

Μια πιθανή λύση είναι να επισκευάσετε ή να επανεγκαταστήσετε το προϊόν. Ωστόσο, μπορεί να θέλετε να επικοινωνήσετε με την Bitdefender για την υποστήριξη αντ 'αυτού, όπως περιγράφεται στην ενότητα *"Ζητήσετε βοήθεια"* (p. 345).

6.1.11. Η λειτουργία αυτόματης συμπλήρωσης στο Πορτοφόλι μου δεν λειτουργεί

Έχετε αποθηκεύσει τα online διαπιστευτήριά σας στο Bitdefender Password Manager και έχετε παρατηρήσει ότι η Αυτόματη Συμπλήρωση δεν λειτουργεί. Συνήθως, αυτό το ζήτημα εμφανίζεται όταν η επέκταση Πορτοφόλι του Bitdefender δεν έχει εγκατασταθεί στο πρόγραμμα περιήγησης σας.

Για να διορθώσετε αυτή την κατάσταση, ακολουθήστε τα εξής βήματα:

- Στον **Internet Explorer:**
  1. Ανοίξτε τον Internet Explorer.
  2. Κάντε κλικ στο Εργαλεία.
  3. Κάντε κλικ στο Manage Add-ons.
  4. Κάντε κλικ στο Γραμμές Εργαλείων και Επεκτάσεις.
  5. Επιλέξτε το **Bitdefender Wallet** και κάντε κλικ στο κουμπί **Enable**.

- Στον **Mozilla Firefox:**
  1. Ανοίξτε τον Mozilla Firefox.
  2. Κάντε κλικ στο κουμπί **Άνοιγμα μενού** στην επάνω δεξιά γωνία της οθόνης.
  3. Κάντε κλικ στο Add- ons.
  4. Κάντε κλικ στο Επεκτάσεις.
  5. Μεταβείτε στο **Bitdefender Πορτοφόλι** και κάντε κλικ στο διακόπτη δίπλα του.
- Στον **Google Chrome:**
  1. Ανοίξτε το Google Chrome.
  2. Μεταβείτε στο εικονίδιο του Μενού.
  3. Επιλέξτε Περισσότερα Εργαλεία.
  4. Κάντε κλικ στο Επεκτάσεις.
  5. Μεταβείτε στο **Bitdefender Πορτοφόλι** και κάντε κλικ στον αντίστοιχο διακόπτη.

Σημείωση
Το add-on θα ενεργοποιηθεί μετά την επανεκκίνηση του browser σας.

Τώρα, ελέγξτε αν η λειτουργία αυτόματης συμπλήρωσης στο Πορτοφόλι λειτουργεί για τους ηλεκτρονικούς λογαριασμούς σας.

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήστε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα "*Ζητήσετε βοήθεια*" (p. 345).

6.1.12. Η αφαίρεση του Bitdefender απέτυχε

Αν θέλετε να καταργήσετε το Bitdefender προϊόν σας και παρατηρήσετε ότι η διαδικασία κολλάει ή το σύστημα δεν ανταποκρίνεται, κάντε κλικ στο **Άκυρο** για να ακυρώσετε την ενέργεια. Εάν αυτό δεν λειτουργεί, κάντε επανεκκίνηση του συστήματος.

Όταν η αφαίρεση αποτυγχάνει, κάποια κλειδιά μητρώου και αρχεία του Bitdefender ενδέχεται να παραμείνουν στο σύστημά σας. Τέτοια υπολείμματα ενδέχεται να εμποδίζουν μια νέα εγκατάσταση του

Bitdefender. Μπορούν επίσης να επηρεάσουν την απόδοση και τη σταθερότητα του συστήματος.

Για να καταργήσετε εντελώς το Bitdefender από το σύστημά σας:

- Στα **Windows 7**:
  1. Κάντε κλικ στο **Εναρξη**, πηγαίνετε στο **Πίνακας Ελέγχου** και κάντε διπλό κλικ στο **Προγράμματα και Δυνατότητες** .
  2. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
  3. Κάντε κλικ στο **Κατάργηση** στο παράθυρο που εμφανίζεται.
  4. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.
- Στα **Windows 8 και στα Windows 8.1**:
  1. Από την οθόνη Έναρξης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Πίνακας Ελέγχου" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του.
  2. Κάντε κλικ στο **Κατάργηση εγκατάστασης προγράμματος** ή στο **Προγράμματα και δυνατότητες** .
  3. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
  4. Κάντε κλικ στο **Κατάργηση** στο παράθυρο που εμφανίζεται.
  5. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.
- Στα **Windows 10**:
  1. Κάντε κλικ στο **Εκκίνηση**και στη συνέχεια, κάντε κλικ στην επιλογή Ρυθμίσεις.
  2. Κάντε κλικ στο εικονίδιο **Σύστημα** στην περιοχή Ρυθμίσεις, στη συνέχεια, επιλέξτε **Εγκατεστημένες εφαρμογές**.
  3. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.

4. Κάντε κλικ στο **Απεγκατάσταση** ξανά για να επιβεβαιώσετε την επιλογή σας.
5. Κάντε κλικ στο **Κατάργηση** στο παράθυρο που εμφανίζεται.
6. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

6.1.13. Το σύστημα μου δεν ξεκιναει μετά την εγκατάσταση του Bitdefender

Αν έχετε μόλις εγκαταστήσει το Bitdefender και δεν μπορείτε να επανεκκινήσετε το σύστημά σας σε κανονική κατάσταση πλέον, μπορεί να υπάρχουν διάφοροι λόγοι για αυτό το θέμα.

Πιθανότατα αυτό οφείλεται σε μία προηγούμενη εγκατάσταση του Bitdefender, η οποία δεν αφαιρέθηκε σωστά ή από άλλη λύση ασφάλειας που εξακολουθεί να υπάρχει στο σύστημα.

Με αυτόν τον τρόπο μπορείτε να αντιμετωπίσετε την κάθε κατάσταση:

- **Είχατε το Bitdefender πριν και δεν το καταργήσετε σωστά.**

  Για να λυθεί αυτό:

  1. Επανεκκινήστε το σύστημά σας και μπείτε σε κατάσταση ασφαλούς λειτουργίας. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο *"Πώς μπορώ να κάνω επανεκκίνηση σε ασφαλή λειτουργία;"* (p. 84).
  2. Αφαιρέστε το Bitdefender από το σύστημά σας:

     - Στα **Windows 7**:

       a. Κάντε κλικ στο **Εναρξη**, πηγαίνετε στο **Πίνακας Ελέγχου** και κάντε διπλό κλικ στο **Προγράμματα και Δυνατότητες** .

       b. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.

       c. Κάντε κλικ στο **Κατάργηση** στο παράθυρο που εμφανίζεται.

       d. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

       e. Επανεκκινήστε το σύστημά σας σε κανονική λειτουργία.

- Στα **Windows 8 και στα Windows 8.1**:
  a. Από την οθόνη Έναρξης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Πίνακας Ελέγχου" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του.
  b. Κάντε κλικ στο **Κατάργηση εγκατάστασης προγράμματος** ή στο **Προγράμματα και δυνατότητες** .
  c. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
  d. Κάντε κλικ στο **Κατάργηση** στο παράθυρο που εμφανίζεται.
  e. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.
  f. Επανεκκινήστε το σύστημά σας σε κανονική λειτουργία.
- Στα **Windows 10**:
  a. Κάντε κλικ στο **Εκκίνηση**και στη συνέχεια, κάντε κλικ στην επιλογή Ρυθμίσεις.
  b. Κάντε κλικ στο εικονίδιο **Σύστημα** στην περιοχή Ρυθμίσεις, στη συνέχεια, επιλέξτε **Εγκατεστημένες εφαρμογές**.
  c. Βρείτε το **Bitdefender Total Security** και επιλέξτε **Κατάργηση εγκατάστασης**.
  d. Κάντε κλικ στο **Απεγκατάσταση** ξανά για να επιβεβαιώσετε την επιλογή σας.
  e. Κάντε κλικ στο **Κατάργηση** στο παράθυρο που εμφανίζεται.
  f. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.
  g. Επανεκκινήστε το σύστημά σας σε κανονική λειτουργία.

3. Επανεγκατάσταση του Bitdefender προιόντος σας.

- **Είχατε μια διαφορετική λύση ασφαλείας πριν και δεν την απεγκαταστήσατε σωστά.**

  Για να λυθεί αυτό:

1. Επανεκκινήστε το σύστημά σας και μπείτε σε κατάσταση ασφαλούς λειτουργίας. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο *"Πώς μπορώ να κάνω επανεκκίνηση σε ασφαλή λειτουργία;"* (p. 84).
2. Απεγκαταστήστε την άλλη λύση ασφαλείας από το σύστημά σας:
   - Στα **Windows 7**:
     a. Κάντε κλικ στο **Εναρξη**, πηγαίνετε στο **Πίνακας Ελέγχου** και κάντε διπλό κλικ στο **Προγράμματα και Δυνατότητες** .
     b. Βρείτε το όνομα του προγράμματος που θέλετε να καταργήσετε και επιλέξτε **Κατάργηση** .
     c. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.
   - Στα **Windows 8 και στα Windows 8.1**:
     a. Από την οθόνη Έναρξης των Windows, εντοπίστε το **Control Panel** (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Πίνακας Ελέγχου" απευθείας στην οθόνη Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιό του.
     b. Κάντε κλικ στο **Κατάργηση εγκατάστασης προγράμματος** ή στο **Προγράμματα και δυνατότητες** .
     c. Βρείτε το όνομα του προγράμματος που θέλετε να καταργήσετε και επιλέξτε **Κατάργηση** .
     d. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.
   - Στα **Windows 10**:
     a. Κάντε κλικ στο **Εκκίνηση**και στη συνέχεια, κάντε κλικ στην επιλογή Ρυθμίσεις.
     b. Κάντε κλικ στο εικονίδιο **Σύστημα** στην περιοχή Ρυθμίσεις, στη συνέχεια, επιλέξτε **Εγκατεστημένες εφαρμογές**.
     c. Βρείτε το όνομα του προγράμματος που θέλετε να καταργήσετε και επιλέξτε **Απεγκατάσταση**.

d. Περιμένετε την ολοκλήρωση της διαδικασίας κατάργησης εγκατάστασης και, στη συνέχεια, κάντε επανεκκίνηση του συστήματός σας.

Για να απεγκαταστήσετε σωστά το άλλο λογισμικό, πηγαίνετε στην ιστοσελίδα τους και εκτελέστε το εργαλείο της απεγκατάστασης τους ή επικοινωνήσετε απευθείας μαζί τους με σκοπό να σας δώσουν τις κατευθυντήριες γραμμές για την απεγκατάσταση.

3. Επανεκκινήστε το σύστημά σας σε κανονική λειτουργία και επανεγκαταστήσετε το Bitdefender.

Έχετε ήδη ακολουθήσει τα παραπάνω βήματα και η κατάσταση δεν έχει λυθεί.

Για να λυθεί αυτό:

1. Επανεκκινήστε το σύστημά σας και μπείτε σε κατάσταση ασφαλούς λειτουργίας. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο "*Πώς μπορώ να κάνω επανεκκίνηση σε ασφαλή λειτουργία;*" (p. 84).
2. Χρησιμοποιήστε την επιλογή Επαναφορά Συστήματος από τα Windows για να επαναφέρετε τη συσκευή σε προηγούμενη ημερομηνία πριν από την εγκατάσταση του προϊόντος Bitdefender.
3. Επανεκκινήστε το σύστημα σε κανονική λειτουργία και επικοινωνήστε με τους εκπροσώπους υποστήριξής μας για βοήθεια, όπως περιγράφεται στην ενότητα "*Ζητήσετε βοήθεια*" (p. 345).

6.2. Αφαίρεση απειλών από το σύστημά σας

Οι απειλές μπορεί να επηρεάσουν το σύστημά σας με πολλούς διαφορετικούς τρόπους και η προσέγγιση του Bitdefender εξαρτάται από το είδος της επίθεσης του κακόβουλου λογισμικού. Επειδή οι ιοί απειλές αλλάζουν τη συμπεριφορά τους συχνά, είναι δύσκολο να καθοριστεί ένα πρότυπο για τη συμπεριφορά τους και τις ενέργειές τους.

Υπάρχουν περιπτώσεις όπου το Bitdefender δεν μπορεί να αφαιρέσει αυτόματα τη μόλυνση του κακόβουλου λογισμικού από το σύστημά σας. Σε τέτοιες περιπτώσεις, απαιτείται παρέμβαση του χρήστη.

- "*Περιβάλλον διάσωσης*" (p. 218)
- "*Τι πρέπει να κάνετε όταν το Bitdefender εντοπίσει απειλές στη συσκευή σας;*" (p. 219)

Εάν δεν μπορείτε να βρείτε το πρόβλημά σας εδώ, ή εάν οι λύσεις που παρουσιάζονται δεν το λύσουν, μπορείτε να επικοινωνήσετε με τους αντιπροσώπους τεχνικής υποστήριξης της Bitdefender, όπως παρουσιάζονται στο κεφάλαιο *"Ζητήσετε βοήθεια"* (p. 345).

6.2.1. Περιβάλλον διάσωσης

Το **Λειτουργία Διάσωσης** είναι μια λειτουργία του Bitdefender που σας επιτρέπει να σαρώσετε και να απολυμάνετε όλα τα υπάρχοντα διαμερίσματα του σκληρού δίσκου εντός και εκτός του λειτουργικού σας συστήματος.

Bitdefender Το περιβάλλον διάσωσης είναι ενσωματωμένο στα Windows RE,

Εκκίνηση του συστήματός σας στο περιβάλλον διάσωσης

Μπορείτε να εισέρθετε στο περιβάλλον διάσωσης μόνο μέσω του Bitdefender σας, ως εξής:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
3. Κάντε κλικ στο **Άνοιγμα** δίπλα στο **Περιβάλλον διάσωσης** .
4. Κάντε κλικ στο **REBOOT** στο παράθυρο που εμφανίζεται.

   Το Bitdefender περιβάλλον διάσωσης θα φορτώσει σε λίγα λεπτά.

Σάρωση του συστήματός σας στο περιβάλλον διάσωσης

Για να σαρώσετε το περιβάλλον διάσωσης του συστήματός σας:

1. Μπείτε σε Περιβάλλον Διάσωσης, όπως περιγράφεται στο "Εκκίνηση του συστήματός σας στο περιβάλλον διάσωσης" (p. 218).
2. Η διαδικασία σάρωσης του Bitdefender ξεκινά αυτόματα μόλις το σύστημα φορτωθεί στο περιβάλλον διάσωσης.
3. Περιμένετε να ολοκληρωθεί η σάρωση. Εάν εντοπιστεί οποιαδήποτε απειλή, ακολουθήστε τις οδηγίες για να την αφαιρέσετε.
4. Για έξοδο από το περιβάλλον διάσωσης, κάντε κλικ στο κουμπί **Κλείσιμο** στο παράθυρο με τα αποτελέσματα σάρωσης.

6.2.2. Τι πρέπει να κάνετε όταν το Bitdefender εντοπίσει απειλές στη συσκευή σας;

Μπορεί να ανακαλύψετε ότι υπάρχει απειλή στη συσκευή σας με έναν από τους παρακάτω τρόπους:

- Σαρώσατε τη συσκευή σας και το Bitdefender εντόπισε μολυσμένα αντικείμενα σε αυτήν.
- Μια ειδοποίηση για απειλές σάς ενημερώνει ότι το Bitdefender αποκλείει μία ή περισσότερες απειλές στη συσκευή σας.

Σε τέτοιες περιπτώσεις, ενημερώστε το Bitdefender για να βεβαιωθείτε ότι έχετε τις πιο πρόσφατες υπογραφές για απειλές και εκτελέστε μια σάρωση του συστήματος για να αναλύσετε το σύστημα.

Από τη στιγμή που η σάρωση του συστήματος έχει τελειώσει, επιλέξτε την ενέργεια που θέλετε για τα μολυσμένα αντικείμενα (Απολύμανση, Διαγραφή, Μετακίνηση σε καραντίνα).

Προειδοποίηση

Αν υποψιάζεστε ότι το αρχείο είναι μέρος του λειτουργικού συστήματος των Windows ή ότι δεν είναι μολυσμένο αρχείο, μην ακολουθήσετε αυτά τα βήματα και επικοινωνήστε με την Εξυπηρέτηση Πελατών του Bitdefender το συντομότερο δυνατόν.

Αν δεν μπορούσε να πραγματοποιηθεί η επιλεγμένη ενέργεια και το αρχείο καταγραφής της σάρωσης αποκαλύπτει μια μόλυνση η οποία δεν μπορούσε να διαγραφεί, θα πρέπει να αφαιρέσετε το αρχείο (α) χειροκίνητα:

Η πρώτη μέθοδος μπορεί να χρησιμοποιηθεί στην κανονική λειτουργία:

1. Απενεργοποιήστε την σε πραγματικό χρόνο προστασία από τους ιούς του Bitdefender :
   a. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
   b. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
   c. Στο παράθυρο **Advanced** , απενεργοποιήστε το **Bitdefender Shield** .
2. Εμφάνιση κρυφών αντικειμένων στα Windows. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο *"Εμφάνιση κρυφών αντικειμένων στα Windows."* (p. 81).
3. Αναζητήστε τη θέση του μολυσμένου αρχείου (ελέγξτε το αρχείο καταγραφής της σάρωσης) και διαγράψτε το.
4. Ενεργοποιήστε την σε πραγματικό χρόνο προστασία από ιούς του Bitdefender .

Σε περίπτωση που η πρώτη μέθοδος απέτυχε να αφαιρέσει τη μόλυνση:

1. Επανεκκινήστε το σύστημά σας και μπείτε σε κατάσταση ασφαλούς λειτουργίας. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο *"Πώς μπορώ να κάνω επανεκκίνηση σε ασφαλή λειτουργία;"* (p. 84).
2. Εμφάνιση κρυφών αντικειμένων στα Windows. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο *"Εμφάνιση κρυφών αντικειμένων στα Windows."* (p. 81).
3. Αναζητήστε τη θέση του μολυσμένου αρχείου (ελέγξτε το αρχείο καταγραφής της σάρωσης) και διαγράψτε το.
4. Επανεκκινήστε το σύστημά σας και μπείτε σε κανονική λειτουργία.

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήστε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα *"Ζητήσετε βοήθεια"* (p. 345).

6.2.3. Πώς μπορώ να καθαρίσω μία απειλή σε ένα αρχείο;

Ένα συμπιεσμένο αρχείο (archive) είναι ένα αρχείο ή μια συλλογή από αρχεία που έχουν συμπιεστεί κάτω από μια ειδική μορφή για να μειωθεί ο απαιτούμενος χώρος στο δίσκο που απαιτείται για την αποθήκευση των αρχείων.

Μερικές από αυτές τις μορφές είναι ανοικτές, παρέχοντας έτσι στο Bitdefender τη δυνατότητα να σαρώσει στο εσωτερικό τους και στη συνέχεια να λάβει τα κατάλληλα μέτρα για την κατάργησή τους.

Άλλες μορφές αρχείων είναι μερικώς ή πλήρως κλειστές, και το Bitdefender μπορεί να ανιχνεύσει μόνο την παρουσία των ιών μέσα τους, αλλά δεν είναι σε θέση να λάβει οποιαδήποτε άλλα μέτρα.

Εάν το Bitdefender σας ενημερώνει ότι μία απειλή έχει ανιχνευθεί μέσα σε ένα αρχείο και καμία ενέργεια δεν είναι διαθέσιμη, αυτό σημαίνει ότι η κατάργηση της απειλής δεν είναι δυνατή λόγω των περιορισμών σχετικά με τις ρυθμίσεις άδειας του αρχείου .

Δείτε πώς μπορείτε να καθαρίσετε έναν ιό αποθηκευμένο σε ένα αρχείο:

1. Προσδιορίστε το αρχείο που περιλαμβάνει την απειλή εκτελώντας μία σάρωση του συστήματος.
2. Απενεργοποιήστε την σε πραγματικό χρόνο προστασία από τους ιούς του Bitdefender :
   a. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
   b. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
   c. Στο παράθυρο **Advanced** , απενεργοποιήστε το **Bitdefender Shield** .
3. Μεταβείτε στην τοποθεσία του αρχείου το αποσυμπιέστε το χρησιμοποιώντας μια εφαρμογή αρχειοθέτησης, όπως το WinZip.
4. Προσδιορίστε το μολυσμένο αρχείο και διαγράψτε το.
5. Διαγράψτε το αρχικό αρχείο για να βεβαιωθείτε ότι τη μόλυνση έχει αφαιρεθεί τελείως.
6. Επανασυμπιέστε τα αρχεία σε ένα νέο αρχείο χρησιμοποιώντας μια εφαρμογή αρχειοθέτησης, όπως το WinZip.
7. Ενεργοποιήστε την σε πραγματικό χρόνο antivirus προστασία του Bitdefender και να εκτελέσετε μια σάρωση του συστήματος για να βεβαιωθείτε ότι δεν υπάρχει άλλη μόλυνση στο σύστημα.

Σημείωση

Είναι σημαντικό να σημειωθεί ότι μία απειλή αποθηκευμένη σε ένα αρχείο δεν είναι μια άμεση απειλή για το σύστημά σας, δεδομένου ότι αυτή πρέπει να αποσυμπιεστεί και να εκτελεστεί, προκειμένου να μολύνει το σύστημά σας.

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήστε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα *"Ζητήσετε βοήθεια"* (p. 345).

6.2.4. Πώς μπορώ να καθαρίσω μία απειλή σε ένα αρχείο e-mail;

Το Bitdefender μπορεί επίσης να προσδιορίσει τις απειλές σε αρχεία e-mail που αποθηκεύονται στο δίσκο.

Μερικές φορές είναι απαραίτητο να προσδιοριστούν τα μολυσμένα μήνυματα χρησιμοποιώντας τις πληροφορίες που παρέχονται στην αναφορά σάρωσης και να διαγράψτε με το χέρι.

Δείτε πώς μπορείτε να καθαρίσετε μία απειλή αποθηκευμένη σε ένα αρχείο e-mail:

1. Σαρώστε τη βάση δεδομένων e-mail με το Bitdefender.
2. Απενεργοποιήστε την σε πραγματικό χρόνο προστασία από τους ιούς του Bitdefender :
   a. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
   b. Στην **ANTIVIRUS** οθόνη, επιλέξτε **Άνοιγμα**.
   c. Στο παράθυρο **Advanced** , απενεργοποιήστε το **Bitdefender Shield** .
3. Ανοίξτε την αναφορά σάρωσης και χρησιμοποιήστε τις πληροφορίες αναγνώρισης (Θέμα, Από, Έως) των μολυσμένων μηνυμάτων για να τους εντοπίσετε στο πρόγραμμα πελάτη ηλεκτρονικού ταχυδρομείου.
4. Διαγράψτε τα μολυσμένα μηνύματα. Τα περισσότερα προγράμματα πελάτες ηλεκτρονικού ταχυδρομείου μετακινούν επίσης το διαγραμμένο μήνυμα σε ένα φάκελο ανάκτησης, από το οποίο μπορεί να ανακτηθεί. Θα πρέπει να βεβαιωθείτε ότι το μήνυμα διαγράφεται επίσης από αυτόν το φάκελο ανάκτησης.
5. Σύμπτυξη του φακέλου που περιέχει το μολυσμένο μήνυμα.
   - Στο Microsoft Outlook 2007: Στο μενού Αρχείο, κάντε κλικ στην επιλογή Διαχείριση αρχείων δεδομένων. Επιλέξτε στους προσωπικούς φακέλους τα αρχεία (.pst) που σκοπεύετε να συμπιέσετε και κάντε κλικ στις Ρυθμίσεις. Κάντε κλικ στο Σύμπτυξη Τώρα.
   - Στο Microsoft Outlook 2010 / 2013/ 2016: Από το μενού Αρχείο, κάντε κλικ στην επιλογή Πληροφορίες και στη συνέχεια Ρυθμίσεις

λογαριασμού (Προσθέστε και αφαιρέστε τους λογαριασμούς ή να αλλάξετε τις υπάρχουσες ρυθμίσεις σύνδεσης). Στη συνέχεια κάντε κλικ στο Αρχείο Δεδομένων, επιλέξτε στους προσωπικούς φακέλους τα αρχεία (.pst) που σκοπεύετε να συμπιέσετε και κάντε κλικ στο Ρυθμίσεις. Κάντε κλικ στο Σύμπτυξη Τώρα.

6. Ενεργοποιήστε την σε πραγματικό χρόνο προστασία από ιούς του Bitdefender .

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήστε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα "*Ζητήσετε βοήθεια*" (p. 345).

6.2.5. Τι πρέπει να κάνω αν υποπτεύομαι ένα αρχείο ως επικίνδυνο;

Μπορεί να υποψιάζεστε ένα αρχείο από το σύστημά σας να είναι επικίνδυνο, ακόμα και αν το Bitdefender σας δεν το εντοπίσε.

Για να βεβαιωθείτε ότι το σύστημά σας είναι προστατευμένο:

1. Εκτελέστε μία **Σάρωση του Συστήματος** με το Bitdefender. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο "*Πώς μπορώ να ελέγξω το σύστημά μου;*" (p. 57).
2. Εάν το αποτέλεσμα σάρωσης φαίνεται να είναι καθαρό, αλλά εξακολουθείτε να έχετε αμφιβολίες και θέλετε να είστε σίγουροι σχετικά με το αρχείο, επικοινωνήστε με τους εκπροσώπους υποστήριξής μας έτσι ώστε να μπορεσούμε να σας βοηθήσουμε.

   Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο "*Ζητήσετε βοήθεια*" (p. 345).

6.2.6. Ποιά είναι τα αρχεία που προστατεύονται με κωδικό πρόσβασης στο αρχείο καταγραφής της σάρωσης;

Αυτή είναι μόνο μια ειδοποίηση η οποία υποδεικνύει ότι το Bitdefender εντόπισε ότι τα αρχεία αυτά είτε προστατεύονται με κωδικό πρόσβασης ή από κάποια μορφή κρυπτογράφησης.

Συνηθέστερα, τα στοιχεία που είναι προστατευμένα με κωδικό πρόσβασης είναι:

- Αρχεία που ανήκουν σε άλλη λύση ασφάλειας.

- Αρχεία που ανήκουν στο λειτουργικό σύστημα.

Για να σαρώσετε πραγματικά το περιεχόμενο, τα αρχεία αυτά θα πρέπει είτε να εξαχθούν ή αλλιώς να αποκρυπτογραφηθούν.

Σε περίπτωση εξαγωγής αυτών των περιεχομένων, ο σαρωτής σε πραγματικό χρόνο του Bitdefender θα τα σαρώσει αυτόματα για να διατηρηθεί η συσκευή σας προστατευμένη. Αν θέλετε να σαρώσετε τα αρχεία με το Bitdefender, θα πρέπει να επικοινωνήσετε με τον κατασκευαστή του προϊόντος για να σας δώσει περισσότερες λεπτομέρειες σχετικά με αυτά τα αρχεία.

Η πρότασή μας προς εσάς είναι να αγνοήσετε αυτά τα αρχεία, επειδή δεν αποτελούν απειλή για το σύστημά σας.

6.2.7. Ποια είναι τα στοιχεία που έχουν παραλειφθεί στο αρχείο καταγραφής της σάρωσης;

Όλα τα αρχεία που φαίνονται να παραλείπονται στην αναφορά σάρωσης είναι καθαρά.

Για αυξημένη απόδοση, το Bitdefender δεν σαρώνει τα αρχεία που δεν έχουν αλλάξει από την τελευταία σάρωση.

6.2.8. Ποια είναι τα υπερ-συμπιεσμένα αρχεία στο αρχείο καταγραφής της σάρωσης;

Τα υπερ- συμπιεσμένα αντικείμενα είναι στοιχεία τα οποία δεν θα μπορούσαν να εξαχθούν από τη μηχανή σάρωσης ή στοιχεία για τα οποία ο χρόνος αποκρυπτογράφησης θα ήταν ένα υπερβολικά μεγάλο χρονικό διάστημα καθιστώντας το σύστημα ασταθές.

Υπερσυμπίεση σημαίνει ότι το Bitdefender παρέληψε τη σάρωση εντός του εν λόγω αρχείου, επειδή η αποσυμπίεση αποδείχθηκε να καταλαμβάνει πάρα πολλούς πόρους του συστήματος. Το περιεχόμενο θα σαρωθεί σε πραγματικό χρόνο, αν χρειαστεί.

6.2.9. Γιατί το Bitdefender διέγραψε αυτόματα ένα μολυσμένο αρχείο;

Αν εντοπιστεί ένα μολυσμένο αρχείο, το Bitdefender θα προσπαθήσει αυτόματα να το απολυμάνει. Εάν η απολύμανση αποτύχει, το αρχείο μετακινείται σε καραντίνα προκειμένου να περιοριστεί η μόλυνση.

Για συγκεκριμένους τύπους απειλών, η επιδιόρθωση δεν είναι δυνατή επειδή το ανιχνευμένο αρχείο είναι εντελώς κακόβουλο. Σε τέτοιες περιπτώσεις, το μολυσμένο αρχείο διαγράφεται από το δίσκο.

Αυτό συμβαίνει συνήθως με τα αρχεία εγκατάστασης που έχουν ληφθεί από αναξιόπιστες ιστοσελίδες. Αν βρεθείτε σε μια τέτοια κατάσταση, κατεβάστε το αρχείο εγκατάστασης από την ιστοσελίδα του κατασκευαστή ή άλλη έμπιστη ιστοσελίδα.

ANTIVIRUS ΓΙΑ MAC

7. ΕΓΚΑΤΆΣΤΑΣΗ ΚΑΙ ΑΦΑΊΡΕΣΗ

Αυτό το κεφάλαιο περιλαμβάνει τα ακόλουθα θέματα:

7.1. Απαιτήσεις συστήματος

Μπορείτε να εγκαταστήσετε το Bitdefender Antivirus for Mac σε υπολογιστές Macintosh με λειτουργικό σύστημα OS X Yosemite (10.10) ή νεότερες εκδόσεις.

Το Mac σας πρέπει επίσης να διαθέτει τουλάχιστον 1 GB διαθέσιμο χώρο στο σκληρό δίσκο.

Μια σύνδεση στο Internet είναι απαραίτητη για να εγγραφείτε και να ενημερώσετε το Bitdefender Antivirus for Mac.

Σημείωση

Bitdefender Anti-tracker και Bitdefender VPN μπορούν να εγκατασταθούν μόνο σε συστήματα που εκτελούν macOS 10.12 ή νεότερες εκδόσεις.

Πώς να μάθετε την έκδοση του Mac OS X και τις πληροφορίες σχετικά με το Mac σας

Κάντε κλικ στο εικονίδιο της Apple στην επάνω αριστερή γωνία της οθόνης και επιλέξτε **About This Mac**. Στο παράθυρο που εμφανίζεται μπορείτε να δείτε την έκδοση του λειτουργικού σας συστήματος και άλλες χρήσιμες πληροφορίες. Κάντε κλικ στο **Αναφορές Συστήματος** για αναλυτικές πληροφορίες για το Hardware.

7.2. Εγκατάσταση του Bitdefender Antivirus for Mac

Η Bitdefender Antivirus for Mac εφαρμογή μπορεί να εγκατασταθεί από τον Bitdefender λογαριασμό σας ως εξής:

1. Συνδεθείτε ως διαχειριστής.
2. Μετάβαση σε: https://central.bitdefender.com.
3. Συνδεθείτε στο Bitdefender λογαρισμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.

4. Επιλέξτε το **Οι συσκευές μου** και στην συνέχεια κάντε κλικ **ΕΓΚΑΤΑΣΤΑΣΗ ΠΡΟΣΤΑΣΙΑΣ** .
5. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:
   - **Προστατέψτε αυτή τη συσκευή**
     a. Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.
     b. Αποθηκεύστε το αρχείο εγκατάστασης.
   - **Προστασία άλλων συσκευών**
     a. Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.
     b. Επιλέξτε **ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΛΗΨΗΣ**.
     c. Πληκτρολογήστε μια διεύθυνση ηλεκτρονικού ταχυδρομείου στο αντίστοιχο πεδίο και κάντε κλικ στην επιλογή **ΑΠΟΣΤΟΛΗ EMAIL** .

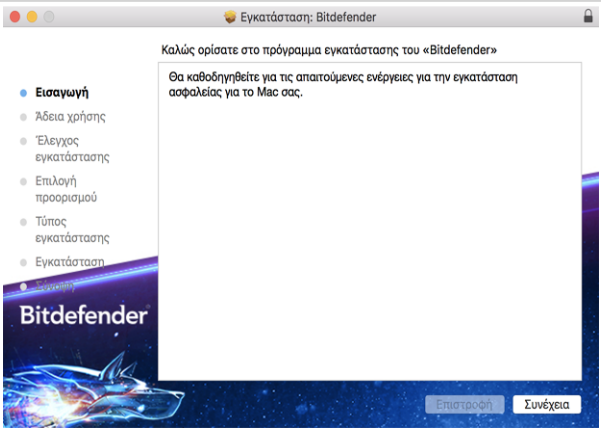
        Λάβετε υπόψη ότι ο παραγόμενος σύνδεσμος λήψης ισχύει μόνο για τις επόμενες 24 ώρες. Εάν λήξει ο σύνδεσμος, θα πρέπει να δημιουργήσετε ένα νέο, ακολουθώντας τα ίδια βήματα.
     d. Στην συσκευή που θέλετε να εγκαταστήσετε το Bitdefender προιόν, ελέγξτε το λογαριασμό ηλεκτρονικού ταχυδρομείου που πληκτρολογήσατε και στην συνέχεια κάντε κλικ στο αντίστοιχο κουμπί λήψης.
6. Εκτελέστε το Bitdefender προϊόν που έχετε κατεβάσει.
7. Ολοκληρώστε τα βήματα εγκατάστασης.

7.2.1. Βήματα εγκατάστασης

Για να εγκαταστήσετε το Bitdefender Antivirus for Mac:

1. Κάντε κλικ στο αρχείο. Αυτό θα ξεκινήσει το πρόγραμμα εγκατάστασης, που θα σας καθοδηγήσει στη διαδικασία εγκατάστασης.
2. Ακολουθήστε τον οδηγό εγκατάστασης.

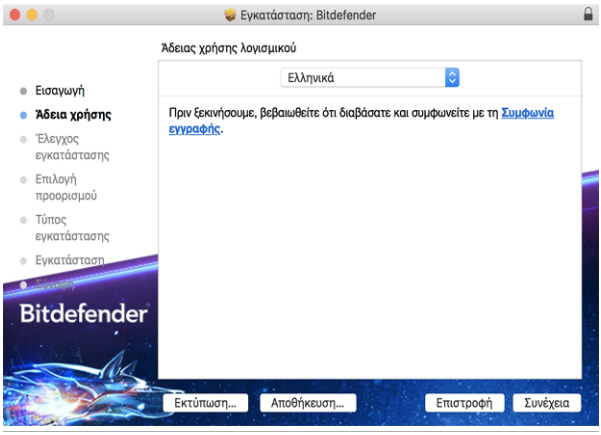
Βήμα 1 - Παράθυρο Καλωσορίσματος



Παράθυρο Καλωσορίσματος

Κάντε κλικ στο **Συνέχεια**.

Βήμα 2 - Διαβάστε την Άδεια Χρήσης



Διαβάστε την Άδεια Χρήσης

Πριν συνεχίσετε με την εγκατάσταση, πρέπει να συμφωνήσετε με τη Συμφωνία Συνδρομής. Αφιερώστε λίγο χρόνο για να διαβάσετε τη

Συμφωνία Συνδρομής επειδή περιέχει τους όρους και τις προϋποθέσεις κάτω από τις οποίες μπορείτε να χρησιμοποιήσετε το Bitdefender Antivirus for Mac.

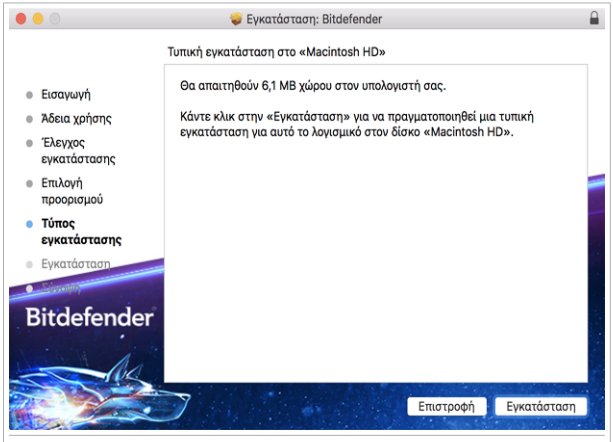
Από αυτό το παράθυρο μπορείτε επίσης να επιλέξετε τη γλώσσα στην οποία θέλετε να εγκαταστήσετε το προϊόν.

Κάντε κλικ στο **Συνέχεια**, και στη συνέχεια κάντε κλικ στο κουμπί **Συμφωνώ**.

Σημαντικό

Εάν δεν συμφωνείτε με αυτούς τους όρους, κάντε κλικ στο **Συνέχεια** και, στη συνέχεια, κάντε κλικ στην επιλογή **Διαφωνώ** για να ακυρώσετε την εγκατάσταση και να κλείσετε το πρόγραμμα εγκατάστασης.

Βήμα 3 - Ξεκινήστε την Εγκατάσταση

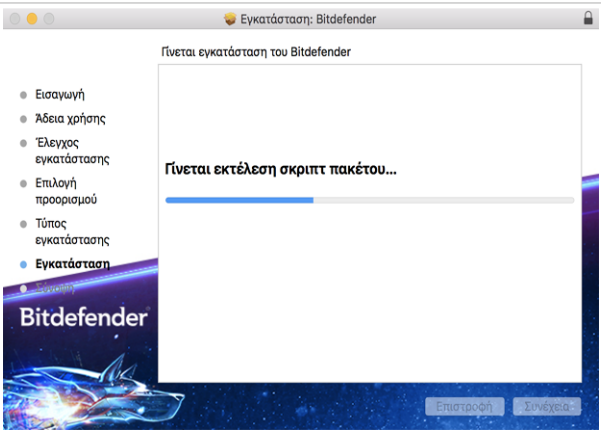


Ξεκινήστε την Εγκατάσταση

Το Bitdefender Antivirus for Mac θα εγκατασταθεί στο Macintosh HD/Library/Bitdefender. Η διαδρομή εγκατάστασης δεν μπορεί να αλλάξει.

Κάντε κλικ στο **Εγκατάσταση** για να ξεκινήσει η εγκατάσταση.

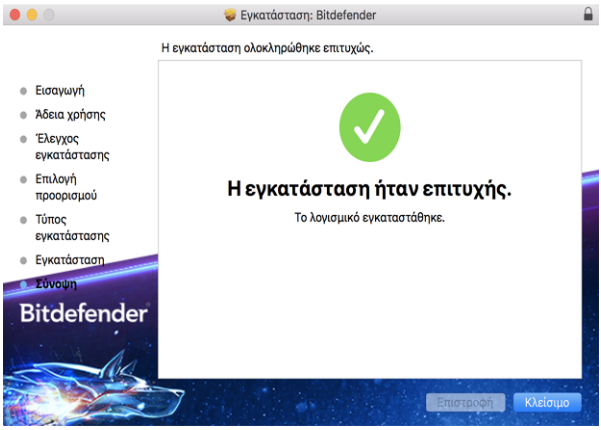
Βήμα 4 - Εγκατάσταση Bitdefender Antivirus for Mac



Εγκατάσταση του Bitdefender Antivirus for Mac

Περιμένετε μέχρι να ολοκληρωθεί η εγκατάσταση, και στη συνέχεια κάντε κλικ στο κουμπί **Συνέχεια**.

Βήμα 5 - Τέλος



ΤΕΛΟΣ

Κάντε κλικ στο **Κλείσιμο** για να κλείσετε το παράθυρο.

Η διαδικασία απεγκατάστασης έχει ολοκληρωθεί.

Σημαντικό

- Εάν εγκαθιστάτε το Bitdefender Antivirus for Mac στο macOS High Sierra 10. 13 ή σε νεότερη έκδοση, εμφανίζεται η ειδοποίηση **Extensions System Blocked** . Αυτή η ειδοποίηση σάς ενημερώνει ότι οι επεκτάσεις που υπογράφηκαν από το Bitdefender έχουν αποκλειστεί και πρέπει να ενεργοποιηθούν χειροκίνητα Κάντε κλικ στο **OK** για να συνεχίσετε. Στο παράθυρο Bitdefender Antivirus for Mac που εμφανίζεται, κάντε κλικ στο **Ασφάλεια και προστασία προσωπικών δεδομένων** Κάντε κλικ στο κουμπί **Να επιτρέπεται** στο κάτω μέρος του παραθύρου ή επιλέξτε τη Bitdefender SRL από τη λίστα και στη συνέχεια κάντε κλικ στο κουμπί **OK** .
- Εάν εγκαθιστάτε το Bitdefender Antivirus for Mac στο macOS Mojave 10.14 ή σε νεότερη έκδοση, θα εμφανιστεί ένα νέο παράθυρο, το οποίο θα σας ενημερώνει ότι πρέπει να **Εκχωρήσετε στο Bitdefender Full Disk Access** και **Να επιτρέπεται η φόρτωση του Bitdefender** . Ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη για να διαμορφώσετε σωστά το προϊόν.

7.3. Αφαίρεση Bitdefender Antivirus for Mac

Όντας μια σύνθετη εφαρμογή, το Bitdefender Antivirus for Mac δεν μπορεί να αφαιρεθεί με το συνήθη τρόπο, σύροντας το εικονίδιο της εφαρμογής από το φάκελο των Applications στον κάδο απορριμμάτων.

Για να αφαιρέσετε το Bitdefender Antivirus for Mac, ακολουθήστε τα εξής βήματα:

1. Ανοίξτε ένα παράθυρο **Finder** και, στη συνέχεια, μεταβείτε στο φάκελο Εφαρμογές.
2. Ανοίξτε τον Bitdefender φάκελο και, στη συνέχεια, κάντε διπλό κλικ στο στοιχείο Απεγκατάσταση Bitdefender.
3. Κάντε κλικ στο κουμπί **Απεγκατάσταση** και περιμένετε να ολοκληρωθεί η διαδικασία.
4. Κάντε κλικ στο **Κλείσιμο** για να τελειώσει.

Σημαντικό

Αν υπάρχει κάποιο λάθος, μπορείτε να επικοινωνήσετε με την Bitdefender Εξυπηρέτηση Πελατών, όπως περιγράφεται στο “Επικοινωνήστε μαζί μας” (p. 344).

8. ΞΕΚΙΝΏΝΤΑΣ

Αυτό το κεφάλαιο περιλαμβάνει τα ακόλουθα θέματα:

8.1. Σχετικά με Bitdefender Antivirus for Mac

Το Bitdefender Antivirus for Mac είναι ένας ισχυρός ανιχνευτής antivirus, το οποίο μπορεί να ανιχνεύσει και να απομακρύνει όλα τα είδη κακόβουλου λογισμικού ("απειλές"), μεταξύ των οποίων:

- ransomware
- adware
- ιοί
- spyware
- Trojans
- keyloggers
- worms

Αυτή η εφαρμογή ανιχνεύει και αφαιρεί όχι μόνο τις απειλές για Mac, αλλά και τις απειλές των Windows, εμποδίζοντας έτσι να στείλετε τυχαία τα μολυσμένα αρχεία στην οικογένεια, τους φίλους και τους συναδέλφους σας χρησιμοποιώντας Η/Υ.

8.2. Άνοιγμα Bitdefender Antivirus for Mac

Έχετε πολλούς τρόπους για να ανοίξει το Bitdefender Antivirus for Mac.

- Κάντε κλικ στο Bitdefender Antivirus for Mac εικονίδιο στο Launchpad.
- Κάντε κλικ στο εικονίδιο στη γραμμή μενού και επιλέξτε **Ανοίξτε το Κύριο Παράθυρο**.
- Ανοίξτε ένα παράθυρο Finder, μεταβείτε στο Applications και κάντε διπλό κλικ στο εικονίδιο Bitdefender Antivirus for Mac.

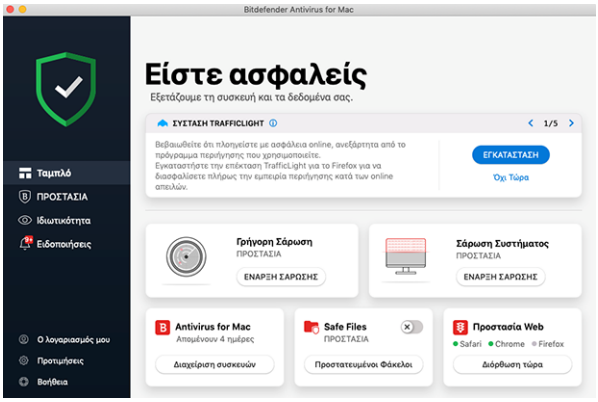
Σημαντικό

Την πρώτη φορά που ανοίγετε το Bitdefender Antivirus for Mac στο MacOS Mojave 10.14 ή σε μια νεότερη έκδοση, εμφανίζεται μια σύσταση προστασίας. Αυτή η σύσταση εμφανίζεται επειδή χρειαζόμαστε δικαιώματα για να σαρώσετε ολόκληρο το σύστημά σας για απειλές. Για να μας δώσετε δικαιώματα, Πρέπει να συνδεθείτε ως διαχειριστής και να ακολουθήσετε τα εξής βήματα:

1. Κάντε κλικ στον σύνδεσμο **Ρυθμίσεις Συστήματος**
2. Κάντε κλικ στο εικονίδιο και πληκτρολογήστε τα credentials διαχειριστή.
3. Ένα νέο παράθυρο ανοίγει. Σύρετε το αρχείο **BDLDaemon** στη λίστα επιτρεπόμενων εφαρμογών.

8.3. Ανοίξτε το Κύριο Παράθυρο

Bitdefender Antivirus for Mac ικανοποιεί τις ανάγκες τόσο των αρχάριων στους υπολογιστές όσο και των πολύ εξειδικευμένων τεχνικά . Το γραφικό περιβάλλον του χρήστη έχει σχεδιαστεί για να ταιριάζει σε κάθε κατηγορία χρηστών.



Ανοίξτε το Κύριο Παράθυρο

Για να εισέλθετε στο μενού του Bitdefender, στην επάνω αριστερή πλευρά, θα εμφανιστεί ένα εισαγωγικός οδηγός με οδηγίες χρήσης και ρύθμισης του προϊόντος. Επιλέξτε το αντίστοιχο σύμβολο για να συνεχίσετε την περιήγηση, ή **Παράλειψη περιήγησης** για να κλείσετε τον οδηγό.

Η γραμμή κατάστασης στο επάνω μέρος του παραθύρου σας ενημερώνει σχετικά με την κατάσταση ασφαλείας του συστήματος χρησιμοποιώντας μηνύματα και χρώματα. Εάν το Bitdefender Antivirus for Mac δεν έχει προειδοποιήσεις, η γραμμή κατάστασης είναι πράσινη. Όταν έχει εντοπιστεί ένα ζήτημα ασφαλείας, η γραμμή κατάστασης αλλάζει το χρώμα του προς το κόκκινο. Για λεπτομερείς πληροφορίες σχετικά με τα θέματα και πώς να τα διορθώσετε, ανατρέξτε στην *"Διόρθωση θεμάτων"* (p. 251).

Για να σας προσφέρουμε αποτελεσματική λειτουργία και αυξημένη προστασία κατά την εκτέλεση διαφορετικών δραστηριοτήτων, ο **Bitdefender Αυτόματος πιλότος** θα ενεργεί ως ο προσωπικός σας σύμβουλος ασφάλειας. Ανάλογα με τη δραστηριότητα που εκτελείτε είτε δουλεύετε είτε κάνετε συναλλαγές online, ο Bitdefender αυτόματος πιλότος του προϊόντος θα σας προτείνει συστάσεις βάσει της χρήσης και των αναγκών της συσκευής. Αυτό θα σας βοηθήσει να ανακαλύψετε και να επωφεληθείτε από τα πλεονεκτήματα που προσφέρουν τα χαρακτηριστικά που περιλαμβάνονται στην εφαρμογή Bitdefender Antivirus for Mac.

Από το μενού πλοήγησης στην αριστερή πλευρά μπορείτε να μεταβείτε στις Bitdefender ενότητες για λεπτομερείς ρυθμίσεις παραμέτρων και σύνθετες εργασίες (καρτέλες **Προστασία** και **Προστασία απορρήτου**), ειδοποιήσεις, ο Bitdefender λογαριασμός σας και η περιοχή Προτιμήσεις . Επικοινωνήστε μαζί μας (καρτέλα **Βοήθεια**) για υποστήριξη σε περίπτωση που έχετε ερωτήσεις ή κάτι απρόσμενο εμφανιστεί.

8.4. Εικονίδιο Dock App

Το Bitdefender Antivirus for Mac εικονίδιο μπορεί να παρατηρήθει στο Dock, μόλις ανοίξετε την εφαρμογή. Το εικονίδιο στο Dock σας παρέχει έναν εύκολο τρόπο για να σαρώσετε τα αρχεία και τους φακέλους για κακόβουλο λογισμικό. Απλά drag and drop το αρχείο ή φάκελο πάνω από το εικονίδιο Dock και η σάρωση θα αρχίσει αμέσως.

Εικονίδιο Dock

8.5. Μενού πλοήγησης

Στην αριστερή πλευρά του Bitdefender interface είναι το μενού πλοήγησης, το οποίο σας επιτρέπει να έχετε γρήγορη πρόσβαση στις Bitdefender λειτουργίες που χρειάζεστε για να χειριστείτε το προϊόν σας. Οι διαθέσιμες καρτέλες σε αυτήν την περιοχή είναι:

- **Dashboard**. Από εδώ, μπορείτε να διορθώσετε γρήγορα ζητήματα ασφαλείας, προβολή συστάσεων σύμφωνα με τις ανάγκες και τα πρότυπα χρήσης του συστήματος σας, εκτέλεση γρήγορων ενεργειών και να μεταβείτε στο Bitdefender λογαριασμό σας για να διαχειριστείτε τις συσκευές που έχετε προσθέσει στη Bitdefender συνδρομή σας .

- **Protection**. Από εδώ, μπορείτε να ξεκινήσετε σαρώσεις για ιούς, να προσθέσετε αρχεία στη λίστα εξαιρέσεων, να προστατεύσετε αρχεία και εφαρμογές από επιθέσεις ransomware, να ασφαλίσετε τα αντίγραφα ασφαλείας του Time Machine και να ρυθμίσετε την προστασία κατά την πλοήγηση στο διαδίκτυο.

- **Απόρρητο**. Από εδώ, μπορείτε να ανοίξετε την εφαρμογή Bitdefender VPN και να εγκαταστήσετε την επέκταση Anti-tracker στον web browser.

- **Ειδοποιήσεις**. Από εδώ μπορείτε να δείτε λεπτομέρειες σχετικά με τις ενέργειες που έγιναν στα σαρωμένα αρχεία.

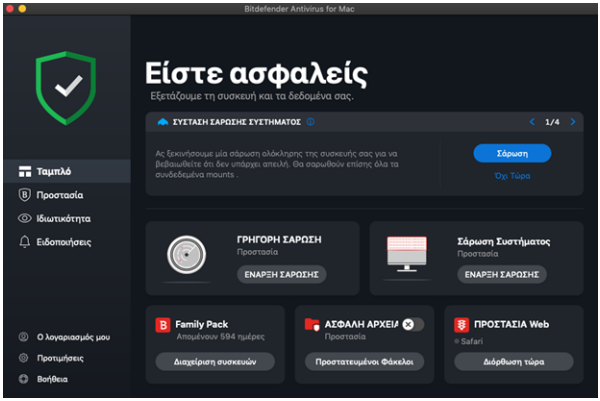
- **Ο λογαριασμός μου**. Αποκτήστε πρόσβαση στον Bitdefender λογαριασμό σας για να επαληθεύσετε τις συνδρομές σας και την εκτέλεση των εργασιών ασφαλείας στις συσκευές που διαχειρίζεστε. Λεπτομέρειες σχετικά με το Bitdefender λογαριασμό και τη συνδρομή που χρησιμοποιείτε είναι διαθέσιμες.

- **Προτιμήσεις** . Από εδώ μπορείτε να ορίσετε τις Bitdefender ρυθμίσεις.

- **Βοήθεια** Από εδώ, όποτε χρειάζεστε βοήθεια για το Bitdefender προϊόν, μπορείτε να επικοινωνήσετε με το τμήμα τεχνικής υποστήριξης. Μπορείτε επίσης να μας στείλετε τα σχόλιά σας για να μας βοηθήσετε να βελτιώσουμε το προϊόν. Μπορείτε επίσης να μας στείλετε τα σχόλιά σας για να μας βοηθήσετε να βελτιώσουμε το προϊόν.

8.6. Dark Mode

Για να προστατέψετε τα μάτια σας από την αντανάκλαση και τα φώτα όταν εργάζεστε τη νύχτα ή σε συνθήκες αθόρυβης λειτουργίας, το Bitdefender Antivirus for Mac υποστηρίζει τη σκοτεινή λειτουργία για το Mojave 10.14 και νεότερο. Τα χρώματα του interface έχουν βελτιστοποιηθεί ώστε να μπορείτε να χρησιμοποιήσετε το Mac χωρίς να ταλαιπωρείτε τα μάτια σας. Το περιβάλλον του Bitdefender Antivirus for Mac προσαρμόζεται ανάλογα με τις ρυθμίσεις εμφάνισης της συσκευής σας.



Dark Mode

9. ΠΡΟΣΤΑΣΊΑ ΑΠΌ ΚΑΚΌΒΟΥΛΟ ΛΟΓΙΣΜΙΚΌ

Αυτό το κεφάλαιο περιλαμβάνει τα ακόλουθα θέματα:

9.1. Βέλτιστες πρακτικές

Για να διατηρήσετε το σύστημά σας προστατευμένο από απειλές και για να αποφύγετε τυχαία μόλυνση άλλων συστημάτων, ακολουθήστε αυτές τις βέλτιστες πρακτικές:

- Διατηρήστε την **Bitdefender Ασπίδα** ενεργοποιημένη, ώστε να επιτρέπεται η αυτόματη σάρωση αρχείων συστήματος από το Bitdefender Antivirus for Mac.
- Διατηρήστε το Bitdefender Antivirus for Macπροϊόν σας ενημερωμένο με τις πιο πρόσφατες πληροφορίες απειλών και ενημερώσεις προϊόντων.
- Ελέγξτε και να διορθώσετε τα ζητήματα που αναφέρθηκαν από το Bitdefender Antivirus for Mac τακτικά. Για αναλυτικές πληροφορίες, ανατρέξτε στο *"Διόρθωση θεμάτων"* (p. 251).
- Ελέγξτε το λεπτομερές αρχείο καταγραφής των γεγονότων που αφορούν το Bitdefender Antivirus for Mac στον υπολογιστή σας. Κάθε φορά που

κάτι σχετικό με την ασφάλεια του συστήματος ή των δεδομένων σας συμβαίνει, ένα νέο μήνυμα, προστίθεται στο Bitdefender ιστορικό. Για περισσότερες λεπτομέρειες δείτε στο "*Ειδοποιήσεις*" (p. 252).

- Θα πρέπει επίσης να συμμορφώνεστε με αυτές τις βέλτιστες πρακτικές:
  - Αποκτήστε την συνήθεια να σαρώνετε τα αρχεία που έχετε κατεβάσει από μια εξωτερική μνήμη αποθήκευσης (όπως ένα USB stick ή ένα CD), ειδικά όταν δεν ξέρετε την πηγή.
  - Εάν έχετε ένα αρχείο DMG, το τοποθετήστε την συσκευή και στη συνέχεια σαρώσετε το περιεχόμενό του (τα αρχεία μέσα στην συσκευή).

  Ο ευκολότερος τρόπος για να σαρώσετε ένα αρχείο, έναν φάκελο ή ένα τόμο είναι να σύρετε και να κάνετε drag&drop πάνω από το Bitdefender Antivirus for Mac παράθυρο ή το εικονίδιο Dock.

Δεν χρειάζεται καμία άλλη ρύθμιση ή ενέργεια. Ωστόσο, αν θέλετε, μπορείτε να προσαρμόσετε τις ρυθμίσεις της εφαρμογής και τις προτιμήσεις για να ταιριάζει καλύτερα στις ανάγκες σας. Για περισσότερες πληροφορίες, ανατρέξτε στην "*Διαμόρφωση Προτιμήσεων*" (p. 256).

9.2. Σάρωση του Mac σας

Εκτός από τη λειτουργία της **Bitdefender Shield** , η οποία παρακολουθεί συνεχώς τις εφαρμογές που εκτελούνται στον υπολογιστή, ψάχνει για απειλητικές ενέργειες και αποτρέπει νέες απειλές από την είσοδο στο σύστημά σας, μπορείτε να σαρώσετε το Mac ή συγκεκριμένα αρχεία οποτεδήποτε θέλετε.

Ο ευκολότερος τρόπος για να σαρώσετε ένα αρχείο, έναν φάκελο ή ένα τόμο είναι να σύρετε και να κάνετε drag&drop πάνω από το Bitdefender Antivirus for Mac παράθυρο ή το εικονίδιο Dock. Ο οδηγός σάρωσης θα εμφανιστεί και θα σας καθοδηγήσει στη διαδικασία σάρωσης.

Μπορείτε επίσης να ξεκινήσετε μια σάρωση ως εξής:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Επιλέξτε την καρτέλα **Δραστηριότητες**.
3. Κάντε κλικ σε ένα από τα τρία κουμπιά σάρωσης για να ξεκινήσει η επιθυμητή σάρωση.

- **Γρήγορη Σάρωση** - ελέγχει για απειλές στις πιο ευάλωτες τοποθεσίες στο σύστημά σας (για παράδειγμα, οι φάκελοι που περιέχουν τα έγγραφα, τις λήψεις, τις λήψεις αλληλογραφίας και τα προσωρινά αρχεία κάθε χρήστη).
- **Σάρωση συστήματος** - εκτελεί έναν ολοκληρωμένο έλεγχο για απειλές ολόκληρου του συστήματος. Όλες οι συνδεδεμένες συσκευές θα σαρωθούν επίσης

Σημείωση

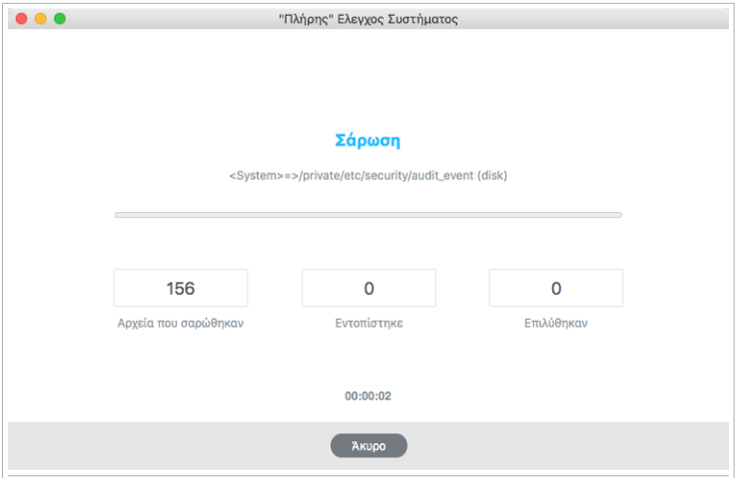
Ανάλογα με το μέγεθος του σκληρού σας δίσκου, σαρώνοντας ολόκληρο το σύστημα μπορεί να διαρκέσει αρκετά (έως μία ώρα ή και περισσότερο). Για βελτιωμένη απόδοση, δεν συνιστάται να εκτελέσετε αυτή την εργασία, ενώ εκτελείτε άλλες εντατική χρήση των πόρων εργασίες (όπως επεξεργασία βίντεο).
Αν προτιμάτε, μπορείτε να επιλέξετε να μην σαρώσετε συγκεκριμένες αποθηκευτικές μονάδες με την προσθήκη τους στη λίστα Εξαιρέσεις από την καρτέλα Προστασία.

- **Προσαρμοσμένη Σάρωση**- σας βοηθά να ελέγξετε συγκεκριμένα αρχεία, φακέλους ή τόμους για απειλές.

Μπορείτε επίσης να ξεκινήσετε μία σάρωση συστήματος ή γρήγορη σάρωση από τον πίνακα ελέγχου.

9.3. Οδηγός Σάρωσης

Κάθε φορά που θα ξεκινάτε μια σάρωση, θα εμφανιστεί ο Bitdefender Antivirus for Mac οδηγός σάρωσης.



Σάρωση σε εξέλιξη

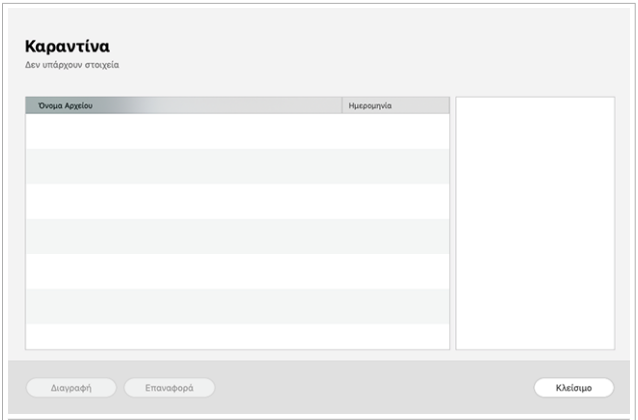
Εμφανίζονται σε πραγματικό χρόνο πληροφορίες σχετικά με την ανίχνευση και τις απειλές που επιλύθηκαν κατά τη διάρκεια της κάθε σάρωσης.

Περιμένετε το Bitdefender Antivirus for Mac ολοκληρώσει τη σάρωση.

Σημείωση
Η διαδικασία σάρωσης μπορεί να πάρει λίγο χρόνο, ανάλογα με την πολυπλοκότητα της σάρωσης.

9.4. Καραντίνα

Το Bitdefender Antivirus for Mac επιτρέπει την απομόνωση των προσβεβλημένων ή ύποπτων αρχείων σε μια ασφαλή περιοχή, που ονομάζεται καραντίνα. Όταν μία απειλή είναι σε καραντίνα δεν μπορεί να κάνει οποιαδήποτε ζημιά, διότι δεν μπορεί να εκτελεστεί ή να διαβαστεί.



Αρχεία στην καραντίνα

Η ενότητα Καραντίνα εμφανίζει όλα τα αρχεία που έχουν απομονωθεί στο φάκελο Καραντίνα.

Για να διαγράψετε ένα αρχείο από την καραντίνα, επιλέξτε το και κάντε κλικ στο **Delete**. Αν θέλετε να επαναφέρετε το αρχείο σε καραντίνα στην αρχική του θέση, επιλέξτε το και κάντε κλικ στο κουμπί **Επαναφορά**.

Για να προβάλετε μια λίστα με όλα τα στοιχεία που προστέθηκαν στην καραντίνα:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Θα ανοίξει το παράθυρο **Antivirus**.

   Κάντε κλικ στο κουμπί **Άνοιγμα** στο παράθυρο **Καραντίνα** .

9.5. Bitdefender Ασπίδα (προστασία πραγματικού χρόνου)

Η Bitdefender παρέχει προστασία σε πραγματικό χρόνο από ένα ευρύ φάσμα απειλών, ελέγχοντας όλες τις εγκατεστημένες εφαρμογές, τις ενημερωμένες εκδόσεις τους και τα νέα και τροποποιημένα αρχεία.

Για να απενεργοποιήσετε την προστασία σε πραγματικό χρόνο:

1. Πατήστε **Προτιμήσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Απενεργοποιήστε τη **Bitdefender Ασπίδα** στο παράθυρο **Προστασίας** .

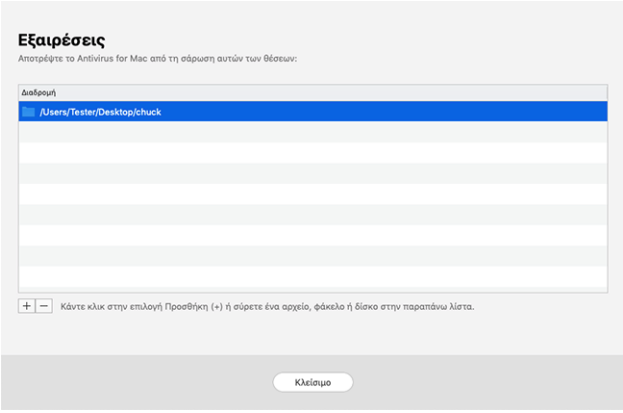
Προειδοποίηση

Αυτό είναι ένα κρίσιμο ζήτημα ασφάλειας. Σας συνιστούμε να απενεργοποιήσετε την προστασία κατά την πρόσβαση για τον ελάχιστο δυνατό χρόνο, και μόνο εφόσον είναι αναγκαία η απενεργοποίηση. Αν η σε πραγματικό χρόνο προστασία είναι απενεργοποιημένη, δεν θα προστατεύεστε από απειλές.

9.6. Εξαιρέσεις σαρώσεων

Αν θέλετε, μπορείτε να ρυθμίσετε το Bitdefender Antivirus for Mac να μην σαρώσει συγκεκριμένα αρχεία, φακέλους, ή ακόμα και ένα ολόκληρο volume. Για παράδειγμα, μπορεί να θέλετε να εξαιρέσετε από τη σάρωση:

- Τα αρχεία που λανθασμένα έχουν χαρακτηριστεί ως μολυσμένα (γνωστά ως false positives)
- Τα αρχεία που προκαλούν σφάλματα σάρωσης
- Backup volumes



Εξαιρέσεις σαρώσεων

Η λίστα εξαιρέσεων περιέχει τις τοποθεσίες που έχουν αποκλειστεί από τη σάρωση.

Για να αποκτήσετε πρόσβαση στη λίστα εξαιρέσεων:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Θα ανοίξει το παράθυρο **Antivirus**.

Κάντε κλικ στο κουμπί **Άνοιγμα** στο παράθυρο **Εξαιρέσεις** .

Υπάρχουν δύο τρόποι για να ορίσετε μια εξαίρεση σάρωσης:

- Με Drag&drop ένα αρχείο, το φάκελο ή τον δίσκο πάνω από τη λίστα εξαιρέσεων.
- Κάντε κλικ στο κουμπί με την ένδειξη με το σύμβολο συν (+), που βρίσκεται κάτω από τη λίστα εξαιρέσεων. Στη συνέχεια, επιλέξτε το αρχείο, το φάκελο ή τον δίσκο που πρέπει να εξαιρεθούν από τη σάρωση.

Για να αφαιρέσετε μια εξαίρεση σάρωσης, επιλέξτε τη από τη λίστα και κάντε κλικ στο κουμπί με το σύμβολο μείον (-), που βρίσκεται κάτω από τη λίστα εξαιρέσεων.

9.7. ΠΡΟΣΤΑΣΙΑ Web

Το Bitdefender Antivirus for Mac χρησιμοποιεί τις επεκτάσεις τθυ trafficlight να εξασφαλίσει την web εμπειρία σας. Το trafficlight ελέγχει και να φιλτράρει όλες την κινηση στο web, μπλοκάροντας κάθε κακόβουλο περιεχόμενο.

Οι επεκτάσεις συνεργάζονται και ενσωματώνονται με τα ακόλουθα προγράμματα περιήγησης στο Web: Mozilla Firefox, Google Chrome και Safari.

Ενεργοποίηση επεκτάσεων Traffic Light

Για να ενεργοποιήσετε τις επεκτάσεις TrafficLight:

1. Κάντε κλικ στο κουμπί **Διόρθωση τώρα στην κάρτα** στην κάρτα **Προστασία web** στον Πίνακα ελέγχου.
2. Ανοίγει το παράθυρο **Προστασία στο Web** .

   Εμφανίζεται το ο browser που έχετε εγκαταστήσει στο σύστημά σας. Για να εγκαταστήσετε την επέκταση Κυκλοφορίας Φως στο πρόγραμμα περιήγησής σας, κάντε κλικ στην επιλογή **Get Extension**.
3. Θα μεταφερθείτε στο:

   https://bitdefender.com/solutions/trafficlight.html
4. Επιλέξτε **FREE DOWNLOAD**.
5. Ακολουθήστε τα βήματα για να εγκαταστήσετε την επέκταση TrafficLight που αντιστοιχεί στο web browser σας.

Διαχείριση ρυθμίσεων επεκτάσεων

Μια σειρά από χαρακτηριστικά είναι διαθέσιμα για να σας προστατεύσει από όλα τα είδη απειλών που μπορεί να συναντήσετε κατά την περιήγηση στο διαδίκτυο. Για πρόσβαση σε αυτά, κάντε κλικ στο εικονίδιο TrafficLight δίπλα στις ρυθμίσεις του προγράμματος περιήγησής σας και, στη συνέχεια, κάντε κλικ στο κουμπί **Ρυθμίσεις** :

- **Bitdefender Ρυθμίσεις TrafficLight**
  - Προστασία Ιστού - σας αποτρέπει από την πρόσβαση σε ιστότοπους που χρησιμοποιούνται για κακόβουλα προγράμματα, επιθέσεις ηλεκτρονικού ψαρέματος και απάτες.
  - Σύμβουλος αναζήτησης - παρέχει εκ των προτέρων προειδοποίηση για επικίνδυνους ιστότοπους στα αποτελέσματα αναζήτησης.
- **Εξαιρέσεις**

  Εάν βρίσκεστε στον ιστότοπο που θέλετε να προσθέσετε σε εξαιρέσεις, κάντε κλικ στην επιλογή **Προσθήκη τρέχοντος ιστότοπου στη λίστα** .

  Εάν θέλετε να προσθέσετε έναν άλλο ιστότοπο, πληκτρολογήστε τη διεύθυνσή του στο αντίστοιχο πεδίο και, στη συνέχεια, κάντε κλικ στο κουμπί .

  Δεν θα εμφανίζεται καμία προειδοποίηση σε περίπτωση εμφάνισης απειλών στις σελίδες που έχουν εξαιρεθεί. Αυτός είναι ο λόγος για τον οποίο θα πρέπει να προστεθούν στον ιστότοπο μόνο οι ιστότοποι που εμπιστεύεστε πλήρως.

Βαθμολογία σελίδων και ειδοποιήσεις

Ανάλογα με το πώς το TrafficLight κατατάσσει την ιστοσελίδα που βλέπετε αυτή τη στιγμή, ένα από τα παρακάτω εικονίδια εμφανίζονται στην περιοχή του:

Αυτή είναι μια ασφαλής σελίδα για να επισκεφθείτε. Μπορείτε να συνεχίσετε την εργασία σας.
Αυτή η ιστοσελίδα μπορεί να περιέχει επικίνδυνο περιεχόμενο. Να είστε προσεκτικοί αν αποφασίσετε να την επισκεφτείτε.
Θα πρέπει να φύγετε αμέσως από την ιστοσελίδα καθώς περιέχει κακόβουλο λογισμικό ή άλλες απειλές.

Στο Safari, το φόντο των εικονιδίων του Traffic Light είναι μαύρο.

9.8. Anti-tracker

Πολλοί ιστότοποι που επισκέπτεστε χρησιμοποιούν trackers για τη συλλογή πληροφοριών σχετικά με τη συμπεριφορά σας, είτε για να τις μοιραστεί με εταιρείες τρίτων είτε για να προβάλλει διαφημίσεις που είναι πιο συναφείς για εσάς. Με αυτόν τον τρόπο, οι ιδιοκτήτες ιστότοπων κερδίζουν χρήματα για να σας παρέχουν δωρεάν περιεχόμενο ή να συνεχίσουν να λειτουργούν. Εκτός από τη συλλογή πληροφοριών, οι trackers μπορούν να επιβραδύνουν την εμπειρία περιήγησης ή να χρησιμοποιήσουν το bandwidth σας.

Με την επέκταση ενεργοποιημένη του Bitdefender Anti-Tracker στο πρόγραμμα περιήγησης ιστού, αποφεύγετε να σας παρακολουθούν, ώστε τα δεδομένα σας να παραμένουν ιδιωτικά κατά την περιήγηση στο διαδίκτυο και να επιταχύνετε τον χρόνο που χρειάζεται να φορτώσουν οι ιστότοποι.

Η επέκταση του Bitdefender είναι συμβατή με τα ακόλουθα προγράμματα περιήγησης ιστού:

- Google Chrome
- Mozilla Firefox
- Safari

Οι trackers που ανιχνεύουμε ομαδοποιούνται στις παρακάτω κατηγορίες:

- **Διαφήμιση** - χρησιμοποιείται για την ανάλυση της επισκεψιμότητας των ιστότοπων, της συμπεριφοράς των χρηστών ή των επισκεπτών.
- **Αλληλεπίδραση Πελατών** - χρησιμοποιείται για τη μέτρηση της αλληλεπίδρασης του χρήστη με διαφορετικές φόρμες εισόδου, όπως η συνομιλία ή η υποστήριξη.
- **Απαραίτητο** - χρησιμοποιείται για την παρακολούθηση σημαντικών λειτουργιών ιστοσελίδας.
- **Ανάλυση Ιστοστελίδας** - χρησιμοποιείται για τη συλλογή δεδομένων σχετικά με τη χρήση της ιστοσελίδας.
- **Κοινωνικά Δίκτυα** - χρησιμοποιείται για την παρακολούθηση του κοινωνικού κοινού, της δραστηριότητας και της εμπλοκής του χρήστη με διαφορετικές πλατφόρμες κοινωνικών μέσων.

Ενεργοποίηση του Bitdefender Anti-tracker

Για να ενεργοποιήσετε το Bitdefender Anti-tracker στον browser σας:

1. Πατήστε **Απόρρητο** στο μενού πλοήγησης του Bitdefender interface.
2. Επιλέξτε την καρτέλα **Anti-tracker** .
3. Κάντε κλικ στην επιλογή **Ενεργοποίηση επέκτασης** δίπλα στο πρόγραμμα περιήγησης ιστού για το οποίο θέλετε να ενεργοποιήσετε την επέκταση.

9.8.1. Περιβάλλον Anti-tracker

Όταν είναι ενεργοποιημένη η επέκταση Bitdefender Anti-tracker, εμφανίζεται το εικονίδιο δίπλα στη γραμμή αναζήτησης στο πρόγραμμα περιήγησής σας. Κάθε φορά που επισκέπτεστε έναν ιστότοπο, μπορεί να παρατηρηθεί ένας μετρητής στο εικονίδιο, αναφερόμενος στους εντοπισμένους και αποκλεισμένους trackers. Για να δείτε περισσότερες λεπτομέρειες σχετικά με τους αποκλεισμένους trackers, κάντε κλικ στο εικονίδιο για να ανοίξετε το περιβάλλον. Εκτός από τον αποκλεισμό του αριθμού των trackers , μπορείτε να δείτε τον χρόνο που απαιτείται για τη φόρτωση της σελίδας και τις κατηγορίες στις οποίες ανήκουν οι εντοπισμένοι trackers. Για να προβάλετε τη λίστα με τους ιστότοπους που παρακολουθούν, κάντε κλικ στην κατηγορία που θέλετε.

Για να απενεργοποιήσετε το Bitdefender από το να μπλοκάρει τους trackers στον ιστότοπο που επισκέπτεστε αυτήν τη στιγμή, κάντε κλικ στην επιλογή **Παύση προστασίας σε αυτόν τον ιστότοπο**. Αυτή η ρύθμιση ισχύει μόνο εφόσον έχετε ανοιχτό τον ιστότοπο και θα επανέλθει στην αρχική κατάσταση όταν κλείσετε τον ιστότοπο.

Για να επιτρέψετε σε trackers από συγκεκριμένη κατηγορία να παρακολουθούν τη δραστηριότητά σας, κάντε κλικ στην επιθυμητή δραστηριότητα και, στη συνέχεια, κάντε κλικ στο αντίστοιχο κουμπί. Αν αλλάξετε γνώμη, κάντε ξανά κλικ στο ίδιο κουμπί.

9.8.2. Απενεργοποιώντας το Bitdefender Anti-tracker

Για να απενεργοποιήσετε το Bitdefender Anti-tracker στον browser σας:

1. Ανοίξτε τον browser σας.

2. Επιλέξτε το εικονίδιο δίπλα στη γραμμή διευθύνσεων του browser σας.
3. Κάντε κλικ στο εικονίδιο στην επάνω δεξιά πλευρά της οθόνης.
4. Χρησιμοποιήστε τον αντίστοιχο διακόπτη για το απενεργοποιήσετε.

   Το Bitdefender εικονίδιο γίνεται γκρι.

9.8.3. Επιτρέποντας την παρακολούθηση ενός ιστότοπου

Εάν θέλετε να παρακολουθείστε την ώρα που επισκέπτεστε έναν συγκεκριμένο ιστότοπο, μπορείτε να προσθέσετε τη διεύθυνσή του στις εξαιρέσεις ως εξής:

1. Ανοίξτε τον browser σας.
2. Κάντε κλικ στο κουμπί δίπλα στη γραμμή αναζήτησης.
3. Κάντε κλικ στο εικονίδιο στην επάνω δεξιά πλευρά της οθόνης.
4. Εάν βρίσκεστε στον ιστότοπο που θέλετε να προσθέσετε σε εξαιρέσεις, κάντε κλικ στην επιλογή **Προσθήκη τρέχοντος ιστότοπου στη λίστα** .

   Εάν θέλετε να προσθέσετε έναν άλλο ιστότοπο, πληκτρολογήστε τη διεύθυνσή του στο αντίστοιχο πεδίο και, στη συνέχεια, κάντε κλικ στο κουμπί .

9.9. ΑΣΦΑΛΗ ΑΡΧΕΙΑ

Το Ransomware είναι ένα κακόβουλο λογισμικό που επιτίθεται σε ευάλωτα συστήματα κλειδώνοντας τα, και ζητά χρήματα για να επιτρέψει στο χρήστη να ανακτήσει τον έλεγχο του συστήματός του. Αυτό το κακόβουλο λογισμικό ενεργεί έξυπνα, εμφανίζοντας ψεύτικα μηνύματα για να πανικοβάλει το χρήστη, πιέζοντάς τον να προβεί στη πληρωμή που του ζητά.

Χρησιμοποιώντας την τελευταία λέξη της τεχνολογίας, η Bitdefender εξασφαλίζει την ακεραιότητα του συστήματος προστατεύοντας κρίσιμους τομείς του συστήματος από επιθέσεις ransomware χωρίς να επηρεάσει το σύστημα. Ωστόσο, μπορεί επίσης να θέλετε να προστατέψετε τα προσωπικά σας αρχεία, όπως έγγραφα, φωτογραφίες ή ταινίες από την πρόσβαση σε εφαρμογές που δεν είναι αξιόπιστες. Με τα Bitdefender

Ασφαλή Αρχεία μπορείτε να ρυθμίσετε προσωπικά αρχεία σε ένα shelter και να ρυθμίσετε μόνοι σας σε ποιες εφαρμογές θα πρέπει να επιτρέπεται να πραγματοποιούν αλλαγές στα προστατευμένα αρχεία και ποιές όχι.

Για να προσθέσετε αργότερα αρχεία στο προστατευμένο περιβάλλον:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Επιλέξτε την καρτέλα **Anti-Ransomware** .
3. Κάντε κλικ στο κουμπί **Προστατευμένα αρχεία** στην περιοχή Ασφαλή αρχεία.
4. Κάντε κλικ στο κουμπί με την ένδειξη με το σύμβολο συν (+), που βρίσκεται κάτω από τη λίστα εξαιρέσεων. Στη συνέχεια, επιλέξτε το αρχείο, τον φάκελο ή τον τόμο που θα προστατεύσετε σε περίπτωση που οι επιθέσεις ransomware θα προσπαθήσουν να έχουν πρόσβαση σε αυτές.

Για να αποφύγετε την επιβράδυνση του συστήματος, σας συνιστούμε να προσθέσετε το πολύ 30 φακέλους ή να αποθηκεύσετε πολλά αρχεία σε έναν μόνο φάκελο.

Από προεπιλογή, οι φάκελοι Εικόνες, Βίντεο, Μουσική, Επιφάνεια εργασίας και Λήψεις προστατεύονται από επιθέσεις απειλής.

Σημείωση

Οι προσαρμοσμένοι φάκελοι προστατεύονται μόνο για τους τρέχοντες χρήστες. Δεν μπορούν να προστεθούν εξωτερικές μονάδες δίσκου, αρχεία συστήματος και εφαρμογών στο περιβάλλον προστασίας.

Θα ενημερώνεστε κάθε φορά που μια άγνωστη εφαρμογή με ασυνήθιστη συμπεριφορά θα προσπαθήσει να τροποποιήσει τα αρχεία που προσθέσατε. Κάντε κλικ στο κουμπί **Επέτρεψε** ή **Αποκλεισμός** και προσθέστε το στη λίστα Διαχείριση εφαρμογών .

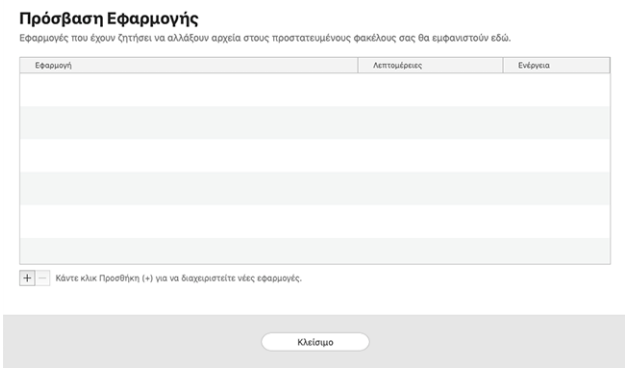
9.9.1. Πρόσβαση σε εφαρμογές

Αυτές οι εφαρμογές που προσπαθούν να αλλάξουν ή να διαγράψουν τα προστατευμένα αρχεία μπορεί να επισημανθούν ως δυνητικά ανασφαλείς και προστεθούν στη λίστα των "αποκλεισμένων εφαρμογών". Αν μια τέτοια εφαρμογή είναι αποκλεισμένη και είστε σίγουροι ότι η συμπεριφορά της είναι φυσιολογική, μπορείτε να την εξαιρέσετε ακολουθώντας τα παρακάτω βήματα:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του Bitdefender interface.
2. Επιλέξτε την καρτέλα **Anti-Ransomware** .
3. Κάντε κλικ στην επιλογή **Πρόσβαση εφαρμογών** στην περιοχή Ασφαλή Αρχεία.
4. Αλλάξτε την κατάσταση στην επιλογή Να επιτρέπεται δίπλα στην αποκλεισμένη εφαρμογή.

Οι εφαρμογές που έχουν οριστεί στην επιλογή Να επιτρέπεται μπορούν να οριστούν και ως Αποκλεισμένες.

Χρησιμοποιήστε τη μέθοδο drag& ή κάντε κλικ στο σύμβολο συν (+) για να προσθέσετε περισσότερες εφαρμογές στη λίστα.



ΑΣΦΑΛΗ ΑΡΧΕΙΑ

9.10. Προστσία Time Machine

Η Bitdefender Time Machine Protection χρησιμεύει ως ένα επιπλέον επίπεδο ασφάλειας του backup δίσκο σας, συμπεριλαμβανομένων όλων των αρχείων που έχετε αποφασίσει να αποθηκεύσετε σε αυτό, εμποδίζοντας την πρόσβαση από οποιαδήποτε εξωτερική πηγή. Στην περίπτωση που φάκελοι από το Time Machine δίσκο σας κρυπτογραφηθούν από ransomware, θα είστε σε θέση να τους ανακτήσει χωρίς να πληρώσετε για αντάλλαγμα λύτρα.

Σε περίπτωση που χρειαστεί να επαναφέρετε στοιχεία από ένα εφεδρικό αντίγραφο του Time Machine, ανατρέξτε στη σελίδα υποστήριξης της Apple για οδηγίες.

Ενεργοποίηση ή απενεργοποίηση της Time Machine προστασίας

Για να ενεργοποιήσετε ή να απενεργοποιήσετε την προστασία του Time Machine:

1. Πατήστε **Προστασία** στο μενού πλοήγησης του **Bitdefender interface**.
2. Επιλέξτε την καρτέλα **Anti-Ransomware** .
3. Ενεργοποιήστε ή απενεργοποιήστε το διακόπτη **Προστασία Time Machine** .

9.11. Διόρθωση θεμάτων

Το Bitdefender Antivirus for Mac εντοπίζει αυτόματα και σας ενημερώνει για μια σειρά από ζητήματα που μπορούν να επηρεάσουν την ασφάλεια του συστήματος και των δεδομένων σας. Με αυτόν τον τρόπο, μπορείτε να διορθώσετε κινδύνους ασφαλείας εύκολα και έγκαιρα.

Η διόρθωση των θεμάτων που υποδεικνύεται από το Bitdefender Antivirus for Mac είναι ένας γρήγορος και εύκολος τρόπος για να εξασφαλιστεί η βέλτιστη προστασία των συστημάτων και των δεδομένων σας.

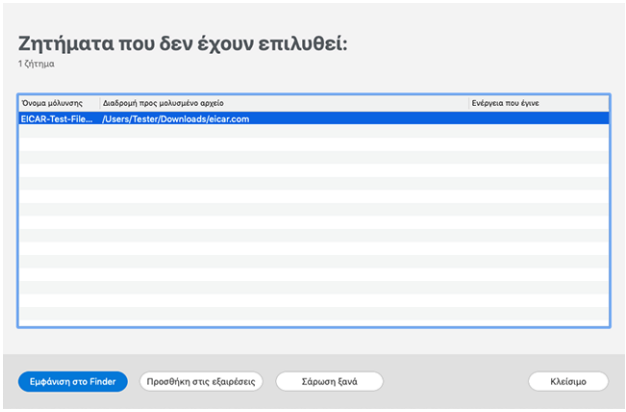
Τα θέματα που εντοπίζονται περιλαμβάνουν:

- Η νέα ενημέρωση πληροφοριών απειλής δεν έχει ληφθεί από τους servers μας.
- Έχουν εντοπιστεί απειλές στο σύστημά σας και το προϊόν δεν μπορεί να τους καθαρίσει αυτόματα.
- Η προστασία σε πραγματικό χρόνο είναι απενεργοποιημένη

Για να ελέγξετε και να διορθώσετε θέματα που ανιχνευτήκαν:

1. Εάν το Bitdefender δεν έχει προειδοποιήσεις, η γραμμή κατάστασης είναι πράσινη. Όταν έχει εντοπιστεί ένα ζήτημα ασφαλείας, η γραμμή κατάστασης αλλάζει το χρώμα του προς το κόκκινο.
2. Ελέγξτε την περιγραφή για περισσότερες πληροφορίες.

3. Όταν εντοπιστεί ένα πρόβλημα, κάντε κλικ στο αντίστοιχο κουμπί για να αναλάβετε δράση.



Παράθυρο Άλυτων Απειλών

Η λίστα των ανεπίλυτων απειλών ενημερώνεται μετά από κάθε σάρωση του συστήματος, ανεξάρτητα από το αν η σάρωση γίνεται αυτόματα στο παρασκήνιο ή αρχίζει από εσάς.

Μπορείτε να επιλέξετε να κάνετε τις ακόλουθες ενέργειες για τις άλυτες απειλές:

- Χειροκίνητη διαγραφή. Επιλέξτε αυτή την ενέργεια για να αφαιρέσει τις απειλές χειροκίνητα.
- Προσθήκη στις εξαιρέσεις. Η ενέργεια αυτή δεν είναι διαθέσιμη για απειλές που βρέθηκαν μέσα σε συμπιεσμένα αρχεία.

9.12. Ειδοποιήσεις

Το Bitdefender διατηρεί ένα λεπτομερές αρχείο καταγραφής των γεγονότων σχετικά με τη δραστηριότητά του στον υπολογιστή σας. Κάθε φορά που συμβαίνει κάτι σχετικό με την ασφάλεια του συστήματος ή των δεδομένων σας, ένα νέο μήνυμα προστίθεται στις Ενημερώσεις του Bitdefender με τον ιδιο τρόπο που ένα νέο μήνυμα ηλεκτρονικού ταχυδρομείου εμφανίζεται στα Εισερχόμενα σας.

Οι Ενημερωςεις αποτελούν ένα πολύ σημαντικό εργαλείο για την παρακολούθηση και τη διαχείριση της προστασίας του Bitdefender σας.

Για παράδειγμα μπορείτε εύκολα να ελέγξετε αν η ενημέρωση πραγματοποιήθηκε με επιτυχία, αν βρέθηκαν απειλές στον υπολογιστή σας κ.λπ. Επιπλέον, μπορείτε να κάνετε περαιτέρω ενέργειες αν χρειαστεί ή να αλλάξετε ενέργειες που έχουν γίνει από το Bitdefender.

Για να αποκτήσετε πρόσβαση στο ιστορικό Ειδοποιήσεων, κάντε κλικ στο **Ειδοποιήσεις** στο μενού πλοήγησης στο Bitdefender interface. Κάθε φορά που συμβαίνει κάποιο σημαντικό γεγονός, ένας μετρητής μπορεί να παρατηρηθεί στο 2 εικονίδιο.

Ανάλογα με τον τύπο και τη σοβαρότητα, οι ειδοποιήσεις ομαδοποιούνται σε:

- **Critical** τα συμβάντα δείχνουν κρίσιμα θέματα. Θα πρέπει να τα ελέγξετε αμέσως.
- **Προσοχή** τα συμβάντα δείχνουν μη κρίσιμα θέματα Θα πρέπει να τα ελέγξετε και να τα διορθώσετε όταν έχετε το χρόνο.
- Οι **πληροφορίες** συμβάντων δείχνουν επιτυχείς εργασίες

Κάντε κλικ σε κάθε καρτέλα για να βρείτε περισσότερες λεπτομέρειες σχετικά με τα συμβάντα που δημιουργούνται. Τα συνοπτικά στοιχεία εμφανίζονται με ένα κλικ σε κάθε τίτλο συμβάντος, και συγκεκριμένα: μια σύντομη περιγραφή, η δράση που το Bitdefender πήρε όταν συνέβη, και την ημερομηνία και την ώρα, όταν αυτό συνέβη. Επιλογές μπορεί να παρέχονται για να ληφθεί περαιτέρω ενέργεια εάν χρειαστεί.

Για να σας βοηθήσει να διαχειριστείτε εύκολα τα καταγεγραμμένα συμβάντα, κάθε τμήμα του παραθύρου Ενημερώσεις παρέχει επιλογές για τη διαγραφή ή σήμανση ως αναγνωσμένου όλων των γεγονότων σε αυτό το τμήμα.

9.13. ενημερώσεις

Νέες απειλές ανιχνεύεται και προσδιορίζονται κάθε μέρα. για αυτό είναι πολύ σημαντικό να ενημερώνεται το Bitdefender Antivirus for Mac με τις τελευταίες ενημερώσεις πληροφοριών απειλής.

Οι ενημερώσεις πληροφοριών απειλής εκτελούνται εν κινήσει, πράγμα που σημαίνει ότι τα ενημερωμένα αρχεία αντικαθίστανται σταδιακά, έτσι ώστε η ενημέρωση να μην επηρεάζει τη λειτουργία του προϊόντος και ταυτόχρονα να αποκλείεται οποιαδήποτε ευπάθεια.

- Όταν το Bitdefender Antivirus for Mac είναι ενημερωμένο, μπορεί να ανιχνεύσει τις πιο πρόσφατες απειλές και να καθαρίσει τυχών μολυσμένα αρχεία.
- Εάν το Bitdefender Antivirus for Mac δεν είναι ενημερωμένο , δεν θα είναι σε θέση να εντοπίζει και να απομακρύνει τις απειλές που ανακαλύφθηκαν από τα Bitdefender Labs.

9.13.1. Ζητώντας ενημέρωση

Μπορείτε να ζητήσετε μια ενημέρωση χειροκίνητα όποτε θέλετε.

Μια ενεργή σύνδεση στο Internet είναι απαραίτητη προκειμένου να ελέγξετε για διαθέσιμες ενημερώσεις και να τις κατεβάσετε.

Για να ζητήσετε μια ενημερωμένη έκδοση χειροκίνητα:

1. Κάντε κλικ στο κουμπί **Actions** στη γραμμή μενού.
2. Επιλέξτε **Ενημέρωση βάσης δεδομένων** .

Εναλλακτικά, μπορείτε να ζητήσετε μια ενημέρωση χειροκίνητα πατώντας CMD + U.

Μπορείτε να δείτε την πρόοδο της ενημέρωσης και την λήψη των αρχείων.

9.13.2. Παίρνοντας ενημερώσεις μέσω ενός Proxy Server

Το Bitdefender Antivirus for Mac μπορεί να παίρνει ενημερώσεις μόνο μέσω proxy servers που δεν απαιτούν έλεγχο ταυτότητας. Δεν χρειάζεται να διαμορφώσετε τις ρυθμίσεις του προγράμματος.

Εάν συνδέεστε στο Internet μέσω ενός proxy server που απαιτεί έλεγχο ταυτότητας, θα πρέπει να μεταβείτε σε απευθείας σύνδεση με το Διαδίκτυο τακτικά προκειμένου να λάβετε τις ενημερώσεις.

9.13.3. Αναβάθμιση σε νέα έκδοση

Περιστασιακά, έχουμε δημοσιεύουμε ενημερώσεις του προϊόντος για να προσθέσετε νέα χαρακτηριστικά και βελτιώσεις ή και να διορθώσουμε ζητήματα του προϊόντος. Αυτές οι ενημερώσεις απαιτούν επανεκκίνηση του συστήματος, προκειμένου να ξεκινήσει η εγκατάσταση των νέων αρχείων. Από προεπιλογή, εάν μια ενημερωμένη έκδοση απαιτεί επανεκκίνηση του υπολογιστή, το Bitdefender Antivirus for Mac θα συνεχίζει να δουλεύει με τα προηγούμενα αρχεία μέχρι να επανεκκινήσετε το

σύστημα. Στην περίπτωση αυτή, η διαδικασία ενημέρωσης δεν θα παρέμβει στην εργασία του χρήστη.

Όταν η ενημέρωση έκδοση του προϊόντος ολοκληρωθεί, ένα παράθυρο θα σας ενημερώσει για την επανεκκίνηση του συστήματος. Αν χάσετε αυτή την ειδοποίηση, μπορείτε είτε να κάνετε κλικ στο **Restart to upgrade** από τη γραμμή μενού ή να κάνετε επανεκκίνηση του συστήματος.

9.13.4. Εύρεση πληροφοριών σχετικά με το Bitdefender Antivirus for Mac

Για να βρείτε πληροφορίες για την έκδοση Bitdefender Antivirus for Mac που έχετε εγκαταστήσει, μεταβείτε στο παράθυρο **Περί** Στο ίδιο παράθυρο μπορείτε να δείτε τη Συμφωνία Συνδρομής, την Πολιτική Απορρήτου και Άδειες ανοιχτού κώδικα.

Για να αποκτήσετε πρόσβαση στο παράθυρο Περί:

1. Άνοιγμα Bitdefender Antivirus for Mac.
2. Κάντε κλικ στο κουμπί του Bitdefender Antivirus for Mac στη γραμμή μενού και επιλέξτε **Περί Antivirus για Mac**.

10. ΔΙΑΜΌΡΦΩΣΗ ΠΡΟΤΙΜΉΣΕΩΝ

Αυτό το κεφάλαιο περιλαμβάνει τα ακόλουθα θέματα:

10.1. Προτιμήσεις Πρόσβασης

Για να ανοίξετε το παράθυρο Προτιμήσεις του Bitdefender Antivirus for Mac :

1. Κάντε κάτι από τα εξής:
   - Πατήστε **Προτιμήσεις** στο μενού πλοήγησης του Bitdefender interface.
   - Κάντε κλικ στο κουμπί του Bitdefender Antivirus for Mac στη γραμμή μενού και επιλέξτε **Preferences**.

10.2. Προτιμήσεις Προστασίας

Το παράθυρο προτιμήσεις προστασία σας επιτρέπει να ρυθμίσετε τη συνολική προσέγγιση της σάρωσης. Μπορείτε να ρυθμίσετε τις δράσεις που θα γίνουν εάν ανιχνευτούν μολυσμένα και ύποπτα αρχεία και άλλες γενικές ρυθμίσεις.

- **Bitdefender Ασπίδα.** Η Bitdefender Ασπίδα παρέχει προστασία σε πραγματικό χρόνο από ένα ευρύ φάσμα απειλών, ελέγχοντας όλες τις εγκατεστημένες εφαρμογές, τις ενημερωμένες εκδόσεις τους και τα νέα και τροποποιημένα αρχεία. Δεν σας συνιστούμε να απενεργοποιήσετε την Bitdefender Ασπίδα, αλλά αν το κάνετε, κάντε το για όσο το δυνατόν λιγότερο χρόνο. Εάν η Bitdefender Ασπίδα είναι απενεργοποιημένη, δεν θα προστατεύεστε από απειλές .

- **Σάρωση μόνο νέων και τροποποιημένων αρχείων.** Επιλέξτε αυτό το πλαίσιο ελέγχου για να ρυθμίσετε το Bitdefender Antivirus for Mac για να ανιχνεύσει μόνο τα αρχεία που δεν έχουν σαρωθεί πριν ή που έχουν τροποποιηθεί από την τελευταία σάρωση τους.

Μπορείτε να επιλέξετε να μην εφαρμόσετε αυτήν τη ρύθμιση για προσαρμοσμένη και drag&drop σάρωση, διαγράφοντας το αντίστοιχο πλαίσιο ελέγχου.

- **Μη σάρωση περιεχομένου σε αντίγραφα ασφαλείας.** Επιλέξτε αυτό το πλαίσιο ελέγχου για να εξαιρέσετε αρχεία αντιγράφων ασφαλείας από τη σάρωση. Αν τα μολυσμένα αρχεία αποκατασταθεί σε μεταγενέστερο χρόνο, το Bitdefender Antivirus for Mac θα τους εντοπίσει αυτόματα και θα λάβει τα κατάλληλα μέτρα.

10.3. Προτιμήσεις Σάρωσης

Μπορείτε να επιλέξετε μια συνολική ενέργεια που πρέπει να ληφθεί για όλα τα θέματα και τα ύποπτα στοιχεία που βρέθηκαν κατά τη διάρκεια μιας διαδικασίας σάρωσης.

Ενέργεια για μολυσμένα αρχεία

Προσπαθήστε να καθαρίσετε ή να μεταφέρετε σε καραντίνα - Αν εντοπιστούν μολυσμένα αρχεία, η Bitdefender θα προσπαθήσει να τα καθαρίσει (να αφαιρέσει τον κακόβουλο κώδικα) ή να τα μετακινήσει στην καραντίνα.

Καμία ενέργεια - Δεν θα γίνει καμία ενέργεια στα αρχεία που εντοπίστηκαν.

Ενέργεια για ύποπτα αρχεία

Μετακίνηση αρχείων σε καραντίνα - Αν εντοπιστούν ύποπτα αρχεία, η Bitdefender θα τα μεταφέρει σε καραντίνα.

Καμία ενέργεια - Δεν θα γίνει καμία ενέργεια στα αρχεία που εντοπίστηκαν.

10.4. Ειδικές προσφορές

Όταν οι προσφορές είναι διαθέσιμες, το Bitdefender προϊόν έχει ρυθμιστεί να σας ειδοποιεί μέσω ενός αναδυόμενου παραθύρου. Αυτό σας δίνει την ευκαιρία να επωφεληθείτε από τις ευνοϊκές τιμές και να διατηρήσετε τις συσκευές προστατευμένες για μεγαλύτερο χρονικό διάστημα.

Για να ενεργοποιήσετε ή να απενεργοποιήσετε τις ειδοποιήσεις για ειδικές προσφορές:

1. Πατήστε **Προτιμήσεις** στο μενού πλοήγησης του Bitdefender interface.
2. Επιλέξτε την καρτέλα **Άλλα**.

3. Ενεργοποιήστε ή απενεργοποιήστε το διακόπτη **Οι προσφορές μου** .

Η επιλογή **Οι προσφορές μου** είναι ενεργοποιημένη από προεπιλογή.

11. VPN

Αυτό το κεφάλαιο περιλαμβάνει τα ακόλουθα θέματα:

11.1. Σχετικά με το VPN

Με το Bitdefender VPN μπορείτε να διατηρείτε τα προσωπικά σας δεδομένα ιδιωτικά κάθε φορά που συνδέεστε σε ασύρματα ασύρματα δίκτυα, ενώ βρίσκεστε σε αεροδρόμια, εμπορικά κέντρα, καφετέριες ή ξενοδοχεία. Με αυτόν τον τρόπο, ατυχείς καταστάσεις όπως η κλοπή προσωπικών δεδομένων, ή προσπαθείες κάποιου να καταστήσει τη διεύθυνση IP της συσκευής σας προσβάσιμη στους χάκερς, μπορεί να αποφευχθεί.

Το VPN χρησιμεύει ως σήραγγα μεταξύ της συσκευής σας και του δικτύου που συνδέετε για να εξασφαλίζετε τη σύνδεσή σας, κρυπτογραφώντας τα δεδομένα χρησιμοποιώντας κρυπτογράφηση τραπεζικής ποιότητας και αποκρύπτοντας τη διεύθυνση IP όπου κι αν βρίσκεστε. Η επισκεψιμότητά σας μεταφέρεται μέσω ενός ξεχωριστού διακομιστή. καθιστώντας έτσι τη συσκευή σας σχεδόν αδύνατη να ταυτοποιηθεί μέσω των μυριάδων άλλων συσκευών που χρησιμοποιούν τις υπηρεσίες μας. Επιπλέον, ενώ είστε συνδεδεμένοι στο διαδίκτυο μέσω του Bitdefender VPN, μπορείτε να αποκτήσετε πρόσβαση σε περιεχόμενο που συνήθως περιορίζεται σε συγκεκριμένες περιοχές.

Σημείωση

Ορισμένες χώρες ασκούν λογοκρισία στο Διαδίκτυο και ως εκ τούτου η χρήση των VPN στην επικράτειά τους έχει απαγορευτεί από το νόμο. Για να αποφύγετε νομικές συνέπειες, μπορεί να εμφανιστεί ένα προειδοποιητικό μήνυμα όταν επιχειρήσετε να χρησιμοποιήσετε την εφαρμογή Bitdefender VPN για πρώτη φορά. Συνεχίζοντας τη χρήση της εφαρμογής, επιβεβαιώνετε ότι γνωρίζετε τους ισχύοντες κανονισμούς των χωρών και τους κινδύνους στους οποίους ενδέχεται να εκτεθείτε.

11.2. Ανοίγοντας το VPN

Υπάρχουν τρεις τρόποι για να ανοίξετε την εφαρμογή Bitdefender VPN:

- Πατήστε **Privacy** στο μενού πλοήγησης του **Bitdefender interface**.

  Κάντε κλικ στο κουμπί **Άνοιγμα** στην κάρτα Bitdefender VPN.

- Κάντε κλικ στο εικονίδιο από τη γραμμή μενού.

- Μεταβείτε στο φάκελο Εφαρμογές , ανοίξτε το φάκελο Bitdefender και στη συνέχεια κάντε διπλό κλικ στο Bitdefender VPN .

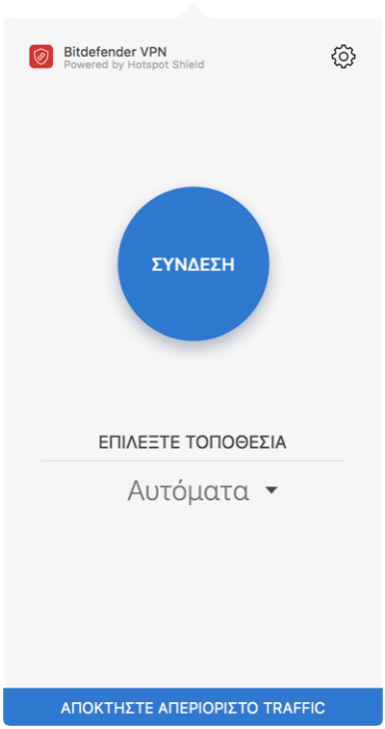
Την πρώτη φορά που θα ανοίξετε την εφαρμογή, θα σας ζητηθεί να επιτρέψετε στην Bitdefender να προσθέσει διαμορφώσεις. Επιτρέποντας στην Bitdefender να προσθέσει διαμορφώσεις, συμφωνείτε ότι όλες οι δραστηριότητες δικτύου της συσκευής σας μπορούν να φιλτραριστούν ή να ελεγχθούν όταν χρησιμοποιείτε την εφαρμογή VPN.

Σημείωση
Η εφαρμογή Bitdefender VPN μπορεί να εγκατασταθεί μόνο σε macOS Sierra (10.12.6), MacOS High Sierra (10.13.6) ή macOS Mojave (10.14 ή νεότερη).

11.3. Interface

Το παράθυρο του VPN εμφανίζει την κατάσταση της εφαρμογής, συνδεδεμένη ή αποσυνδεδεμένη. Η τοποθεσία του διακομιστή για χρήστες με τη δωρεάν έκδοση ορίζεται αυτόματα από την Bitdefender στον πιο κατάλληλο διακομιστή, ενώ οι premium χρήστες έχουν τη δυνατότητα να αλλάξουν την τοποθεσία του διακομιστή σε οποίο θέλουν να συνδεθούν επιλέγοντας τον από την λίστα **Εικονικές τοποθεσίες**. σχετικά με τις συνδρομές VPN, ανατρέξτε στο "*Συνδρομές*" (p. 262).

Για σύνδεση ή αποσύνδεση, κάντε κλικ στην κατάσταση που εμφανίζεται στο πάνω μέρος της οθόνης. Το εικονίδιο της γραμμής μενού εμφανίζεται μαύρο όταν το VPN είναι συνδεδεμένο και λευκό όταν αποσυνδεθεί το VPN.



VPN Interface

Κατά τη σύνδεση, ο χρόνος που παρήλθε εμφανίζεται στο κάτω μέρος του interface, Για να έχετε πρόσβαση σε περισσότερες επιλογές, κάντε κλικ στο ⚙ στην επάνω δεξιά πλευρά:

- **Ο λογαριασμός μου** - εμφανίζονται λεπτομέρειες σχετικά με τον Bitdefender λογαριασμό σας και τη συνδρομή VPN. Κάντε κλικ στην επιλογή **Αλλαγή λογαριασμού** , εάν θέλετε να συνδεθείτε με άλλον λογαριασμό.
- **Ρυθμίσεις** - ανάλογα με τις ανάγκες σας, μπορείτε να προσαρμόσετε τη συμπεριφορά του προϊόντος σας:
  - Ειδοποιήσεις
  - Ρυθμίστε το VPN για εκτέλεση κατά την εκκίνηση του συστήματος
  - Αναφορές προϊόντος

- Αυτόματη σύνδεση - που βρίσκεται στην καρτέλα **Για προχωρημένους** , αυτή η δυνατότητα σάς επιτρέπει να συνδέετε αυτόματα το Bitdefender VPN κάθε φορά που αποκτάτε πρόσβαση σε ένα μη ασφαλές ή δημόσιο Wi-Fi ή όταν ξεκινά μια εφαρμογή κοινής χρήσης αρχείων peer-to-peer.
- **Υποστήριξη** - μεταφέρεστε στην πλατφόρμα του Κέντρου υποστήριξης από όπου μπορείτε να διαβάσετε ένα χρήσιμο άρθρο σχετικά με τον τρόπο χρήσης του Bitdefender VPN.
- **Σχετικά με** - Εμφανίζονται πληροφορίες σχετικά με την εγκατεστημένη έκδοση.
- **Έξοδος** - έξοδος από την εφαρμογή.

11.4. Συνδρομές

Το Bitdefender VPN προσφέρει δωρεάν μια ημερήσια ποσόστωση κίνησης 200 MB ανά συσκευή για να εξασφαλίσει τη σύνδεσή σας κάθε φορά που χρειάζεστε και σας συνδέει αυτόματα με τη βέλτιστη τοποθεσία του server.

Για να έχετε απεριόριστη κίνηση και απεριόριστη πρόσβαση στο περιεχόμενο σε όλο τον κόσμο επιλέγοντας μια τοποθεσία διακομιστή σύμφωνα με τη βούλησή σας, αναβαθμίστε την έκδοση Premium.

Μπορείτε να πραγματοποιήσετε αναβάθμιση στην έκδοση Bitdefender Premium VPN ανά πάσα στιγμή κάνοντας κλικ στο κουμπί **Αναβάθμιση** που είναι διαθέσιμο στη διεπαφή του προϊόντος.

Η συνδρομή Bitdefender Premium VPN είναι ανεξάρτητη από τη Bitdefender Antivirus for Mac συνδρομή , πράγμα που σημαίνει ότι θα μπορείτε να το χρησιμοποιήσετε για ολόκληρη τη διαθεσιμότητα, ανεξάρτητα από την κατάσταση της συνδρομής κατά των ιών. Σε περίπτωση που λήξει η συνδρομή Bitdefender Premium VPN, αλλά το προϊόν για το Bitdefender Antivirus for Mac εξακολουθεί να είναι ενεργό, θα επανέλθετε στην ελεύθερη έκδοση.

Το Bitdefender VPN είναι προϊόν πολλαπλής πλατφόρμας, διαθέσιμο σε Bitdefender προϊόντα συμβατά με Windows, mac OS, Android και iOS. Μόλις αναβαθμίσετε στην premium έκδοση, να είστε σε θέση να χρησιμοποιήσετε τη συνδρομή σας σε όλα τα προϊόντα, υπό την προϋπόθεση ότι θα συνδεθείτε με τον ίδιο Bitdefender λογαριασμό.

12. BITDEFENDER CENTRAL

Αυτό το κεφάλαιο περιλαμβάνει τα ακόλουθα θέματα:

12.1. σχετικά με Bitdefender Central

Bitdefender Central είναι η πλατφόρμα όπου έχετε πρόσβαση στις λειτουργίες και τις υπηρεσίες του προϊόντος στο διαδίκτυο και μπορείτε να εκτελείτε εξ αποστάσεως σημαντικές εργασίες στις συσκευές Bitdefender που είναι εγκατεστημένες. Μπορείτε να συνδεθείτε στον Bitdefender λογαριασμό από οποιονδήποτε υπολογιστή ή κινητή συσκευή που συνδέεται στο Internet μέσω του https://central.bitdefender.com, ή απευθείας μέσω της Bitdefender Central εφαρμογής για Android και iOS συσκευές.

Για να εγκαταστήσετε την Bitdefender Centralεφαρμογή στις συσκευές σας:

- **Σε Android** - αναζητήστε Bitdefender Central στο Google Play και στη συνέχεια κατεβάστε και εγκαταστήστε την εφαρμογή. Ακολουθήστε τα απαιτούμενα βήματα για να ολοκληρώσετε την εγκατάσταση.
- **Σε iOS** - αναζητήστε Bitdefender Central στο App Store και στη συνέχεια κάντε λήψη και εγκατάσταση της εφαρμογής. Ακολουθήστε τα απαιτούμενα βήματα για να ολοκληρώσετε την εγκατάσταση.

Μόλις έχετε πρόσβαση, μπορείτε να αρχίσετε να κάνετε τα εξής:

- Λήψη και εγκατάσταση του Bitdefender σε Windows, macOS, iOS και σε Android λειτουργικά συστήματα. Τα προϊόντα που διατίθενται για λήψη είναι:
  - Bitdefender Antivirus for Mac
  - Η σειρά προϊόντων Bitdefender για Windows
  - Bitdefender Mobile Security για Android
  - Bitdefender Mobile Security για iOS
- Διαχειριστείτε και ανανεώστε τις Bitdefender συνδρομές σας.

- Προσθέστε νέες συσκευές στο δίκτυό σας και διαχειριστείτε τις από όπου κι αν βρίσκεστε.

12.2. Πρόσβαση στο Bitdefender Central

Υπάρχουν διάφοροι τρόποι για να αποκτήσετε πρόσβαση στο Bitdefender Central. Ανάλογα με την εργασία που θέλετε να εκτελέσετε, μπορείτε να χρησιμοποιήσετε οποιαδήποτε από τις ακόλουθες δυνατότητες:

- Από τη κεντρική διεπαφή του Bitdefender Antivirus for Mac:
  1. Κάντε κλικ στο **Go to your account** σύνδεσμο στο κάτω δεξιά μέρος της οθόνης.
- Από τον πλοηγό σας:
  1. Ανοίξτε ένα πρόγραμμα περιήγησης σε οποιαδήποτε συσκευή με πρόσβαση στο Διαδίκτυο.
  2. Μετάβαση σε: https://central.bitdefender.com.
  3. Συνδεθείτε στο λογαριασμό σας χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
- Από την συσκευή σας Android ή iOS:

  Ανοίξτε την Bitdefender Central εφαρμογή που έχετε εγκαταστήσει.

Σημείωση
Σε αυτό το υλικό έχουμε συμπεριλάβει τις επιλογές που μπορείτε να βρείτε στο web interface.

12.3. 2-Factor Authentication

Η μέθοδος 2-Factor Authentication προσθέτει ένα πρόσθετο επίπεδο ασφαλείας στον Bitdefenderλογαριασμό σας, απαιτώντας έναν κωδικό επαλήθευσης εκτός από τα διαπιστευτήριά σας σύνδεσης. Έτσι θα αποτρέψετε την υποκλοπή του λογαριασμού σας και θα προστατευτείτε από επιθέσεις.

Ενεργοποίηση 2-Factor Authentication

Ενεργοποιώντας το 2-Factor Authentication, ο Bitdefender λογαριασμός σας θα είναι πολύ πιο ασφαλής. Η ταυτότητά σας θα επαληθεύεται κάθε φορά που θα συνδεθείτε από διαφορετικές συσκευές,για να εγκαταστήσετε

ένα από τα Bitdefender προϊόντα, να ελέγξτε την κατάσταση της συνδρομής σας ή να εκτελέστε απομακρυσμένα εργασίες στις συσκευές σας.

Για να ενεργοποιήσετε το 2-Factor Authentication:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο εικονίδιο στην επάνω δεξιά πλευρά της οθόνης.
3. Κάντε κλικ στο **Bitdefender Λογαριασμός** στο μενού.
4. Επιλέξτε την καρτέλα **Κωδικός και ασφάλεια**
5. Κάντε κλικ στο κουμπί **ΕΝΑΡΞΗ ΤΩΡΑ**.

   Επιλέξτε μία από τις ακόλουθες μεθόδους:

   - **Εφαρμογή Authenticator** - χρησιμοποιήστε μια εφαρμογή ελέγχου ταυτότητας για να δημιουργήσετε έναν κωδικό κάθε φορά που θέλετε να συνδεθείτε στον Bitdefender λογαριασμό σας.

     Εάν θέλετε να χρησιμοποιήσετε μια εφαρμογή ελέγχου ταυτότητας, αλλά δεν είστε σίγουροι για το τι θα επιλέξετε, υπάρχει διαθέσιμη μια λίστα με τις εφαρμογές ελέγχου ταυτότητας που συστήνουμε.

     a. Κάντε κλικ στο κουμπί **ΧΡΗΣΙΜΟΠΟΙΗΣΤΕ ΤΗΝ ΕΦΑΡΜΟΓΗ AUTHENTICATOR** για να ξεκινήσετε.

     b. Για να συνδεθείτε σε μια συσκευή Android ή iOS, χρησιμοποιήστε τη συσκευή σας για να σαρώσετε τον QR κωδικό .

     Για να συνδεθείτε σε laptop ή επιτραπέζιο υπολογιστή, μπορείτε να προσθέσετε χειροκίνητα τον εμφανιζόμενο κώδικα.

     Κάντε κλικ στο **CONTINUE**.

     c. Εισάγετε τον κωδικό που παρέχεται από την εφαρμογή ή αυτόν που εμφανίστηκε στο προηγούμενο βήμα και στη συνέχεια πατήστε **ΕΝΕΡΓΟΠΟΙΗΣΗ** .

   - **E-mail** - κάθε φορά που συνδέεστε στο Bitdefender λογαριασμό σας, θα σταλεί στο εισερχόμενό σας email ένας κωδικός επαλήθευσης. Ελέγξτε το email και, στη συνέχεια, χρησιμοποιήστε τον κωδικό που λάβατε.

     a. Κάντε κλικ στο κουμπί **ΧΡΗΣΗ EMAIL** για να ξεκινήσετε.

     b. Ελέγξτε το email και πληκτρολογήστε τον κωδικό που λάβατε.

     c. Κάντε κλικ στο κουμπί **ΕΝΕΡΓΟΠΟΙΗΣΗ**.

Σε περίπτωση που θέλετε να σταματήσετε να χρησιμοποιείτε το 2-Factor Authentication:

1. Κάντε κλικ στο κουμπί **ΑΠΕΝΕΡΓΟΠΟΙΗΣΗ 2-FACTOR AUTHENTICATION**
2. Ελέγξτε την εφαρμογή ή το email σας και πληκτρολογήστε τον κωδικό που λάβατε.
3. Επιβεβαιώστε την επιλογή σας.

12.4. Προσθήκη έμπιστης συσκευής

Για να βεβαιωθείτε ότι μόνο εσείς μπορείτε να αποκτήσετε πρόσβαση στο Bitdefender λογαριασμό σας, ίσως χρειαστεί πρώτα έναν κωδικό ασφαλείας. Εάν θέλετε να παραλείψετε αυτό το βήμα κάθε φορά που συνδέεστε από την ίδια συσκευή, σας συνιστούμε να την ορίσετε ως αξιόπιστη συσκευή.

Για να δηλώσετε συσκευές ως αξιόπιστες:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο εικονίδιο 👤 στην επάνω δεξιά πλευρά της οθόνης.
3. Κάντε κλικ στο **Bitdefender Λογαριασμός** στο μενού.
4. Επιλέξτε την καρτέλα **Κωδικός και ασφάλεια**
5. Κάντε κλικ στην επιλογή **Έμπιστες Συσκευές**.
6. Εμφανίζεται η λίστα με τις συσκευές όπου το Bitdefender που είναι εγκατεστημένο. Κάντε κλικ στην επιθυμητή συσκευή.

Μπορείτε να προσθέσετε όσες συσκευές επιθυμείτε, υπό την προϋπόθεση ότι έχει εγκατασταθεί το Bitdefender και η συνδρομή σας είναι έγκυρη.

12.5. Δραστηριότητα

Στην περιοχή Δραστηριότητα έχετε πρόσβαση στις πληροφορίες σχετικά με τις συσκευές που έχουν εγκαταστήσει το Bitdefender.

Μόλις αποκτήσετε πρόσβαση στο παραθύρο **Δραστηριότητα**, θα είναι διαθέσιμες οι ακόλουθες κάρτες :

- **Οι συσκευές μου**. Εδώ μπορείτε να δείτε τον αριθμό των συνδεδεμένων συσκευών μαζί με την κατάσταση προστασίας τους. Για να διορθώσετε τα ζητήματα εξ αποστάσεως στις συσκευές που εντοπίστηκαν, κάντε κλικ στο κουμπί **Επίλυση προβλημάτων** και, στη συνέχεια, κάντε κλικ στο κουμπί **Σάρωση και επίλυση προβλημάτων**.

Για να δείτε λεπτομέρειες σχετικά με τα εντοπισμένα προβλήματα, κάντε κλικ στο **Προβολή προβλημάτων** .

Δεν είναι δυνατή η ανάκτηση πληροφοριών σχετικά με τις απειλές που ανιχνεύθηκαν σε iOS συσκευές.

- **Αποκλεισμένες απειλές**. Εδώ μπορείτε να δείτε ένα γράφημα που παρουσιάζει ένα συνολικό στατιστικό στοιχείο, συμπεριλαμβανομένων των πληροφοριών για τις απειλές που αποκλείστηκαν κατά τις τελευταίες 24 ώρες και επτά ημέρες. Οι πληροφορίες που εμφανίζονται ανακτώνται ανάλογα με την κακόβουλη συμπεριφορά που εντοπίζεται στα αρχεία, τις εφαρμογές και τις διευθύνσεις URL που αποκτήθηκε πρόσβαση.
- **Οι κορυφαίοι χρήστες με αποκλεισμένες απειλές**. Εδώ μπορείτε να δείτε τους χρήστες όπου βρέθηκαν οι περισσότερες απειλές.
- **Οι κορυφαίες συσκευές με αποκλεισμένες απειλές**. Εδώ μπορείτε να δείτε τις συσκευές όπου βρέθηκαν οι περισσότερες απειλές.

12.6. Οι Συνδρομές μου

Η Bitdefender Central πλατφόρμα σας δίνει τη δυνατότητα να διαχειριστείτε εύκολα τις συνδρομές που έχετε για όλες τις συσκευές σας.

12.6.1. Ενεργοποίηση συνδρομής

Μια συνδρομή μπορεί να ενεργοποιηθεί κατά τη διάρκεια της διαδικασίας εγκατάστασης χρησιμοποιώντας τον λογαριασμό σας Bitdefender. Μαζί με την διαδικασία ενεργοποίησης, η ισχύς της συνδρομής αρχίζει να μετρά αντίστροφα.

Αν έχετε αγοράσει ένα κωδικό ενεργοποίησης από έναν από τους μεταπωλητές μας ή σας τον έκαναν δώρο, τότε μπορείτε να προσθέσετε τη διάρκεια της συνδρομής στην δική σας Bitdefender συνδρομή.

Για να ενεργοποιήσετε μια συνδρομή χρησιμοποιώντας έναν κωδικό ενεργοποίησης, ακολουθήστε τα εξής βήματα:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο ☰ εικονίδιο που βρίσκεται στην επάνω αριστερή γωνία του παραθύρου και, στη συνέχεια, επιλέξτε το **Οι Συνδρομές μου** πάνελ.
3. Κάντε κλικ στο κουμπί **ΚΩΔΙΚΟΣ ΕΝΕΡΓΟΠΟΙΗΣΗΣ**, στη συνέχεια, πληκτρολογήστε τον κωδικό στο αντίστοιχο πεδίο.

4. Κάντε κλικ στο **ΕΝΕΡΓΟΠΟΙΗΣΗ** για να συνεχίσετε.

Η συνδρομή ενεργοποιήθηκε.

Για να ξεκινήσετε την εγκατάσταση του προϊόντος στις συσκευές σας, ανατρέξτε στο "*Εγκατάσταση του Bitdefender Antivirus for Mac*" (p. 227).

12.7. Οι συσκευές μου

Η περιοχή **Οι συσκευές μου** στον Bitdefender λογαριασμό σας, σας δίνει τη δυνατότητα να εγκαταστήσετε, να διαχειριστείτε και να ολοκληρώσετε ενέργειες εξ αποστάσεως στο Bitdefender προϊόν σας σε οποιαδήποτε συσκευή, υπό την προϋπόθεση ότι είναι ενεργοποιημένη και συνδεδεμένη στο Internet. Οι κάρτες συσκευής εμφανίζουν το όνομα της συσκευής, την κατάσταση προστασίας και αν υπάρχουν κίνδυνοι ασφαλείας που επηρεάζουν την προστασία των συσκευών σας.

12.7.1. Προσαρμόστε το προϊόν σας

Για να εντοπίσετε εύκολα τις συσκευές σας, μπορείτε να προσαρμόσετε το όνομα της συσκευής:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το **Οι συσκευές μου**.
3. Πατήστε την επιθυμητή κάρτα συσκευής και, στη συνέχεια, το εικονίδιο ⋮ στην επάνω δεξιά γωνία της οθόνης.
4. Επιλέξτε **Ρυθμίσεις**.
5. Πληκτρολογήστε ένα νέο όνομα στο πεδίο **Όνομα συσκευής** και, στη συνέχεια, επιλέξτε **ΑΠΟΘΗΚΕΥΣΗ**.

Μπορείτε να δημιουργήσετε και να ορίσετε έναν ιδιοκτήτη σε κάθε μία από τις συσκευές σας για καλύτερη διαχείριση:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το **Οι συσκευές μου**.
3. Πατήστε την επιθυμητή κάρτα συσκευής και, στη συνέχεια, το εικονίδιο ⋮ στην επάνω δεξιά γωνία της οθόνης.
4. Επιλέξτε **Προφίλ**.

5. Επιλέξτε **Προσθήκη κατόχου** και στη συνέχεια συμπληρώστε τα αντίστοιχα πεδία. Προσαρμόστε το προφίλ προσθέτοντας μια φωτογραφία, επιλέγοντας μια ημερομηνία γέννησης, να προσθέσετε μια email διεύθυνση και έναν τηλεφωνικό αριθμό.
6. Κάντε κλικ στο **ΠΡΟΣΘΗΚΗ** για να αποθηκεύσετε ένα προφίλ.
7. Επλέξτε τον επιθυμητό ιδιοκτήτη από τη λίστα **Ιδιοκτήτης συσκευής** και στη συνέχεια κάντε κλικ στο **ΑΝΤΙΣΤΟΙΧΙΣΗ**.

12.7.2. Ενέργειες εξ αποστάσεως

Για να ενημερώσετε εξ αποστάσεως το Bitdefender σε μια συσκευή:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το **Οι συσκευές μου**.
3. Πατήστε την επιθυμητή κάρτα συσκευής και, στη συνέχεια, το εικονίδιο ⋮ στην επάνω δεξιά γωνία της οθόνης.
4. Επιλέξτε **Αναβάθμιση**.

Μόλις κάνετε κλικ σε μια κάρτα συσκευής, οι ακόλουθες καρτέλες είναι διαθέσιμες:

- **Ταμπλώ**. Σε αυτό το παράθυρο μπορείτε να δείτε λεπτομέρειες σχετικά με την επιλεγμένη συσκευή, να ελέγξετε την κατάσταση προστασίας και πόσες απειλές έχουν αποκλειστεί τις τελευταίες επτά ημέρες. Η κατάσταση προστασίας μπορεί να είναι πράσινη, όταν δεν υπάρχει κανένα πρόβλημα που να επηρεάζει τη συσκευή σας, κίτρινη όταν η συσκευή σας χρειαστεί την προσοχή σας ή κόκκινη όταν η συσκευή κινδυνεύει. Όταν υπάρχουν ζητήματα που επηρεάζουν τη συσκευή σας, κάντε κλικ στο αναπτυσσόμενο βέλος στην επάνω περιοχή κατάστασης για να μάθετε περισσότερες λεπτομέρειες. Από εδώ μπορείτε να διορθώσετε χειροκίνητα ζητήματα που επηρεάζουν την ασφάλεια των συσκευών σας.
- **ΠΡΟΣΤΑΣΙΑ**. Από αυτό το παράθυρο μπορείτε να εκτελέσετε μια Σάρωση εξ αποστάσεως στη συσκευή σας. Κάντε κλικ στο κουμπί **ΣΑΡΩΣΗ** για να ξεκινήσει η διαδικασία. Μπορείτε επίσης να ελέγξετε πότε πραγματοποιήθηκε η τελευταία σάρωση στη συσκευή καθώς και μία διαθέσιμη αναφορά της τελευταίας σάρωσης με τις πιο σημαντικές πληροφορίες. Για περισσότερες πληροφορίες σχετικά με αυτές τις δύο διαδικασίες σάρωσης, ανατρέξτε στο *"Σάρωση του Mac σας"* (p. 239).

13. ΣΥΧΝΈΣ ΕΡΩΤΉΣΕΙΣ

Πώς μπορώ να δοκιμάσω το Bitdefender Antivirus for Mac πριν να αγοράσω μια συνδρομή;

Είστε ένας νέος πελάτης του Bitdefender και θα θέλατε να δοκιμάσετε το προϊόν μας πριν από την αγορά. Η δοκιμαστική περίοδος είναι 30 ημέρες και μπορείτε να συνεχίσετε να χρησιμοποιείτε το εγκατεστημένο προϊόν μόνο αν αγοράσετε μια Bitdefender συνδρομή. Για να δοκιμάσετε το Bitdefender Antivirus for Mac, θα πρέπει να:

1. Δημιουργήστε ένα Bitdefender λογαριασμό ακολουθώντας τα παρακάτω βήματα:
   a. Μετάβαση σε: https://central.bitdefender.com.
   b. Πληκτρολογήστε τις απαιτούμενες πληροφορίες στα αντίστοιχα πεδία. Τα δεδομένα που εισαγάγατε εδώ παραμένουν εμπιστευτικά.
   c. Πριν προχωρήσετε περαιτέρω, πρέπει να συμφωνήσετε με τους Όρους Χρήσης. Αποκτήστε πρόσβαση στους Όρους Χρήσης και διαβάστε προσεκτικά, καθώς περιέχουν τους όρους και τις προϋποθέσεις υπό τις οποίες μπορείτε να χρησιμοποιήσετε Bitdefender.

      Επιπλέον, μπορείτε να έχετε πρόσβαση και να διαβάσετε την Πολιτική Απορρήτου.
   d. Πατήστε στο **ΔΗΜΙΟΥΡΓΙΑ ΛΟΓΑΡΙΑΣΜΟΥ**.
2. Κατεβάστε το Bitdefender Antivirus for Mac ως εξής:
   a. Επιλέξτε το **Οι συσκευές μου** και στην συνέχεια κάντε κλικ **ΕΓΚΑΤΑΣΤΑΣΗ ΠΡΟΣΤΑΣΙΑΣ** .
   b. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:
      - **Προστατέψτε αυτή τη συσκευή**
        i. Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.
        ii. Αποθηκεύστε το αρχείο εγκατάστασης.
      - **Προστασία άλλων συσκευών**

i. Επιλέξτε αυτήν την επιλογή και στη συνέχεια επιλέξτε τον κάτοχο της συσκευής. Εάν η συσκευή ανήκει σε κάποιον άλλο, κάντε κλικ στο αντίστοιχο κουμπί.

ii. Επιλέξτε **ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΛΗΨΗΣ**.

iii. Πληκτρολογήστε μια διεύθυνση ηλεκτρονικού ταχυδρομείου στο αντίστοιχο πεδίο και κάντε κλικ στην επιλογή **ΑΠΟΣΤΟΛΗ EMAIL** .

Λάβετε υπόψη ότι ο παραγόμενος σύνδεσμος λήψης ισχύει μόνο για τις επόμενες 24 ώρες. Εάν λήξει ο σύνδεσμος, θα πρέπει να δημιουργήσετε ένα νέο, ακολουθώντας τα ίδια βήματα.

iv. Στην συσκευή που θέλετε να εγκαταστήσετε το Bitdefender προιόν, ελέγξτε το λογαριασμό ηλεκτρονικού ταχυδρομείου που πληκτρολογήσατε και στην συνέχεια κάντε κλικ στο αντίστοιχο κουμπί λήψης.

c. Εκτελέστε το Bitdefender προϊόν που έχετε κατεβάσει.

Εχω έναν κωδικό ενεργοποίησης. Πώς μπορώ να προσθέσω το ημέρες διάρκειας στην συνδρομή μου;

Αν έχετε αγοράσει ένα κωδικό ενεργοποίησης από έναν από τους μεταπωλητές μας ή σας τον έκαναν δώρο, τότε μπορείτε να προσθέσετε τη διάρκεια της συνδρομής στην δική σας Bitdefender συνδρομή.

Για να ενεργοποιήσετε μια συνδρομή χρησιμοποιώντας έναν κωδικό ενεργοποίησης, ακολουθήστε τα εξής βήματα:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο εικονίδιο που βρίσκεται στην επάνω αριστερή γωνία του παραθύρου και, στη συνέχεια, επιλέξτε το **Οι Συνδρομές μου** πάνελ.
3. Κάντε κλικ στο κουμπί **ΚΩΔΙΚΟΣ ΕΝΕΡΓΟΠΟΙΗΣΗΣ**, στη συνέχεια, πληκτρολογήστε τον κωδικό στο αντίστοιχο πεδίο.
4. Κάντε κλικ στο **ΕΝΕΡΓΟΠΟΙΗΣΗ** για να συνεχίσετε.

Η επέκταση είναι ορατή τώρα στο Bitdefender λογαριασμό σας, και στο εγκατεστημένο προϊόν σας Bitdefender Antivirus for Mac, στο κάτω δεξιά μέρος της οθόνης.

Το αρχείο καταγραφής της σάρωσης δείχνει ότι υπάρχουν ακόμα άλυτα θέματα. Πώς μπορώ να τα αφαιρέσω;

Τα εκκρεμή στοιχεία στο αρχείο καταγραφής της σάρωσης μπορεί να είναι:

- αρχεία με περιορισμένη πρόσβαση (xar, rar, κλπ)

  Λύση: Χρησιμοποιήστε την επιλογή **Reveal in Finder** για να βρείτε το αρχείο και να το διαγράψετε χειροκίνητα για να βρείτε το αρχείο και να το διαγράψετε χειροκίνητα Φροντίστε να αδειάσετε και τον κάδο απορριμμάτων.

- mailboxes με περιορισμένη πρόσβαση (Thunderbird, κλπ)

  Λύση: Χρησιμοποιήστε την εφαρμογή για να καταργήσετε την καταχώρηση που περιέχει το μολυσμένο αρχείο.

- Περιεχόμενο σε αντίγραφα ασφαλείας

  Επίλυση: Ενεργοποιήστε την επιλογή **Μην σαρώνετε περιεχόμενο σε αντίγραφα ασφαλείας** στις προτιμήσεις προστασίας ή **Προσθήκη στις εξαιρέσεις** των αρχείων που ανιχνεύτηκαν.

  Αν τα μολυσμένα αρχεία αποκατασταθεί σε μεταγενέστερο χρόνο, το Bitdefender Antivirus for Mac θα τους εντοπίσει αυτόματα και θα λάβει τα κατάλληλα μέτρα.

  Σημείωση
  Περιορισμένη πρόσβαση σε αρχεία σημαίνει αρχεία του Bitdefender Antivirus for Mac μπορεί μόνο να ανοίξει, αλλά δεν μπορεί να τα τροποποιήσει.

Πού μπορώ να δω τις λεπτομέρειες σχετικά με τη δραστηριότητα της εφαρμογής;

Το Bitdefender διατηρεί ένα αρχείο καταγραφής όλων των σημαντικών ενεργειών, αλλαγών κατάστασης και άλλων κρίσιμων μηνυμάτων που σχετίζονται με την δραστηριότητα του. Για να αποκτήσετε πρόσβαση σε αυτές τις πληροφορίες, Επιλέξτε **Ειδοποιήσεις** στο μενού πλοήγησης στο Bitdefender interface.

Μπορώ να ενημερώσω το Bitdefender Antivirus for Mac μέσω ενός Proxy Server?

Το Bitdefender Antivirus for Mac μπορεί να παίρνει ενημερώσεις μόνο μέσω proxy servers που δεν απαιτούν έλεγχο ταυτότητας. Δεν χρειάζεται να διαμορφώσετε τις ρυθμίσεις του προγράμματος.

Εάν συνδέεστε στο Internet μέσω ενός proxy server που απαιτεί έλεγχο ταυτότητας, θα πρέπει να μεταβείτε σε απευθείας σύνδεση με το Διαδίκτυο τακτικά προκειμένου να λάβετε τις ενημερώσεις.

Πώς μπορώ να απεγκαταστήσω το Bitdefender Antivirus for Mac;

Για να αφαιρέσετε το Bitdefender Antivirus for Mac, ακολουθήστε τα εξής βήματα:

1. Ανοίξτε ένα παράθυρο **Finder** και, στη συνέχεια, μεταβείτε στο φάκελο Εφαρμογές.
2. Ανοίξτε τον Bitdefender φάκελο και, στη συνέχεια, κάντε διπλό κλικ στο στοιχείο Απεγκατάσταση Bitdefender.
3. Κάντε κλικ στο κουμπί **Απεγκατάσταση** και περιμένετε να ολοκληρωθεί η διαδικασία.
4. Κάντε κλικ στο **Κλείσιμο** για να τελειώσει.

Σημαντικό

Αν υπάρχει κάποιο λάθος, μπορείτε να επικοινωνήσετε με την Bitdefender Εξυπηρέτηση Πελατών, όπως περιγράφεται στο "Επικοινωνήστε μαζί μας" (p. 344).

Πώς μπορώ να καταργήσω τις επεκτάσεις TrafficLight από τον web browser μου;

- Για να αφαιρέσετε τις επεκτάσεις TrafficLight από τον Mozilla Firefox, ακολουθήστε τα εξής βήματα:
  1. Πηγαίνετε στο **Tools** και επιλέξτε **Add-ons**.
  2. Επιλέξτε **Extensions** στην αριστερή στήλη.
  3. Επιλέξτε την επέκταση και κάντε κλικ στο **Remove**.
  4. Κάντε επανεκκίνηση του προγράμματος περιήγησης για να ολοκληρωθεί η διαδικασία αφαίρεσης.
- Για να αφαιρέσετε τις επεκτάσεις TrafficLight από τον Mozilla Firefox, ακολουθήστε τα εξής βήματα:

1. Από πάνω δεξιά, επιλέξτε **Περισσότερα** .
2. Μεταβείτε στο **Περισσότερα εργαλεία** και επιλέξτε **Επεκτάσεις** .
3. Κάντε κλικ στο **Κατάργηση...** εικονίδιο δίπλα στην επέκταση που θέλετε να καταργήσετε.
4. Επιλέξτε **Αφαίρεση** για να επιβεβαιώσετε τη διαδικασία κατάργησης.

- Για να αφαιρέσετε το Bitdefender TrafficLight απο το Safari, ακολουθήστε τα παρακάτω βήματα:
  1. Μεταβείτε στις **Ρυθμίσεις** ή επιλέξτε **Command-Comma(,)**.
  2. Επιλέξτε **Επεκτάσεις**.

     Εμφανίζεται μια λίστα με τις εγκατεστημένες επεκτάσεις.
  3. Επιλέξτε την επέκταση Bitdefender TrafficLight και, στη συνέχεια, κάντε κλικ στο κουμπί **Κατάργηση εγκατάστασης** .
  4. Κάντε κλικ **Απεγκατάσταση** για να επιβεβαιώσετε τη διαδικασία κατάργησης.

Πότε πρέπει να χρησιμοποιήσω το Bitdefender VPN;

Πρέπει να είστε προσεκτικοί κατά την πρόσβαση, κατά το upload ή download περιεχόμενου στο Internet. Για να είστε ασφαλείς κατά την περιήγηση στον ιστό, σας συνιστούμε να χρησιμοποιήσετε το VPN Bitdefender όταν:

- θέλετε να συνδεθείτε με δημόσια ασύρματα δίκτυα
- θέλετε να αποκτήσετε πρόσβαση σε περιεχόμενο που κανονικά είναι περιορισμένο σε συγκεκριμένες περιοχές, ανεξάρτητα από το αν είστε στο εσωτερικό ή στο εξωτερικό
- θέλετε να διατηρήσετε τα προσωπικά σας δεδομένα ιδιωτικά (ονόματα χρήστη, κωδικοί πρόσβασης, πληροφορίες πιστωτικής κάρτας κ.λπ.)
- θέλετε να αποκρύψετε τη IP διεύθυνση σας

Θα επηρεάσει αρνητικά το Bitdefender VPN τη διάρκεια ζωής της μπαταρίας της συσκευής μου;

Το Bitdefender VPN έχει σχεδιαστεί για να προστατεύει τα προσωπικά σας δεδομένα, να αποκρύπτει την IP διεύθυνση σας ενώ είναι συνδεδεμένο σε μη ασφαλή ασύρματα δίκτυα και να έχει πρόσβαση σε περιορισμένο περιεχόμενο σε ορισμένες χώρες. Συστήνουμε να χρησιμοποιήσετε το VPN μόνο όταν το χρειάζεστε καινα το αποσυνδέετε όταν είστε εκτός σύνδεσης.

Γιατί αντιμετωπίζω την επιβράδυνση του Διαδικτύου όταν συνδέεται με το Bitdefender VPN;

Το Bitdefender VPN έχει σχεδιαστεί για να σας προσφέρει μια ελαφριά εμπειρία κατά την πλοήγηση στο διαδίκτυο, Παρόλα αυτά, η σύνδεση στο διαδίκτυο ή η απόσταση από τον server στον οποίο συνδέεστε μπορεί να προκαλέσει επιβράδυνση. για να συνδεθείτε από τη θέση σας σε έναν απομακρυσμένο φιλοξενούμενο server (π.χ. από την Αμερική στην Κίνα), σας συνιστούμε να επιτρέψετε στο Bitdefender VPN να σας συνδέσει αυτόματα στον πλησιέστερο διακομιστή ή να βρείτε ένα server πιο κοντά στην τρέχουσα τοποθεσία σας.

MOBILE SECURITY ΓΙΑ IOS

14. ΤΙ ΕΊΝΑΙ ΤΟ BITDEFENDER MOBILE SECURITY FOR IOS

Οι δραστηριότητες στο διαδίκτυο, όπως η πληρωμή λογαριασμών, η πραγματοποίηση κρατήσεων για διακοπές ή η αγορά αγαθών και υπηρεσιών είναι βολικές και χωρίς προβλήματα. Όμως, καθώς πολλές δραστηριότητες εξελίχθηκαν στο διαδίκτυο, και αν παρακαμφθούν τα μέτρα ασφαλείας, υπάρχει κίνδυνος παραβίασης των προσωπικών δεδομένων. Και τι είναι πιο σημαντικό από την προστασία των δεδομένων που είναι αποθηκευμένα σε ηλεκτρονικούς λογαριασμούς και στο προσωπικό smartphone;

Το Bitdefender Mobile Security for iOS σας επιτρέπει να:

- Προστατέψτε τα δεδομένα σας κατά τη χρήση ασύρματων ασύρματων δικτύων.
- Μείνετε ενήμεροι για τους κακόβουλους ιστότοπους και domains όταν είστε συνδεδεμένοι στο διαδίκτυο.
- Ελέγξτε εάν έχουν σημειωθεί τυχόν διαρροές στους ηλεκτρονικούς λογαριασμούς που χρησιμοποιείτε καθημερινά.

Το Bitdefender Mobile Security for iOS διανέμεται δωρεάν και απαιτεί ενεργοποίηση με ένα Bitdefender λογαριασμό.

15. ΞΕΚΙΝΏΝΤΑΣ

Απαιτήσεις Συσκευής

ο Bitdefender Mobile Security for iOS λειτουργεί σε οποιαδήποτε iOS 11.2 συσκευή και χρειάζεται μια ενεργή σύνδεση στο διαδίκτυο για να ενεργοποιηθεί και ανιχνεύει εάν έχει σημειωθεί διαρροή δεδομένων στους λογαριασμούς σας στο διαδίκτυο.

Εγκατάσταση του Bitdefender Mobile Security for iOS

- **Απο το Bitdefender Central**
  - Σε iOS
    1. Πρόσβαση στο Bitdefender Central.
    2. Πατήστε στο ☰ ιεικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι Συσκευές μου**.
    3. Επιλέξτε **ΕΓΚΑΤΑΣΤΑΣΗ ΠΡΟΣΤΑΣΙΑΣ** και, στη συνέχεια, πατήστε **Προστατέψτε αυτή τη συσκευή** .
    4. Επιλέξτε τον κάτοχο της συσκευής. Αν η συσκευή ανήκει σε κάποιον άλλο, πατήστε το αντίστοιχο κουμπί.
    5. Θα μεταφερθείτε στην **App Store** εφαρμογή. Στην οθόνη του App Store, πατήστε την επιλογή εγκατάστασης.
  - Σε Windows, macOS, Android
    1. Πρόσβαση στο Bitdefender Central.
    2. Πατήστε στο ☰ ιεικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι συσκευές μου**.
    3. Επιλέξτε **ΕΓΚΑΤΑΣΤΑΣΗ ΠΡΟΣΤΑΣΙΑΣ** και, στη συνέχεια, πατήστε **Προστατέψτε άλλες συσκευές** .
    4. Επιλέξτε τον κάτοχο της συσκευής. Αν η συσκευή ανήκει σε κάποιον άλλο, πατήστε το αντίστοιχο κουμπί.
    5. Επιλέξτε **ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΕΓΚΑΤΑΣΤΑΣΗΣ**.
    6. Πληκτρολογήστε μια email διεύθυνση στο αντίστοιχο πεδίο και πατήστε **ΑΠΟΣΤΟΛΗ EMAIL** Λάβετε υπόψη ότι ο παραγόμενος σύνδεσμος λήψης ισχύει μόνο για τις επόμενες 24 ώρες. Εάν λήξει

ο σύνδεσμος, θα πρέπει να δημιουργήσετε ένα νέο, ακολουθώντας τα ίδια βήματα.

7. Στη συσκευή που θέλετε να εγκαταστήσετε το Bitdefender, ελέγξτε το λογαριασμό ηλεκτρονικού ταχυδρομείου που πληκτρολογήσατε και κάντε κλικ στο αντίστοιχο κουμπί λήψης.

- **Από το App Store**

  Αναζητήστε το Bitdefender Mobile Security for iOS για να εντοπίσετε και να εγκαταστήσετε την εφαρμογή.

Ένας οδηγός εισαγωγής που περιέχει λεπτομέρειες σχετικά με τις λειτουργίες του προϊόντος εμφανίζεται την πρώτη φορά που ανοίγετε την εφαρμογή. Πατήστε **Ξεκινήστε** για να συνεχίσετε.

Πριν περάσετε από τα βήματα επικύρωσης, πρέπει να συμφωνήσετε με τη Συμφωνία Συνδρομής. Αφιερώστε λίγο χρόνο για να διαβάσετε τη Συμφωνία Συνδρομής επειδή περιέχει τους όρους και τις προϋποθέσεις κάτω από τις οποίες μπορείτε να χρησιμοποιήσετε το Bitdefender Mobile Security for iOS.

Επιλέξτε **Συνέχεια** για να μεταβείτε στο επόμενο παράθυρο.

Συνδεθείτε στον Bitdefender λογαριασμό σας

Για να χρησιμοποιήσετε το Bitdefender Mobile Security for iOS, πρέπει να συνδέσετε τη συσκευή σας με ένα Bitdefender λογαριασμό, Facebook, Google, Apple ή Microsoft, συνδεόμενοι στο λογαριασμό από την εφαρμογή. Την πρώτη φορά που ανοίγετε την εφαρμογή, θα σας ζητηθεί να συνδεθείτε σε έναν λογαριασμό.

Για να συνδέσετε τη συσκευή με το Bitdefender λογαρισμό:

1. Πληκτρολογήστε την email του Bitdefender account σας στο αντίστοιχο πεδίο και στη συνέχεια πατήστε **ΕΠΟΜΕΝΟ** . Εάν δεν έχετε Bitdefender λογαριασμό και θέλετε να δημιουργήσετε ένα , επιλέξτε τον αντίστοιχο σύνδεσμο και ακολουθήστε τις οδηγίες στην οθόνη μέχρι να ενεργοποιηθεί ο λογαριασμός.

   Για να συνδεθείτε χρησιμοποιώντας ένα Facebook, Google, Apple ή Microsoft λογαριασμό, επιλέξτε την υπηρεσία που θέλετε να χρησιμοποιήσετε από την περιοχή **Ή ΣΥΝΔΕΘΕΙΤΕ ΜΕ** . την επιλεγμένη υπηρεσία. Ακολουθήστε τις οδηγίες για να συνδέσετε το λογαριασμό σας με το Bitdefender Mobile Security for iOS.

Σημείωση
Το Bitdefender δεν πρόκειται να αποκτήσει πρόσβαση σε οποιαδήποτε εμπιστευτική πληροφορία όπως τον κωδικό πρόσβασης του λογαριασμού που χρησιμοποιείτε για την σύνδεση ή τις προσωπικές πληροφορίες των φίλων σας και των επαφών σας.

2. Εισάγετε τον κωδικό πρόσβασης και στη συνέχεια κάντε κλικ στο **ΣΥΝΔΕΣΗ**.

   Από εδώ μπορείτε επίσης να έχετε πρόσβαση στην Bitdefender Πολιτική Απορρήτου .

Ταμπλό

Πατήστε στο εικονίδιο Bitdefender Mobile Security for iOS στο πάνω μέρος της εφαρμογής της συσκευής σας για να ανοίξει το interface της εφαρμογής.

Την πρώτη φορά που θα αποκτήσετε πρόσβαση στην εφαρμογή, θα σας ζητηθεί να επιτρέψετε στο Bitdefender να σας στείλει ειδοποιήσεις. Πατήστε **Επιτρέπω** για να ενημερώνεστε κάθε φορά που το Bitdefender σάς κοινοποιεί κάτι σχετικό με την εφαρμογή σας. Για να διαχειριστείτε τις ειδοποιήσεις του Bitdefender, μεταβείτε στην περιοχή Ρυθμίσεις > Ειδοποιήσεις >Mobile Security.

Για να αποκτήσετε πρόσβαση στις πληροφορίες που χρειάζεστε, πατήστε το αντίστοιχο εικονίδιο στο κάτω μέρος της οθόνης.

VPN

Διατηρήστε το ιδιωτικό σας απόρρητο, ανεξάρτητα από το δίκτυο στο οποίο είστε συνδεδεμένοι, διατηρώντας κρυπτογραφημένη την επικοινωνία σας στο διαδίκτυο. Για περισσότερες πληροφορίες, ανατρέξτε στην “*VPN*” (p. 283).

ΠΡΟΣΤΑΣΙΑ Web

Παραμείνετε ασφαλείς κατά την πλοήγησή σας στο διαδίκτυο για την περίπτωση που λιγότερο ασφαλείς εφαρμογές προσπαθήσουν να αποκτήσουν πρόσβαση σε μη αξιόπιστα domains. Για περισσότερες πληροφορίες, ανατρέξτε στην “*ΠΡΟΣΤΑΣΙΑ Web*” (p. 286).

Ιδιωτικότητα του λογαριασμού

Μάθετε αν οι email λογαριασμοί σας έχουν διαρρεύσει ή όχι. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Ιδιωτικότητα του λογαριασμού"* (p. 289).

Για να δείτε πρόσθετες επιλογές, αγγίξτε το εικονίδιο ••• στη συσκευή σας ενώ βρίσκεστε στην αρχική οθόνη της εφαρμογής. Οι ακόλουθες επιλογές είναι διαθέσιμες:

- **Επαναφορά αγορών** - από εδώ μπορείτε να επαναφέρετε τις προηγούμενες συνδρομές που έχετε αγοράσει μέσω του λογαριασμού σας iTunes.
- **Ρυθμίσεις** - από εδώ έχετε πρόσβαση σε:
  - **Ρυθμίσεις VPN**
    - **Συμφωνία** - μπορείτε να διαβάσετε τους όρους υπό τους οποίους χρησιμοποιείτε την υπηρεσία Bitdefender VPN. Αν πατήσετε **δεν συμφωνώ πλέον**, δεν θα μπορείτε να χρησιμοποιήσετε το Bitdefender VPN τουλάχιστον μέχρι να πατήσετε **Συμφωνώ**.
    - **Άνοιγμα προειδοποίησης Wi-Fi** - μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε την ειδοποίηση προϊόντος που εμφανίζεται κάθε φορά που συνδέεστε σε ένα μη ασφαλές δίκτυο Wi-Fi. Ο λόγος της συγκεκριμένης ειδοποίησης είναι ώστε να σας βοηθήσουν να διατηρήσετε τα δεδομένα σας ιδιωτικά και ασφαλή χρησιμοποιώντας το Bitdefender VPN.
  - **Ρυθμίσεις προστασίας ιστού**
    - **Συμφωνία** - μπορείτε να διαβάσετε τους όρους υπό τους οποίους χρησιμοποιείτε την υπηρεσία Bitdefender Web Protection. Αν πατήσετε **δεν συμφωνώ πλέον**, δεν θα μπορείτε να χρησιμοποιήσετε το Bitdefender VPN τουλάχιστον μέχρι να πατήσετε **Συμφωνώ**.
    - **Ενεργοποίηση ειδοποίησης προστασίας ιστού** - Σας ειδοποιεί ότι η Προστασία ιστού μπορεί να ενεργοποιηθεί μετά την ολοκλήρωση μιας περιόδου σύνδεσης VPN.
  - Αναφορές προϊόντος
- **Ανατροφοδότηση** - εκκινεί το προεπιλεγμένο πρόγραμμα ηλεκτρονικού ταχυδρομείου από όπου μπορείτε να μας στείλετε τα σχόλιά σας σχετικά με την εφαρμογή.

- **Πληροφορίες σχετικά με την εφαρμογή** - από εδώ, έχετε πρόσβαση σε πληροφορίες σχετικά με την εγκατεστημένη έκδοση και τη Συμφωνία συνδρομής, την Πολιτική Απορρήτου και Αδειών χρήσης ανοιχτού κώδικα.

16. VPN

Με το Bitdefender VPN μπορείτε να διατηρείτε τα προσωπικά σας δεδομένα ιδιωτικά κάθε φορά που συνδέεστε σε ασύρματα ασύρματα δίκτυα, ενώ βρίσκεστε σε αεροδρόμια, εμπορικά κέντρα, καφετέριες ή ξενοδοχεία. Με αυτόν τον τρόπο, ατυχείς καταστάσεις όπως η κλοπή προσωπικών δεδομένων, ή προσπαθείες κάποιου να καταστήσει τη διεύθυνση IP της συσκευής σας προσβάσιμη στους χάκερς, μπορεί να αποφευχθεί.

Το VPN χρησιμεύει ως σήραγγα μεταξύ της συσκευής σας και του δικτύου που συνδέετε για να εξασφαλίζετε τη σύνδεσή σας, κρυπτογραφώντας τα δεδομένα χρησιμοποιώντας κρυπτογράφηση τραπεζικής ποιότητας και αποκρύπτοντας τη διεύθυνση IP όπου κι αν βρίσκεστε. Η επισκεψιμότητά σας μεταφέρεται μέσω ενός ξεχωριστού διακομιστή. καθιστώντας έτσι τη συσκευή σας σχεδόν αδύνατη να ταυτοποιηθεί μέσω των μυριάδων άλλων συσκευών που χρησιμοποιούν τις υπηρεσίες μας. Επιπλέον, ενώ είστε συνδεδεμένοι στο διαδίκτυο μέσω του Bitdefender VPN, μπορείτε να αποκτήσετε πρόσβαση σε περιεχόμενο που συνήθως περιορίζεται σε συγκεκριμένες περιοχές.

Σημείωση

Η Κίνα, το Ιράκ, τα Ηνωμένα Αραβικά Εμιράτα, η Τουρκία, η Λευκορωσία, το Ομάν, το Ιράν και η Ρωσία ασκούν λογοκρισία στο internet και ως εκ τούτου η χρήση του VPN στην επικράτειά τους έχει απαγορευτεί από το νόμο. Για αυτό το λόγο, το Bitdefender VPN δεν θα είναι διαθέσιμο στην επικράτειά τους.

Για να ενεργοποιήσετε το Bitdefender VPN:

1. Επιλέξτε το εικονίδιο στο κάτω μέρος της οθόνης.
2. Επιλέξτε **Σύνδεση** κάθε φορά που θέλετε να παραμείνετε προστατευμένοι ενώ είστε συνδεδεμένοι σε μη ασφαλή ασύρματα δίκτυα.

   Επιλέξτε **Αποσύνδεση** όποτε θέλετε να απενεργοποιήσετε τη σύνδεση.

Σημείωση

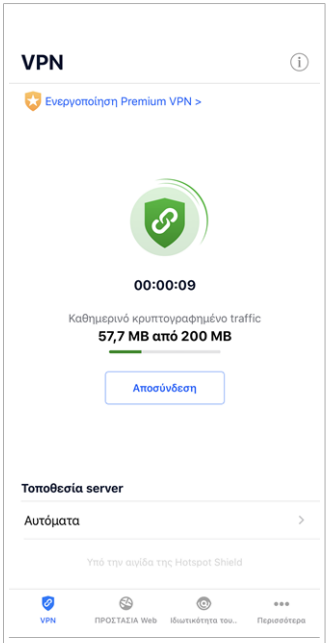
Την πρώτη φορά που θα ενεργοποιήσετε το VPN, θα σας ζητηθεί να επιτρέψετε στο Bitdefender να ρυθμίσει τις παραμέτρους VPN που θα παρακολουθούν την κυκλοφορία δικτύου. Πατήστε **Επιτρέπω** για να συνεχίσετε. Εάν έχει οριστεί μέθοδος ελέγχου ταυτότητας (δακτυλικό

αποτύπωμα ή κωδικός PIN) για την προστασία του smartphone σας, πρέπει να το χρησιμοποιήσετε.

Το εικονίδιο VPN εμφανίζεται στη γραμμή κατάστασης όταν είναι ενεργό το VPN.

Για να εξοικονομήσετε ενέργεια από τη μπαταρία, σας συνιστούμε να απενεργοποιήσετε το VPN όταν δεν το χρειάζεστε.

Εάν έχετε premium συνδρομή και επιθυμείτε να συνδεθείτε χειροκίνητα με ένα server, επιλέξτε **Αυτόματα** στην οθόνη του VPN και, στη συνέχεια, επιλέξτε τη τοποθεσία που θέλετε. σχετικά με τις συνδρομές VPN, ανατρέξτε στο "*Συνδρομές*" (p. 284).



VPN

16.1. Συνδρομές

Το Bitdefender VPN προσφέρει δωρεάν μια ημερήσια quota κίνησης 200 MB ανά συσκευή για να εξασφαλίσει τη σύνδεσή σας κάθε φορά που χρειάζεστε και σας συνδέει αυτόματα με τη βέλτιστη τοποθεσία του server.

Για να έχετε απεριόριστη κίνηση και απεριόριστη πρόσβαση στο περιεχόμενο σε όλο τον κόσμο επιλέγοντας μια τοποθεσία διακομιστή σύμφωνα με τη βούλησή σας, αναβαθμίστε την έκδοση Premium.

Μπορείτε να αναβαθμίσετε ανά πάσα στιγμή στην έκδοση Bitdefender Premium VPN πατώντας το κουμπί **ΑΝΑΒΑΘΜΙΣΤΕ ΣΕ PREMIUM VPN** που είναι διαθέσιμο στο παράθυρο VPN. Υπάρχουν δύο τύποι συνδρομών για να επιλέξετε: ετήσια και μηνιαία.

Η συνδρομή Bitdefender Premium VPN είναι ανεξάρτητη από τη Bitdefender Mobile Security for iOS συνδρομή , πράγμα που σημαίνει ότι θα μπορείτε να το χρησιμοποιήσετε για ολόκληρη τη διαθεσιμότητα. Σε περίπτωση που λήξει η συνδρομή Bitdefender Premium VPN θα επανέλθετε στην ελεύθερη έκδοση.

Το Bitdefender VPN είναι προϊόν πολλαπλής πλατφόρμας, διαθέσιμο σε Bitdefender προϊόντα συμβατά με Windows, mac OS, Android και iOS. Μόλις αναβαθμίσετε στην premium έκδοση, να είστε σε θέση να χρησιμοποιήσετε τη συνδρομή σας σε όλα τα προϊόντα, υπό την προϋπόθεση ότι θα συνδεθείτε με τον ίδιο Bitdefender λογαριασμό.

17. ΠΡΟΣΤΑΣΙΑ WEB

Η Bitdefender Προστασία Web εξασφαλίζει μια ασφαλή εμπειρία περιήγησης ειδοποιώντας σας σχετικά με πιθανές κακόβουλες ιστοσελίδες και όταν λιγότερο ασφαλείς εγκατεστημένες εφαρμογές θα προσπαθήσουν να αποκτήσουν πρόσβαση σε μη αξιόπιστα domains.

Όταν μια διεύθυνση URL δείχνει σε έναν γνωστό ιστότοπο ηλεκτρονικού "ψαρέματος" (phishing) ή παράνομο περιεχόμενο ή σε κακόβουλο περιεχόμενο όπως spyware ή ιούς, η ιστοσελίδα αποκλείεται και εμφανίζεται μια ειδοποίηση. Το ίδιο συμβαίνει όταν οι εγκατεστημένες εφαρμογές προσπαθούν να έχουν πρόσβαση σε κακόβουλα domains.

Σημαντικό
Εάν βρίσκεστε σε μια περιοχή όπου η χρήση μιας υπηρεσίας VPN δεν επιτρέπεται από το νόμο, η λειτουργικότητα του Web Protection δεν θα είναι διαθέσιμη.

Για να ενεργοποιήσετε την Προστασία Web:

1. Επιλέξτε το εικονίδιο στο κάτω μέρος της οθόνης.
2. Πατήστε **Συμφωνώ** .
3. Ενεργοποιήστε το διακόπτη Web Προστασία.

Σημείωση
Την πρώτη φορά που ενεργοποιείτε την Web Προστασία, ενδέχεται να σας ζητηθεί να επιτρέψετε στο Bitdefender να ρυθμίσει τις παραμέτρους VPN που θα παρακολουθούν την κυκλοφορία δικτύου. Πατήστε **Επιτρέπω** για να συνεχίσετε. Εάν έχει οριστεί μέθοδος ελέγχου ταυτότητας (δακτυλικό αποτύπωμα ή κωδικός PIN) για την προστασία του smartphone σας, πρέπει να το χρησιμοποιήσετε. Για να μπορέσετε να ανιχνεύσετε την πρόσβαση σε μη αξιόπιστες ιστοσελίδες, η Προστασία Web λειτουργεί μαζί με το VPN.

Σημαντικό
Η δυνατότητα Προστασίας Ιστού και το VPN δεν μπορούν να λειτουργούν ταυτόχρονα. Όποτε ένα από αυτά είναι ενεργοποιημένο, το άλλο (εάν είναι ενεργό εκείνη τη στιγμή) θα απενεργοποιείται.

17.1. Bitdefender ειδοποιήσεις

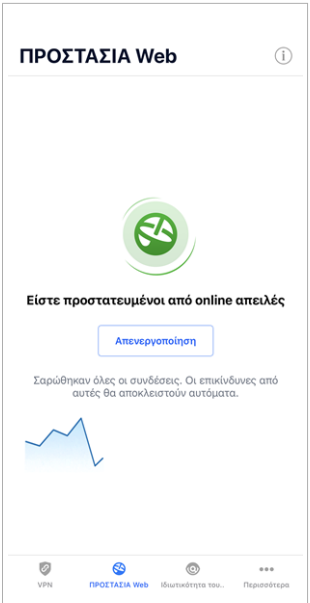
Κάθε φορά που προσπαθείτε να επισκεφθείτε έναν ιστότοπο που έχει χαρακτηριστεί ως μη ασφαλής, ο ιστότοπος αποκλείεται. Για να σας ενημερώσουμε για το συμβάν, ειδοποιήστε από το Bitdefender στο κέντρο ειδοποιήσεων και στο πρόγραμμα περιήγησής σας. Η σελίδα περιέχει πληροφορίες όπως η διεύθυνση URL της ιστοσελίδας και την εντοπισμένη απειλή. Θα πρέπει να αποφασίσετε τι θα κάνετε στη συνέχεια.

Επίσης, λαμβάνετε ειδοποίηση από το κέντρο ειδοποιήσεων κάθε φορά που μια λιγότερο ασφαλής εφαρμογή προσπαθεί να αποκτήσει πρόσβαση σε μη αξιόπιστες ιστοσελίδες. Πατήστε την εμφανιζόμενη ειδοποίηση για να ανακατευθυνθείτε στο παράθυρο, όπου μπορείτε να αποφασίσετε τι πρέπει να κάνετε στη συνέχεια.

Οι ακόλουθες επιλογές είναι διαθέσιμες και στις δύο περιπτώσεις:

- Πλοηγηθείτε μακριά από τον ιστότοπο, κάνοντας κλικ στο κουμπί **ΕΠΙΣΤΡΟΦΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ**
- Προχωρήστε στον ιστότοπο, παρά την προειδοποίηση, πατώντας την εμφανιζόμενη ειδοποίηση και στη συνέχεια **Θέλω να αποκτήσω πρόσβαση στη σελίδα**.

  Επιβεβαιώστε την επιλογή σας.



ΠΡΟΣΤΑΣΙΑ Web

17.2. Συνδρομές

Η Προστασία Web είναι ένα χαρακτηριστικό που βασίζεται στη συνδρομή και υπάρχει η δυνατότητα να το δοκιμάσετε δωρεάν ώστε να μπορείτε να αποφασίσετε αν ανταποκρίνεται στις απαιτήσεις σας. Υπάρχουν δύο τύποι συνδρομών για να επιλέξετε: ετήσια και μηνιαία.

Σε περίπτωση λήξης της συνδρομής για την Προστασία Web Bitdefender, δεν θα λάβετε ειδοποιήσεις όταν θα έχετε πρόσβαση σε κακόβουλο περιεχόμενο.

Εάν έχετε αγοράσει ένα από τα πακέτα Bitdefender, όπως το Bitdefender Total Security, τότε έχετε απεριόριστη πρόσβαση στην Web Προστασία.

18. ΙΔΙΩΤΙΚΌΤΗΤΑ ΤΟΥ ΛΟΓΑΡΙΑΣΜΟΎ

Η Bitdefender προστασία προσωπικών δεδομένων του λογαριασμού ανιχνεύει εάν έχουν προκύψει διαρροές δεδομένων στους λογαριασμούς που χρησιμοποιείτε για την πραγματοποίηση πληρωμών μέσω ηλεκτρονικού ταχυδρομείου, την αγορά ή την υπογραφή σε εφαρμογές ή ιστότοπους. Τα δεδομένα που μπορούν να αποθηκευτούν σε έναν λογαριασμό μπορεί να είναι κωδικοί πρόσβασης ή πληροφορίες τραπεζικού λογαριασμού και, εάν δεν ασφαλίζεται σωστά, ενδέχεται να προκύψει κλοπή ταυτότητας ή εισβολή στην ιδιωτική ζωή.

Η κατάσταση απορρήτου ενός λογαριασμού εμφανίζεται αμέσως μετά την επικύρωση.

Για να ελέγξετε εάν έχει διαρρεύσει κάποιος λογαριασμός, πατήστε **Σάρωση για διαρροές** .

Για να ξεκινήσετε να ασφαλίζετε τις προσωπικές σας πληροφορίες:

1. Επιλέξτε το εικονίδιο στο κάτω μέρος της οθόνης.
2. Πατήστε **Προσθήκη λογαριασμού** .
3. Πληκτρολογήστε την e-mail διεύθυνσή σας στο αντίστοιχο πεδίο και στη συνέχεια κάντε κλικ στο **Επόμενο**.

   Το Bitdefender πρέπει να επικυρώσει αυτόν τον λογαριασμό πριν εμφανίσει ιδιωτικές πληροφορίες. Επομένως, αποστέλλεται ένα email με κωδικό επικύρωσης στη email διεύθυνση που ορίστηκε.
4. Ελέγξτε τα εισερχόμενά σας και, στη συνέχεια, πληκτρολογήστε τον κωδικό που λάβατε στην περιοχή **Απόρρητο λογαριασμού** της εφαρμογής σας. Εάν δεν μπορείτε να βρείτε το email επικύρωσης στο φάκελο Εισερχόμενα, ελέγξτε το φάκελο Spam.

   Εμφανίζεται η κατάσταση απορρήτου του επικυρωμένου λογαριασμού.

Αν διαπιστώσετε διαρροές σε οποιονδήποτε από τους λογαριασμούς σας, σας συνιστούμε να αλλάξετε τον κωδικό πρόσβασής σας το συντομότερο δυνατό. Για να δημιουργήσετε έναν ισχυρό και ασφαλή κωδικό πρόσβασης, λάβετε υπόψη σας τις παρακάτω συμβουλές:

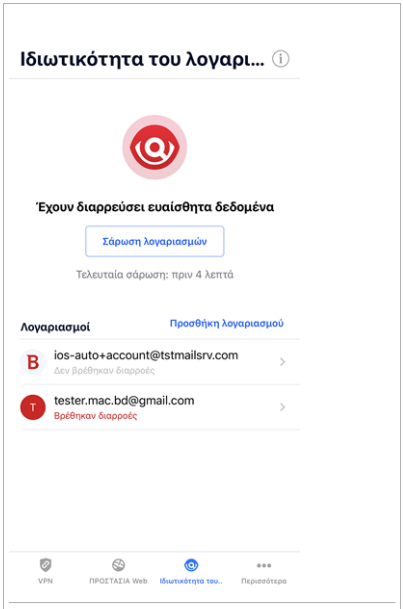
- Φροντίστε να είναι τουλάχιστον 8 χαρακτήρες.
- Να περιλαμβάνετε μικρούς και μεγάλους χαρακτήρες.

- Προσθέστε τουλάχιστον έναν αριθμό ή σύμβολο όπως #, @, % or !.

Μόλις έχετε ασφαλίσει έναν λογαριασμό που ήταν μέρος μιας παραβίασης της ιδιωτικής ζωής, μπορείτε να επιβεβαιώσετε τις αλλαγές, επισημαίνοντας τις αναγνωρισμένες διαρροές ως **Επίλυση** . Για να το κάνετε αυτό:

1. Πατήστε ··· δίπλα στην παράβαση που επιλύσατε.
2. Επιλέξτε **Ορισμός ως επιλυμένο**.

Όταν όλες οι διαρροές που ανιχνεύτηταν επισημανθούν ως **Επίλυση** , ο λογαριασμός δεν θα εμφανίζεται πλέον να έχει διαρρεύσε, τουλάχιστον έως ότου εντοπιστεί νέα διαρροή.



Ιδιωτικότητα του λογαριασμού

19. BITDEFENDER CENTRAL

Bitdefender Central είναι η διαδικτυακή πλατφόρμα όπου μπορείτε να έχετε πρόσβαση σε online υπηρεσίες και χαρακτηριστικά του προϊόντος αυτού και μπορείτε να εκτελέσετε από απόσταση σημαντικές εργασίες σε συσκευές όπου το Bitdefender είναι εγκατεστημένο. Μπορείτε να συνδεθείτε στον Bitdefender λογαριασμό από οποιονδήποτε υπολογιστή ή κινητή συσκευή που συνδέεται στο Internet μέσω του https://central.bitdefender.com, ή απευθείας μέσω της Bitdefender Central εφαρμογής για Android και iOS συσκευές.

Για να εγκαταστήσετε την Bitdefender Centralεφαρμογή στις συσκευές σας:

- **Σε Android** - αναζητήστε Bitdefender Central στο Google Play και στη συνέχεια κατεβάστε και εγκαταστήστε την εφαρμογή. Ακολουθήστε τα απαιτούμενα βήματα για να ολοκληρώσετε την εγκατάσταση.
- **Σε iOS** - αναζητήστε Bitdefender Central στο App Store και στη συνέχεια κάντε λήψη και εγκατάσταση της εφαρμογής. Ακολουθήστε τα απαιτούμενα βήματα για να ολοκληρώσετε την εγκατάσταση.

Μόλις έχετε πρόσβαση, μπορείτε να αρχίσετε να κάνετε τα εξής:

- Λήψη και εγκατάσταση του Bitdefender σε Windows, macOS, iOS και σε Android λειτουργικά συστήματα. Τα προϊόντα που διατίθενται για λήψη είναι:
  - Bitdefender Mobile Security για Android
  - Bitdefender Mobile Security για iOS
  - Bitdefender Antivirus για Mac
  - Η σειρά προϊόντων Bitdefender για Windows
- Διαχειριστείτε και ανανεώστε τις Bitdefender συνδρομές σας.
- Προσθέστε νέες συσκευές στο δίκτυό σας και διαχειριστείτε τις από όπου κι αν βρίσκεστε.

Πρόσβαση στον Bitdefender λογαριασμό σας

Υπάρχουν διάφοροι τρόποι για να αποκτήσετε πρόσβαση στο Bitdefender Central:

- Από τον πλοηγό σας:
  1. Ανοίξτε ένα πρόγραμμα περιήγησης σε οποιαδήποτε συσκευή με πρόσβαση στο Διαδίκτυο.
  2. Μετάβαση σε: https://central.bitdefender.com.
  3. Συνδεθείτε στο λογαριασμό σας χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
- Από την συσκευή σας Android ή iOS:

  Ανοίξτε την Bitdefender Central εφαρμογή που έχετε εγκαταστήσει.

Σημείωση
Σε αυτό το υλικό παρέχονται οι επιλογές και οι οδηγίες που διατίθενται στην πλατφόρμα web.

2-Factor Authentication

Η μέθοδος 2-Factor Authentication προσθέτει ένα πρόσθετο επίπεδο ασφαλείας στον Bitdefenderλογαριασμό σας, απαιτώντας έναν κωδικό επαλήθευσης εκτός από τα διαπιστευτήριά σας σύνδεσης. Έτσι θα αποτρέψετε την υποκλοπή του λογαριασμού σας και θα προστατευτείτε από επιθέσεις.

Ενεργοποίηση 2-Factor Authentication

Ενεργοποιώντας το 2-Factor Authentication, ο Bitdefender λογαριασμός σας θα είναι πολύ πιο ασφαλής. Η ταυτότητά σας θα επαληθεύεται κάθε φορά που θα συνδεθείτε από διαφορετικές συσκευές,για να εγκαταστήσετε ένα από τα Bitdefender προϊόντα, να ελέγξτε την κατάσταση της συνδρομής σας ή να εκτελέστε απομακρυσμένα εργασίες στις συσκευές σας.

Για να ενεργοποιήσετε το 2-Factor Authentication:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο 👤 στην επάνω δεξιά γωνία της οθόνης.
3. Κάντε κλικ στο **Ο Bitdefender Λογαριασμός μου** στο μενού.
4. Επιλέξτε την καρτέλα **Κωδικός και ασφάλεια**
5. Επιλέξτε **2-Factor Authentication**.
6. Επιλέξτε **ΕΝΑΡΞΗ**.

Επιλέξτε μία από τις ακόλουθες μεθόδους:

- **Εφαρμογή Authenticator** - χρησιμοποιήστε μια εφαρμογή ελέγχου ταυτότητας για να δημιουργήσετε έναν κωδικό κάθε φορά που θέλετε να συνδεθείτε στον Bitdefender λογαριασμό σας.

  Εάν θέλετε να χρησιμοποιήσετε μια εφαρμογή ελέγχου ταυτότητας, αλλά δεν είστε σίγουροι για το τι θα επιλέξετε, υπάρχει διαθέσιμη μια λίστα με τις εφαρμογές ελέγχου ταυτότητας που συστήνουμε.

  a. Επιλέξτε **ΧΡΗΣΙΜΟΠΟΙΗΣΤΕ AUTHENTICATOR ΕΦΑΡΜΟΓΗ** για να ξεκινήσετε.

  b. Για να συνδεθείτε σε μια συσκευή Android ή iOS, χρησιμοποιήστε τη συσκευή σας για να σαρώσετε τον QR κωδικό .

     Για να συνδεθείτε σε laptop ή επιτραπέζιο υπολογιστή, μπορείτε να προσθέσετε χειροκίνητα τον εμφανιζόμενο κώδικα.

     Επιλέξτε **ΣΥΝΕΧΕΙΑ**.

  c. Εισάγετε τον κωδικό που παρέχεται από την εφαρμογή ή αυτόν που εμφανίζεται στο προηγούμενο βήμα και στη συνέχεια πατήστε **ΕΝΕΡΓΟΠΟΙΗΣΗ** .

- **E-mail** - κάθε φορά που συνδέεστε στο Bitdefender λογαριασμό σας, θα σταλεί στο εισερχόμενό σας email ένας κωδικός επαλήθευσης. στη συνέχεια πληκτρολογήστε τον κωδικό που λάβατε.

  a. Επιλέξτε **ΧΡΗΣΙΜΟΙΗΣΤΕ EMAIL** για να ξεκινήσετε.

  b. Ελέγξτε το email και πληκτρολογήστε τον παρεχόμενο κωδικό.

     Σημειώστε ότι έχετε πέντε λεπτά για να ελέγξετε τον email λογαριασμό και να πληκτρολογήσετε τον παραγόμενο κώδικα. Εάν λήξει ο χρόνος, θα πρέπει να δημιουργήσετε έναν νέο κωδικό ακολουθώντας τα ίδια βήματα.

  c. Επιλέξτε **ΕΝΕΡΓΟΠΟΙΗΣΗ**.

  d. Σας παρέχονται δέκα κωδικοί ενεργοποίησης. Μπορείτε να τους αντιγράψετε, να τους κατεβάσετε ή να εκτυπώσετε τη λίστα και να την χρησιμοποιήσετε σε περίπτωση που χάσετε το email ή δεν θα μπορείτε να συνδεθείτε. Κάθε κωδικός μπορεί να χρησιμοποιηθεί μόνο μία φορά.

  e. Επιλέξτε **ΕΤΟΙΜΟ**.

Σε περίπτωση που θέλετε να σταματήσετε να χρησιμοποιείτε το 2-Factor Authentication:

1. Επιλέξτε **ΑΠΕΝΕΡΓΟΠΟΙΗΣΗ 2-FACTOR AUTHENTICATION**.
2. Ελέγξτε την εφαρμογή ή το email σας και πληκτρολογήστε τον κωδικό που λάβατε.

   Σημειώστε ότι έχετε πέντε λεπτά για να ελέγξετε τον email λογαριασμό σας και πληκτρολογήσετε τον παραγόμενο κώδικα. Εάν λήξει ο χρόνος, θα πρέπει να δημιουργήσετε έναν νέο κωδικό ακολουθώντας τα ίδια βήματα.
3. Επιβεβαιώστε την επιλογή σας.

Προσθήκη έμπιστης συσκευής

Για να βεβαιωθείτε ότι μόνο εσείς μπορείτε να αποκτήσετε πρόσβαση στο Bitdefender λογαριασμό σας, ίσως χρειαστεί πρώτα έναν κωδικό ασφαλείας. Εάν θέλετε να παραλείψετε αυτό το βήμα κάθε φορά που συνδέεστε από την ίδια συσκευή, σας συνιστούμε να την ορίσετε ως αξιόπιστη συσκευή.

Για να δηλώσετε συσκευές ως αξιόπιστες:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο 👤 στην επάνω δεξιά γωνία της οθόνης.
3. Κάντε κλικ στο **Ο Bitdefender Λογαριασμός μου** στο μενού.
4. Επιλέξτε την καρτέλα **Κωδικός και ασφάλεια**
5. Επιλέξτε **Αξιόπιστες συσκευές**.
6. Εμφανίζεται η λίστα με τις συσκευές όπου το Bitdefender που είναι εγκατεστημένο. Επιλέξτε την επιθυμητή συσκευή.

Μπορείτε να προσθέσετε όσες συσκευές επιθυμείτε, υπό την προϋπόθεση ότι έχει εγκατασταθεί το Bitdefender και η συνδρομή σας είναι έγκυρη.

Οι συσκευές μου

Η περιοχή **Οι συσκευές μου** στον Bitdefender λογαριασμό σας, σας δίνει τη δυνατότητα να εγκαταστήσετε, να διαχειριστείτε και να ολοκληρώσετε ενέργειες εξ αποστάσεως στο Bitdefender προϊόν σας σε οποιαδήποτε συσκευή, υπό την προϋπόθεση ότι είναι ενεργοποιημένη και συνδεδεμένη στο Internet. Οι κάρτες συσκευής εμφανίζουν το όνομα της συσκευής, την

κατάσταση προστασίας και αν υπάρχουν κίνδυνοι ασφαλείας που επηρεάζουν την προστασία των συσκευών σας.

Για να αναγνωρίσετε και να διαχειριστείτε εύκολα τις συσκευές σας, μπορείτε να προσαρμόσετε το όνομα της συσκευής και να δημιουργήσετε ή να αντιστοιχίσετε έναν κάτοχο σε καθένα από αυτά:

1. Πατήστε στο ≡ ιεικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **οι συσκευές μου**.
2. Πατήστε την επιθυμητή κάρτα συσκευής και, στη συνέχεια, το εικονίδιο ⋮ στην επάνω δεξιά γωνία της οθόνης. Διαθέσιμες επιλογές:

- **Ρυθμίσεις** - από εδώ μπορείτε να αλλάξετε το όνομα της επιλεγμένης συσκευής.
- **Προφίλ** - από εδώ μπορείτε να αντιστοιχίσετε ένα προφίλ στην επιλεγμένη συσκευή. Πατήστε **Προσθήκη κατόχου** , και στη συνέχεια συμπληρώστε τα αντίστοιχα πεδία, Ορίστε το Όνομα, τη διεύθυνση ηλεκτρονικού ταχυδρομείου, τον αριθμό τηλεφώνου, την ημερομηνία γέννησης και προσθέστε ακόμη και μια εικόνα προφίλ.
- **Κατάργηση** - Από εδώ, ένα προφίλ μαζί με την εκχωρηθείσα συσκευή μπορούν να καταργηθούν από το Bitdefender λογαριασμό σας.

Συνδεθείτε με έναν διαφορετικό Bitdefender λογαριασμό

Για να συνδεθείτε με έναν διαφορετικό Bitdefender λογαριασμό:

1. Επιλέξτε το ••• εικονίδιο στο κάτω μέρος της οθόνης.
2. Επιλέξτε **Αποσύνδεση**.
3. Πληκτρολογήστε τη διεύθυνση ηλεκτρονικού ταχυδρομείου και τον κωδικό πρόσβασης του Bitdefender λογαριασμού σας στο τα αντίστοιχα πεδία.
4. Πατήστε **ΣΥΝΔΕΣΗ**.

MOBILE SECURITY ΓΙΑ ANDROID

20. ΧΑΡΑΚΤΗΡΙΣΤΙΚΆ ΠΡΟΣΤΑΣΊΑΣ

Το Bitdefender Mobile Security προστατεύει την Android συσκευή σας με τα παρακάτω χαρακτηριστικά:

- Σαρωτής Κακόβουλου Λογισμικού
- ΠΡΟΣΤΑΣΙΑ Web
- VPN
- Anti-Theft, συμπεριλαμβανομένων:
  - Απομακρυσμένη τοποθεσία
  - Απομακρυσμένο κλείδωμα συσκευής
  - Απομακρυσμένη διαγραφή συσκευής
  - Απομακρυσμένες ειδοποιήσεις συσκευής
- Ιδιωτικότητα του λογαριασμού
- Κλείδωμα Εφαρμογών
- ΑΝΑΦΟΡΕΣ
- WearON

Μπορείτε να χρησιμοποιήσετε τα χαρακτηριστικά του προϊόντος για 14 μέρες, δωρεάν. Μετά τη λήξη της περιόδου, θα πρέπει να αγοράσετε την πλήρη έκδοση του προϊόντος για να προστατεύσετε τη συσκευή σας.

21. ΞΕΚΙΝΏΝΤΑΣ

Απαιτήσεις Συσκευής

Bitdefender Mobile Security λειτουργεί σε κάθε συσκευή που έχει λογισμικό Android 4.1 και άνω. Απαιτείται ενεργή σύνδεση στο Internet για τη in-the-cloud σάρωση κακόβουλου λογισμικού.

Εγκατάσταση του Bitdefender Mobile Security

- **Απο το Bitdefender Central**
  - Σε Android
    1. Μετάβαση σε: https://central.bitdefender.com.
    2. Συνδεθείτε στον Bitdefender λογαριασμό σας.
    3. Πατήστε στο ☰ εικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι συσκευές μου**.
    4. Επιλέξτε **ΕΓΚΑΤΑΣΤΑΣΗ ΠΡΟΣΤΑΣΙΑΣ** και, στη συνέχεια, πατήστε **Προστατέψτε αυτή τη συσκευή** .
    5. Επιλέξτε τον κάτοχο της συσκευής. Αν η συσκευή ανήκει σε κάποιον άλλο, πατήστε το αντίστοιχο κουμπί.
    6. Θα μεταφερθείτε στην **Google Play** εφαρμογή. Στην οθόνη του Google Play, πατήστε την επιλογή εγκατάστασης.
  - Σε Windows, macOS, iOS
    1. Μετάβαση σε: https://central.bitdefender.com.
    2. Συνδεθείτε στον Bitdefender λογαριασμό σας.
    3. Πατήστε στο ☰ εικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι συσκευές μου**.
    4. Επιλέξτε **ΕΓΚΑΤΑΣΤΑΣΗ ΠΡΟΣΤΑΣΙΑΣ** και, στη συνέχεια, πατήστε **Προστατέψτε άλλες συσκευές** .
    5. Επιλέξτε τον κάτοχο της συσκευής. Αν η συσκευή ανήκει σε κάποιον άλλο, πατήστε το αντίστοιχο κουμπί.
    6. Επιλέξτε **ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΕΓΚΑΤΑΣΤΑΣΗΣ**.

7. Πληκτρολογήστε μια email διεύθυνση στο αντίστοιχο πεδίο και πατήστε **ΑΠΟΣΤΟΛΗ EMAIL** Λάβετε υπόψη ότι ο παραγόμενος σύνδεσμος λήψης ισχύει μόνο για τις επόμενες 24 ώρες. Εάν λήξει ο σύνδεσμος, θα πρέπει να δημιουργήσετε ένα νέο, ακολουθώντας τα ίδια βήματα.
8. Στη συσκευή που θέλετε να εγκαταστήσετε το Bitdefender, ελέγξτε το λογαριασμό ηλεκτρονικού ταχυδρομείου που πληκτρολογήσατε και κάντε κλικ στο αντίστοιχο κουμπί λήψης.

- **Από το Google Play**

  Αναζητήστε το Bitdefender Mobile Security για να εντοπίσετε και να εγκαταστήσετε την εφαρμογή.

  Εναλλακτικά, σαρώστε τον κωδικό QR:

QR Code

Πριν περάσετε από τα βήματα επικύρωσης, πρέπει να συμφωνήσετε με τη Συμφωνία Συνδρομής. Αφιερώστε λίγο χρόνο για να διαβάσετε τη Συμφωνία Συνδρομής επειδή περιέχει τους όρους και τις προϋποθέσεις κάτω από τις οποίες μπορείτε να χρησιμοποιήσετε το Bitdefender Mobile Security.

Επιλέξτε **ΣΥΝΕΧΕΙΑ** για να μεταβείτε στο επόμενο παράθυρο.

Συνδεθείτε στον Bitdefender λογαριασμό σας

Για να χρησιμοποιήσετε το Bitdefender Mobile Security, πρέπει να συνδέσετε τη συσκευή σας με ένα Bitdefender λογαριασμό, Facebook, Google ή Microsoft ή Apple, συνδεόμενοι στο λογαριασμό από την εφαρμογή. Την πρώτη φορά που ανοίγετε την εφαρμογή, θα σας ζητηθεί να συνδεθείτε σε έναν λογαριασμό.

Εάν εγκαταστήσατε το Bitdefender Mobile Security από το Bitdefender λογαριασμό σας, η εφαρμογή θα προσπαθήσει να συνδεθεί αυτόματα σε αυτό το λογαριασμό.

Για να συνδέσετε τη συσκευή με το Bitdefender λογαρισμό:

1. Πληκτρολογήστε τη διεύθυνση ηλεκτρονικού ταχυδρομείου και τον κωδικό πρόσβασης του Bitdefender λογαριασμού σας στο τα αντίστοιχα πεδία. Εάν δεν έχετε Bitdefender λογαριασμό και θέλετε να δημιουργήσετε έναν λογαριασμό, επιλέξτε τον αντίστοιχο σύνδεσμο.
2. Πατήστε **ΣΥΝΔΕΣΗ**.

Για να συνδεθείτε χρησιμοποιώντας ένα Facebook, Google ή Microsoft λογαριασμό, επιλέξτε την υπηρεσία που θέλετε να χρησιμοποιήσετε από την περιοχή **Ή ΣΥΝΔΕΘΕΙΤΕ ΜΕ** . την επιλεγμένη υπηρεσία. Ακολουθήστε τις οδηγίες για να συνδέσετε το λογαριασμό σας με το Bitdefender Mobile Security.

Σημείωση
Το Bitdefender δεν πρόκειται να αποκτήσει πρόσβαση σε οποιαδήποτε εμπιστευτική πληροφορία όπως τον κωδικό πρόσβασης του λογαριασμού που χρησιμοποιείτε για την σύνδεση ή τις προσωπικές πληροφορίες των φίλων σας και των επαφών σας.

Διαμορφώστε την προστασία

Μόλις συνδεθείτε με επιτυχία στην εφαρμογή, εμφανίζεται το παράθυρο **Διαμόρφωση προστασίας** . ια να ασφαλίσετε τη συσκευή σας, σας συνιστούμε να ακολουθήσετε αυτά τα βήματα:

- **Κατάσταση συνδρομής.** Για να είστε προστατευμένοι χρησιμοποιώντας το Bitdefender Mobile Security, θα πρέπει να ενεργοποιήσετε το προϊόν σας με μια συνδρομή, η οποία καθορίζει πόσο καιρό μπορείτε να χρησιμοποιήσετε το προϊόν. Μόλις λήξει, η εφαρμογή σταματά να εκτελεί τα καθήκοντά της και να προστατεύει τη συσκευή σας.

  Εάν έχετε έναν κωδικό ενεργοποίησης, πατήστε **ΕΧΩ ΕΝΑ ΚΩΔΙΚΟ**, και, στη συνέχεια, πατήστε **ΕΝΕΡΓΟΠΟΙΗΣΗ**.

  Εάν έχετε συνδεθεί με νέο Bitdefender λογαριασμό και δεν έχετε κωδικό ενεργοποίησης, μπορείτε να χρησιμοποιήσετε το προϊόν για 14 ημέρες, χωρίς χρέωση.

- **ΠΡΟΣΤΑΣΙΑ Web.** Εάν η συσκευή σας απαιτεί δυνατότητα πρόσβασης για να ενεργοποιήσετε την προστασία του Web, πατήστε **ACTIVATE**. Θα ανακατευθυνθείτε στην επιλογή Accessibility. Bitdefender Mobile Security και στη συνέχεια ενεργοποιήστε τον αντίστοιχο διακόπτη.
- **Σαρωτής Κακόβουλου Λογισμικού.** Εκτελέστε μια πλήρη σάρωση για να βεβαιωθείτε ότι η συσκευή σας δεν παρουσιάζει απειλές. Για να ξεκινήσετε τη διαδικασία σάρωσης, πατήστε **ΣΑΡΩΣΗ ΤΩΡΑ**.

  Μόλις ξεκινήσει η διαδικασία σάρωσης, εμφανίζεται ο πίνακας ελέγχου. Εδώ μπορείτε να δείτε την κατάσταση ασφαλείας της συσκευής σας.

Ταμπλό

Πατήστε στο εικονίδιο Bitdefender Mobile Security στο πάνω μέρος της εφαρμογής της συσκευής σας για να ανοίξει το interface της εφαρμογής.

Ο Πίνακας ελέγχου παρέχει πληροφορίες σχετικά με την κατάσταση ασφαλείας της συσκευής σας και μέσω του αυτόματου πιλότου, μπορείτε να βελτιώσετε την ασφάλεια της συσκευής σας δίνοντάς σας συστάσεις σχετικά με τις λειτουργίες.

Η κάρτα κατάστασης στο επάνω μέρος του παραθύρου σας ενημερώνει για την κατάσταση ασφαλείας της συσκευής χρησιμοποιώντας ρητά μηνύματα και χρώματα που υποδηλώνουν. Εάν το Bitdefender Mobile Security δεν έχει προειδοποιήσεις, η κάρτα κατάστασης είναι πράσινη. Σε περίπτωση θέματος ασφαλείας η κάρτα κατάστασης αλλάζει το χρώμα της σε κόκκινο χρώμα.

Για να σας προσφέρουμε αποτελεσματική λειτουργία και αυξημένη προστασία κατά την εκτέλεση διαφορετικών δραστηριοτήτων, ο **Bitdefender Αυτόματος πιλότος** θα ενεργεί ως ο προσωπικός σας σύμβουλος ασφάλειας. Ανάλογα με τη δραστηριότητα που εκτελείτε, ο Bitdefender αυτόματος πιλότος του προϊόντος θα σας προτείνει συστάσεις βάσει της χρήσης και των αναγκών της συσκευής. Αυτό θα σας βοηθήσει να ανακαλύψετε και να επωφεληθείτε από τα πλεονεκτήματα που προσφέρουν τα χαρακτηριστικά που περιλαμβάνονται στην Bitdefender Mobile Security εφαρμογή

Όποτε υπάρχει μία διαδικασία σε εξέλιξη ή μία λειτουργία που απαιτεί τη συμβολή σας, μια κάρτα με περισσότερες πληροφορίες και πιθανές ενέργειες θα εμφανίζεται στο ταμπλό.

Μπορείτε να αποκτήσετε πρόσβαση στις Bitdefender Mobile Security λειτουργίες και να πλοηγηθείτε εύκολα από την κάτω γραμμή πλοήγησης:

Σαρωτής Κακόβουλου Λογισμικού

Σας επιτρέπει να ξεκινήσετε μια σάρωση και να ενεργοποιήσετε ή να απενεργοποιήσετε την Σάρωση Αποθηκευτικού Μέσου. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Σαρωτής Κακόβουλου Λογισμικού"* (p. 304).

ΠΡΟΣΤΑΣΙΑ Web

Εξασφαλίζει μια εμπειρία Ασφαλούς περιήγησης προειδοποιώντας σας για πιθανές κακόβουλες ιστοσελίδες. Για περισσότερες πληροφορίες, ανατρέξτε στην *"ΠΡΟΣΤΑΣΙΑ Web"* (p. 307).

VPN

Κρυπτογραφεί την επικοινωνία μέσω διαδικτύου, βοηθώντας σας να διατηρήσετε το απόρρητό σας ανεξάρτητα από το δίκτυο στο οποίο είστε συνδεδεμένοι. Για περισσότερες πληροφορίες, ανατρέξτε στην *"VPN"* (p. 309).

Anti-Theft

Σας επιτρέπει να ενεργοποιήσετε ή να απενεργοποιήσετε το Anti-Theft και να το ρυθμίσετε. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Χαρακτηριστικά Anti-Theft"* (p. 313).

Ιδιωτικότητα του λογαριασμού

Ελέγχει εάν έχει σημειωθεί διαρροή δεδομένων στους λογαριασμούς σας στο διαδίκτυο. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Ιδιωτικότητα του λογαριασμού"* (p. 318).

Κλείδωμα Εφαρμογών

Σας επιτρέπει να προστατεύσετε τις εγκατεστημένες εφαρμογές σας με τον καθορισμό ενός κωδικού πρόσβασης PIN. Για περισσότερες πληροφορίες, ανατρέξτε στην *"Κλείδωμα Εφαρμογών"* (p. 320).

ΑΝΑΦΟΡΕΣ

Διατηρεί ένα αρχείο καταγραφής όλων των σημαντικών ενεργειών, αλλαγές κατάσταση και άλλα κρίσιμα μηνύματα που σχετίζονται με την δραστηριότητα της συσκευής σας. Για περισσότερες πληροφορίες, ανατρέξτε στην *"ΑΝΑΦΟΡΕΣ"* (p. 326).

WearON

Επικοινωνεί με το SmartWatch σας για να σας βοηθήσει να βρείτε το τηλέφωνό σας σε περίπτωση που το χάσετε ή ξεχάσετε που το

αφήσατε. Για περισσότερες πληροφορίες, ανατρέξτε στην “*WearON*” (p. 328).

22. ΣΑΡΩΤΉΣ ΚΑΚΌΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΎ

Το Bitdefender προστατεύει τη συσκευή και τα δεδομένα σας από κακόβουλες εφαρμογές χρησιμοποιώντας σάρωση κατά την εγκατάσταση καικατά βούληση.

Η διεπαφή Malware Scanner παρέχει μια λίστα με όλους τους τύπους απειλών που αναζητά το Bitdefender, μαζί με τους ορισμούς τους. Απλώς αγγίξτε οποιαδήποτε απειλή για να δείτε τον ορισμό της.

Σημείωση
Βεβαιωθείτε ότι το κινητό σας είναι συνδεδεμένο στο Internet. Αν η συσκευή σας δεν είναι συνδεδεμένη στο Internet, η διαδικασία σάρωσης δεν θα ξεκινήσει.

- **Σάρωση On-install**

  Κάθε φορά που εγκαθιστάτε μια εφαρμογή, το Bitdefender Mobile Security σαρώνει αυτόματα χρησιμοποιώντας τεχνολογία cloud. Η ίδια διαδικασία σάρωσης ξεκινά κάθε φορά που ενημερώνονται οι εγκατεστημένες εφαρμογές.

  Εάν η εφαρμογή είναι κακόβουλη, θα εμφανιστεί μια ειδοποίηση που θα σας ζητά να την απεγκαταστήσετε. Πατήστε **Απεγκατάσταση** για να μεταβείτε στην συγκεκριμένη οθόνη απεγκατάστασης εφαρμογής.

- **On-demand σάρωση**

  Όποτε θελήσετε να βεβαιωθείτε ότι οι εφαρμογές που είναι εγκατεστημένες στη συσκευή σας είναι ασφαλείς στη χρήση, μπορείτε να ξεκινήσετε μια σάρωση.

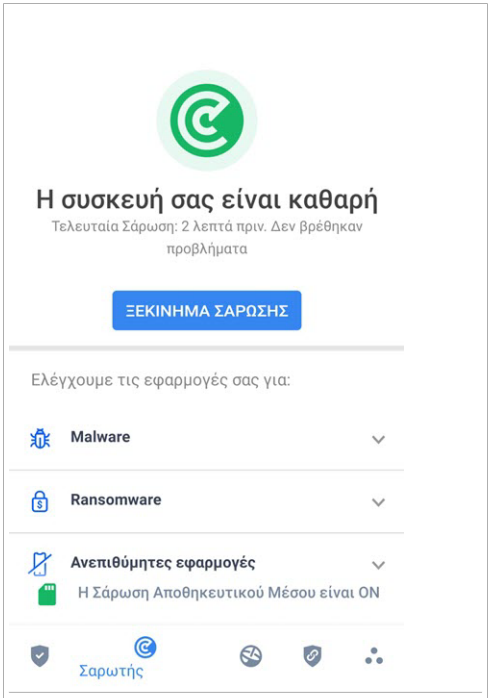
  Για να ξεκινήσετε μια σάρωση:

  1. Πατήστε **Σαρωτής κακόβουλου λογισμικού** στην κάτω γραμμή πλοήγησης.
  2. Πατήστε **ΕΝΑΡΞΗ ΣΑΡΩΣΗΣ**.

  Σημείωση
  Πρόσθετα δικαιώματα απαιτούνται για το Android 6 για την λειτουργία Malware Scanner Αφού πατήσετε το κουμπί **ΕΝΑΡΞΗ ΣΑΡΩΣΗΣ**, επιλέξτε**Επέτρεψε** για τα ακόλουθα:

- Επιτρέπετε το **Antivirus** να πραγματοποιεί και να διαχειρίζεται τις τηλεφωνικές κλήσεις;
- Επιτρέπετε το **Antivirus** να έχει πρόσβαση σε φωτογραφίες, ταινίες, και στα αρχεία στη συσκευή σας;

Η πρόοδος σάρωσης θα εμφανιστεί και μπορείτε να διακόψετε τη διαδικασία ανά πάσα στιγμή.



ΣΑΡΩΣΗ ΚΑΚΟΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

Από προεπιλογή, το Bitdefender Mobile Security θα σαρώσει τον εσωτερικό χώρο αποθήκευσης της συσκευή σας, συμπεριλαμβανομένων τυχόν τοποθετημένων καρτών SD. Με αυτό τον τρόπο, τυχόν επικίνδυνες εφαρμογές που θα μπορούσαν να είναι στην κάρτα μπορούν να ανιχνευθούν πριν να προκαλέσουν βλάβη.

Για να ενεργοποιήσετε ή να απενεργοποιήσετε τη ρύθμιση σάρωσης αποθήκευσης:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Ρυθμίσεις**.
3. Απενεργοποιήστε το διακόπτη **Αποθήκευση σάρωσης** στην περιοχή Σαρωτής κακόβουλων προγραμμάτων.

Εάν εντοπιστούν κακόβουλες εφαρμογές, θα εμφανιστούν πληροφορίες σχετικά με αυτές και θα μπορέσετε να τις αφαιρέσετε πατώντας το κουμπί **ΑΠΕΓΚΑΤΑΣΤΑΣΗ**.

Η κάρτα Σαρωτής Κακόβουλου Λογισμικού εμφανίζει την κατάσταση της συσκευής σας. Όταν η συσκευή είναι ασφαλής, η κάρτα είναι πράσινη. Όταν η συσκευή απαιτεί μια σάρωση, ή όταν υπάρχει μια ενέργεια η οποία απαιτεί την συμβολή σας, η κάρτα θα είναι κόκκινη.

Εάν η έκδοση του Android σας είναι 7. 1 ή νεότερη έκδοση, μπορείτε να αποκτήσετε πρόσβαση σε μια συντόμευση σε σαρωτή κακόβουλου λογισμικού, ώστε να μπορείτε να εκτελείτε σαρώσεις ταχύτερα χωρίς να ανοίξετε το Bitdefender Mobile Security interface . Για να το κάνετε αυτό, πατήστε παρατεταμένα το Bitdefender εικονίδιο που βρίσκεται στην Αρχική οθόνη ή στο συρτάρι εφαρμογών και, στη συνέχεια, επιλέξτε το εικονίδιο .

23. ΠΡΟΣΤΑΣΙΑ WEB

Οι έλεγχοι ασφαλείας στο Web του Bitdefender πραγματοποιούνται μέσω του προεπιλεγμένου Android browser, Google Chrome, Firefox, Opera, Opera Mini, Edge, Samsung Internet και Dolphin. Μια πλήρης λίστα με τα υποστηριζόμενα προγράμματα περιήγησης διατίθεται στην ενότητα Ασφάλεια στο Web.

Σημείωση

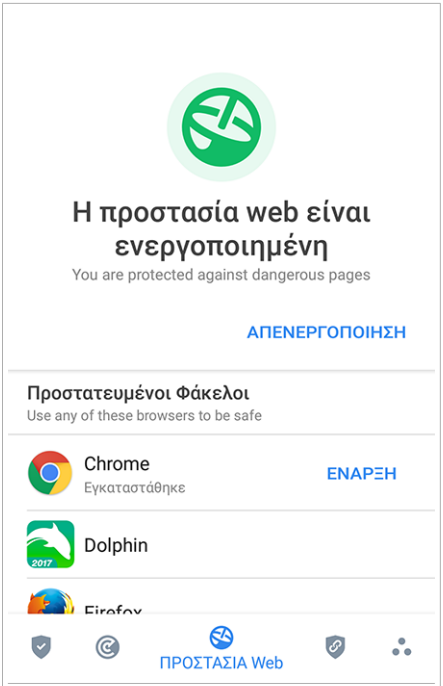
Επιπλέον δικαιώματα απαιτούνται για το Android 6 για τη λειτουργία Web Protection.

Επιτρέψτε να εγγραφεί ως υπηρεσία προσβασιμότητας και πατήστε **ΕΝΕΡΓΟΠΟΙΗΣΗ** όταν σας ζητηθεί. Πατήστε **Antivirus** και ενεργοποιήστε το διακόπτη, στη συνέχεια, επιβεβαιώστε ότι συμφωνείτε με την πρόσβαση στα δικαιώματα της συσκευής σας.

Κάθε φορά που αποκτάτε πρόσβαση σε έναν τραπεζικό ιστότοπο, το Bitdefender Web Protection έχει ρυθμιστεί να σας ειδοποιεί για τη χρήση του VPN Bitdefender. Η ειδοποίηση εμφανίζεται στη γραμμή κατάστασης. Σας συνιστούμε να χρησιμοποιήσετε το Bitdefender VPN ενώ είστε συνδεδεμένοι στον τραπεζικό σας λογαριασμό, έτσι ώστε τα δεδομένα σας να μπορούν να παραμείνουν ασφαλή από ενδεχόμενες παραβιάσεις ασφαλείας.

Για να απενεργοποιήσετε την ειδοποίηση προστασίας στο Web:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Ρυθμίσεις**.
3. Απενεργοποιήστε τον αντίστοιχο διακόπτη στην περιοχή προστασίας Web.



ΠΡΟΣΤΑΣΙΑ Web

24. VPN

Με το Bitdefender VPN μπορείτε να διατηρείτε τα προσωπικά σας δεδομένα ιδιωτικά κάθε φορά που συνδέεστε σε ασύρματα ασύρματα δίκτυα, ενώ βρίσκεστε σε αεροδρόμια, εμπορικά κέντρα, καφετέριες ή ξενοδοχεία. Με αυτόν τον τρόπο, ατυχείς καταστάσεις όπως η κλοπή προσωπικών δεδομένων, ή προσπαθείες κάποιου να καταστήσει τη διεύθυνση IP της συσκευής σας προσβάσιμη στους χάκερς, μπορεί να αποφευχθεί.

Το VPN χρησιμεύει ως σήραγγα μεταξύ της συσκευής σας και του δικτύου που συνδέετε για να εξασφαλίζετε τη σύνδεσή σας, κρυπτογραφώντας τα δεδομένα χρησιμοποιώντας κρυπτογράφηση τραπεζικής ποιότητας και αποκρύπτοντας τη διεύθυνση IP όπου κι αν βρίσκεστε. Η επισκεψιμότητά σας μεταφέρεται μέσω ενός ξεχωριστού διακομιστή. καθιστώντας έτσι τη συσκευή σας σχεδόν αδύνατη να ταυτοποιηθεί μέσω των μυριάδων άλλων συσκευών που χρησιμοποιούν τις υπηρεσίες μας. Επιπλέον, ενώ είστε συνδεδεμένοι στο διαδίκτυο μέσω του Bitdefender VPN, μπορείτε να αποκτήσετε πρόσβαση σε περιεχόμενο που συνήθως περιορίζεται σε συγκεκριμένες περιοχές.

Σημείωση

Ορισμένες χώρες ασκούν λογοκρισία στο Διαδίκτυο και ως εκ τούτου η χρήση των VPN στην επικράτειά τους έχει απαγορευτεί από το νόμο. Για να αποφύγετε νομικές συνέπειες, μπορεί να εμφανιστεί ένα προειδοποιητικό μήνυμα όταν επιχειρήσετε να χρησιμοποιήσετε τη λειτουργία VPN Bitdefender για πρώτη φορά. Συνεχίζοντας τη χρήση της λειτουργίας, επιβεβαιώνετε ότι γνωρίζετε τους ισχύοντες κανονισμούς των χωρών και τους κινδύνους στους οποίους ενδέχεται να εκτεθείτε.

Υπάρχουν δύο τρόποι για να ενεργοποιήσετε ή να απενεργοποιήσετε το Bitdefender VPN:

- Επιλέξτε **ΣΥΝΔΕΣΗ** στην κάρτα VPN από τον Πίνακα ελέγχου.

  Εμφανίζεται η κατάσταση του Bitdefender VPN .

- Επιλέξτε **VPN** στην κάτω γραμμή πλοήγησης και, στη συνέχεια, αγγίξτε το **ΣΥΝΔΕΣΗ**.

  Επιλέξτε **ΣΥΝΔΕΣΗ** κάθε φορά που θέλετε να παραμείνετε προστατευμένοι ενώ είστε συνδεδεμένοι σε μη ασφαλή ασύρματα δίκτυα.

  Επιλέξτε **ΑΠΟΣΥΝΔΕΣΗ** όποτε θέλετε να απενεργοποιήσετε τη σύνδεση.

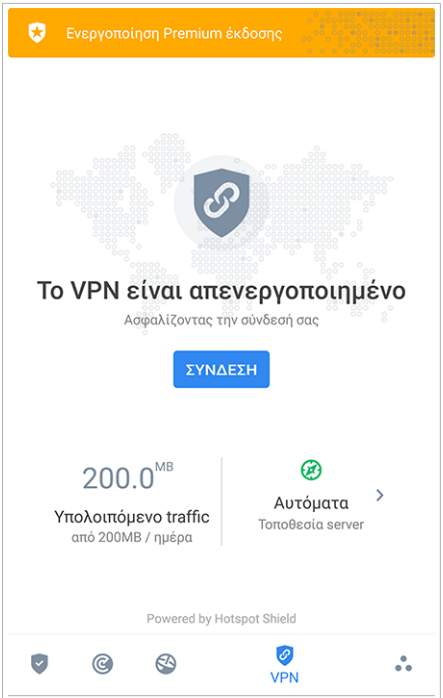
Σημείωση

Την πρώτη φορά που ενεργοποιείτε το VPN, σας ζητείται να επιτρέψετε στο Bitdefender να δημιουργήσει μια σύνδεση VPN που θα παρακολουθεί την κίνηση δικτύου. Πατήστε **OK** για να συνεχίσετε.

Εάν η έκδοση Android είναι 7.1 ή νεότερη, μπορείτε να αποκτήσετε πρόσβαση σε μια συντόμευση στο Bitdefender VPN, χωρίς να ανοίξετε το Bitdefender Mobile Security interface. Για να το κάνετε αυτό, πατήστε παρατεταμένα το Bitdefender εικονίδιο που βρίσκεται στην Αρχική οθόνη ή στο συρτάρι εφαρμογών και, στη συνέχεια, επιλέξτε το εικονίδιο .

Για να εξοικονομήσετε ενέργεια από τη μπαταρία, σας συνιστούμε να απενεργοποιήσετε το VPN όταν δεν το χρειάζεστε.

Εάν έχετε συνδρομή premium και επιθυμείτε να συνδεθείτε με ένα server, πατήστε **ΕΠΙΛΕΞΤΕ ΤΟΠΟΘΕΣΙΑ** στη διασύνδεση VPN και, στη συνέχεια, επιλέξτε τη θέση που θέλετε. σχετικά με τις συνδρομές VPN, ανατρέξτε στο “Συνδρομές” (p. 312).



VPN

Ρυθμίσεις VPN

Για μια προηγμένη διαμόρφωση του VPN σας:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Ρυθμίσεις**.

Στην VPN περιοχή μπορείτε να διαμορφώσετε τις παρακάτω επιλογές:

- Γρήγορη πρόσβαση σύνδεσης VPN - μια ειδοποίηση θα εμφανιστεί στη γραμμή κατάστασης για να σας επιτρέψει να ενεργοποιήσετε γρήγορα το VPN.
- Άνοιγμα προειδοποίησης Wi-Fi - κάθε φορά που συνδέεστε σε ανοιχτό δίκτυο Wi-Fi, ειδοποιείτε στη γραμμή κατάστασης της συσκευής σας να χρησιμοποιείτε VPN.

Συνδρομές

Το Bitdefender VPN προσφέρει δωρεάν μια ημερήσια quota κίνησης 200 MB ανά συσκευή για να εξασφαλίσει τη σύνδεσή σας κάθε φορά που χρειάζεστε και σας συνδέει αυτόματα με τη βέλτιστη τοποθεσία του server.

Για να έχετε απεριόριστη κίνηση και απεριόριστη πρόσβαση στο περιεχόμενο σε όλο τον κόσμο επιλέγοντας μια τοποθεσία διακομιστή σύμφωνα με τη βούλησή σας, αναβαθμίστε την έκδοση Premium.

Μπορείτε να αναβαθμίσετε ανά πάσα στιγμή στην έκδοση Bitdefender Premium VPN πατώντας το κουμπί **ΕΝΕΡΓΟΠΟΙΗΣΗ PREMIUM VPN** στον πίνακα ελέγχου, ή **Ενεργοποίηση Premium έκδοσης**από το παράθυρο VPN.

Η συνδρομή Bitdefender Premium VPN είναι ανεξάρτητη από τη Bitdefender Mobile Security συνδρομή , πράγμα που σημαίνει ότι θα μπορείτε να το χρησιμοποιήσετε για ολόκληρη τη διαθεσιμότητα, ανεξάρτητα από την κατάσταση της συνδρομής κατά των ιών. Σε περίπτωση που λήξει η συνδρομή Bitdefender Premium VPN, αλλά το προϊόν για το Bitdefender Mobile Security εξακολουθεί να είναι ενεργό, θα επανέλθετε στην ελεύθερη έκδοση.

Το Bitdefender VPN είναι προϊόν πολλαπλής πλατφόρμας, διαθέσιμο σε Bitdefender προϊόντα συμβατά με Windows, mac OS, Android και iOS. Μόλις αναβαθμίσετε στην premium έκδοση, να είστε σε θέση να χρησιμοποιήσετε τη συνδρομή σας σε όλα τα προϊόντα, υπό την προϋπόθεση ότι θα συνδεθείτε με τον ίδιο Bitdefender λογαριασμό.

25. ΧΑΡΑΚΤΗΡΙΣΤΙΚΆ ANTI-THEFT

Το Bitdefender μπορεί να σας βοηθήσει να εντοπίσετε τη συσκευή σας και να αποτρέψει να πέσουν τα προσωπικά σας δεδομένα σε λάθος χέρια.

Το μόνο που χρειάζεται να κάνετε είναι να ενεργοποιήσετε το Anti-Theft από τη συσκευή και όταν χρειαστεί μπείτε στο **Bitdefender Central** από οποιοδήποτε web browser, οπουδήποτε.

Σημείωση
Η διεπαφή Anti-Theft περιλαμβάνει επίσης έναν σύνδεσμο για την εφαρμογή Bitdefender Central στο Google Play Store. Μπορείτε να χρησιμοποιήσετε αυτόν τον σύνδεσμο για να κάνετε λήψη της εφαρμογής, σε περίπτωση που δεν το έχετε κάνει ήδη.

Το Bitdefender Mobile Security προσφέρει τις ακόλουθες λειτουργίες Anti-Theft:

Απομακρυσμένος εντοπισμός

Δείτε την τρέχουσα θέση της συσκευής σας στο Google Maps. Η τοποθεσία ανανεώνεται κάθε 5 δευτερόλεπτα, ώστε να μπορείτε να παρακολουθείτε αν είναι σε κίνηση.

Η ακρίβεια της τοποθεσίας εξαρτάται από το πόσο το Bitdefender είναι σε θέση να την προσδιορίσει:

- Εάν το GPS είναι ενεργοποιημένο στη συσκευή, η θέση του μπορεί να εντοπιστεί με προσέγγιση μερικών μέτρων για όσο διάστημα είναι στο εύρος των δορυφόρων GPS (π.χ. δεν είναι μέσα σε ένα κτίριο).
- Αν η συσκευή είναι σε εσωτερικό χώρο, η θέση του μπορεί να προσδιοριστεί με προσέγγιση δεκάδων μέτρων εάν το Wi-Fi είναι ενεργοποιημένο και υπάρχουν διαθέσιμα ασύρματα δίκτυα σε κοντινή απόσταση.
- Σε αντίθετη περίπτωση, η θέση θα προσδιορίζεται με τη χρήση μόνο των πληροφοριών από το δίκτυο κινητής τηλεφωνίας, το οποίο μπορεί να προσφέρει ακρίβεια όχι καλύτερη από αρκετές εκατοντάδες μέτρα.

Απομακρυσμένο Κλείδωμα

Κλειδώστε την οθόνη του υπολογιστή σας και ορίστε έναν αριθμητικό κωδικό PIN για το ξεκλείδωμα του.

Απομακρυσμένη Διαγραφή

Αφαιρέστε όλα τα προσωπικά δεδομένα από την κλεμμένη συσκευή σας.

Αποστολή ειδοποίησης στη συσκευή (Scream)

Στείλετε ένα μήνυμα που θα εμφανίζεται στην οθόνη της συσκευής, από μακρυά, ή ενεργοποιήστε ένα δυνατό ήχο για να ακουστεί από το ηχείο της συσκευής.

Αν χάσετε τη συσκευή σας, μπορείτε να ενημερώσετε όποιον την βρει για το πώς μπορεί να σας την επιστρέψει με την εμφάνιση ενός μηνύματος στην οθόνη της συσκευής.

Αν δεν θυμάστε που αφήσατε τη συσκευή σας και υπάρχει μια πιθανότητα να μην είναι μακριά από εσάς (για παράδειγμα, κάπου γύρω από το σπίτι ή στο γραφείο), υπάρχει καλύτερος τρόπος για να τη βρείτε από το να παίξει ένα δυνατό ήχο; Ο ήχος θα ακούγεται ακόμα και αν η συσκευή είναι σε λειτουργία σίγασης.

Ενεργοποίηση Anti-Theft

Για να ενεργοποιήσετε τις λειτουργίες Anti-Theft, απλώς ολοκληρώστε τη διαδικασία διαμόρφωσης από την κάρτα Anti-Theft που είναι διαθέσιμη στο Ταμπλό.

Εναλλακτικά, μπορείτε να ενεργοποιήσετε το Anti-Theft ακολουθώντας τα παρακάτω βήματα:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Anti-Theft**.
3. Πατήστε **ΕΝΕΡΓΟΠΟΙΗΣΗ**.
4. Η ακόλουθη διαδικασία θα αρχίσει για να σας βοηθήσει να ενεργοποιήσετε αυτήν τη λειτουργία:

Σημείωση

Πρόσθετα δικαιώματα απαιτούνται για το Android 6 για τη λειτουργία Anti-Theft Για να την ενεργοποιήσετε, ακολουθήστε τα παρακάτω βήματα:

a. Πατήστε **Ενεργοποίηση Anti-Theft** στη συνέχεια, πατήστε **ΕΝΕΡΓΟΠΟΙΗΣΗ**.

b. Επιτρέψτε το **Antivirus** να αποκτήσει πρόσβαση στην τοποθεσία αυτής της συσκευής.

a. **Δώστε προνόμια Διαχειριστή**

Αυτά τα προνόμια είναι απαραίτητα για τη λειτουργία Anti-Theft και, ως εκ τούτου, θα πρέπει να χορηγηθούν για να συνεχίσετε.

b. **Ορισμός PIN της Εφαρμογής**

Για να αποφευχθεί η μη εξουσιοδοτημένη πρόσβαση στη συσκευή σας, πρέπει να οριστεί ένας κωδικός PIN. Κάθε φορά που θα γίνει προσπάθεια σύνδεσης στη συσκευή σας, πρέπει πρώτα να εισαχθεί το PIN. Εναλλακτικά σε συσκευές που υποστηρίζουν την επαλήθευση δακτυλικών αποτυπωμάτων, μπορεί να χρησιμοποιηθεί επιβεβαίωση δακτυλικών αποτυπωμάτων αντί του επιλεγμένου κωδικού PIN.

Ο ίδιος κωδικός PIN χρησιμοποιείται από το App Lock για να προστατεύσει τις εγκατεστημένες εφαρμογές σας.

c. **Ενεργοποίηση Στιγμιαία Φωτογράφιση**

Κάθε φορά που κάποιος προσπαθεί να ξεκλειδώσει τη συσκευή σας χωρίς επιτυχία, ενώ το Snap Photo είναι ενεργοποιημένο, το Bitdefender θα τραβήξει μια φωτογραφία του.

Πιο συγκεκριμένα, κάθε φορά που ο κωδικός PIN, ο κωδικός πρόσβασης ή η επιβεβαίωση δακτυλικών αποτυπωμάτων που ορίσατε για την προστασία της συσκευής σας εισάγεται λάθος τρεις φορές στη σειρά, μια φωτογραφία τραβιέται χρησιμοποιώντας την μπροστινή κάμερα μια φωτογραφία τραβιέται χρησιμοποιώντας την μπροστινή κάμερα μαζί με τη χρονική σφραγίδα και το λόγο και μπορείτε να το δείτε όταν ανοίξετε το Bitdefender Mobile Security και επιλέξτε τη λειτουργία Anti-Theft. Εναλλακτικά, μπορείτε να δείτε την ληφθείσα φωτογραφία στο Bitdefender λογαριασμό:

i. Μετάβαση σε: https://central.bitdefender.com.

ii. Συνδεθείτε στο λογαριασμό σας

iii. Πατήστε στο εικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι συσκευές μου**.

iv. Επιλέξτε τη συσκευή σας Android και, στη συνέχεια, την καρτέλα **Anti-Theft** .

v. Επιλέξτε δίπλα στο **Ελέγξτε τα στιγμιότυπα σας** για να δείτε τις πιο πρόσφατες ληφθείσες φωτογραφίες.

Αποθηκεύονται μόνο οι δύο πιο πρόσφατες φωτογραφίες.

Αφού ενεργοποιηθεί η λειτουργία Anti-Theft, μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε τις Web Control εντολές ξεχωριστά από το παράθυρο Anti-Theft κάνοντας κλικ στις αντίστοιχες επιλογές.

Χρήση λειτουργιών Anti-Theft από το Bitdefender Central

Σημείωση

Όλες οι λειτουργίες του Anti-Theft απαιτούν την επιλογή **Background data** να είναι ενεργοποιημένη στις ρυθμίσεις χρήσης δεδομένων της συσκευή σας

Για να αποκτήσετε πρόσβαση στα Anti-Theft χαρακτηριστικά από το Bitdefender λογαριασμό σας:

1. Πρόσβαση στο Bitdefender Central.
2. Πατήστε στο εικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι συσκευές μου**.
3. Στην επιλογή **MY DEVICES** επιλέξτε την επιθυμητή κάρτα της συσκευής.
4. επιλέξτε το **Anti-Theft** πεδίο.
5. Στο κάτω μέρος του παραθύρου, πατήστε το εικονίδιο, και στη συνέχεια το κουμπί που αντιστοιχεί στο χαρακτηριστικό που θέλετε να χρησιμοποιήσετε:

   Εντοπισμός - εμφανίζει την τοποθεσία της συσκευής σας στο Google Maps.

   Ειδοποίηση - πληκτρολογήσετε ένα μήνυμα που θα εμφανίζεται στην οθόνη της συσκευή σας ή/και κάντε τη συσκευή σας να αναπαράγει έναν ήχο ειδοποίησης.

   Κλείδωμα - κλειδώστε την συσκευή σας και ορίστε ένα κωδικό PIN για το ξεκλείδωμα του.

   Διαγραφή - διαγράψετε όλα τα δεδομένα από τη συσκευή σας.

Σημαντικό

Μετά από την απαλοιφή μιας συσκευής, όλες οι λειτουργίες Anti-Theft παύουν να λειτουργούν.

SHOW IP - εμφανίζει την τελευταία διεύθυνση IP για την επιλεγμένη συσκευή.

Ρυθμίσεις Anti-Theft

Αν θέλετε να ενεργοποιήσετε ή να απενεργοποιήσετε τις απομακρυσμένες εντολές:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Anti-Theft**.
3. Ενεργοποιήστε ή απενεργοποιήστε τις επιθυμητές επιλογές.

26. ΙΔΙΩΤΙΚΌΤΗΤΑ ΤΟΥ ΛΟΓΑΡΙΑΣΜΟΎ

Η Bitdefender προστασία προσωπικών δεδομένων του λογαριασμού ανιχνεύει εάν έχουν προκύψει διαρροές δεδομένων στους λογαριασμούς που χρησιμοποιείτε για την πραγματοποίηση πληρωμών μέσω ηλεκτρονικού ταχυδρομείου, την αγορά ή την υπογραφή σε εφαρμογές ή ιστότοπους. Τα δεδομένα που μπορούν να αποθηκευτούν σε έναν λογαριασμό μπορεί να είναι κωδικοί πρόσβασης ή πληροφορίες τραπεζικού λογαριασμού και, εάν δεν ασφαλίζεται σωστά, ενδέχεται να προκύψει κλοπή ταυτότητας ή εισβολή στην ιδιωτική ζωή.

Η κατάσταση απορρήτου ενός λογαριασμού εμφανίζεται αμέσως μετά την επικύρωση.

Οι αυτόματες επανέλεγχοι ρυθμίζονται ώστε να εκτελούνται στο παρασκήνιο, αλλά οι χειροκίνητοι έλεγχοι μπορούν να εκτελούνται και καθημερινά.

Οι ειδοποιήσεις θα εμφανίζονται κάθε φορά που ανακαλύπτονται νέες διαρροές που περιλαμβάνουν οποιονδήποτε από τους επικυρωμένους email λογαριασμούς.

Για να ξεκινήσετε να ασφαλίζετε τις προσωπικές σας πληροφορίες:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Απόρρητο λογαριασμού**.
3. Επιλέξτε **ΕΝΑΡΞΗ**.
4. Η διεύθυνση email που χρησιμοποιήθηκε για τη δημιουργία του λογαριασμού σας Bitdefender εμφανίζεται και προστίθεται αυτόματα στη λίστα των λογαριασμών που παρακολουθούνται.
5. Για να προσθέσετε έναν άλλο λογαριασμό, πατήστε **ΠΡΟΣΘΗΚΗ ΛΟΓΑΡΙΑΣΜΟΥ** στο παράθυρο "Απόρρητο λογαριασμού" και, στη συνέχεια, πληκτρολογήστε τη διεύθυνση ηλεκτρονικού ταχυδρομείου.

   Πατήστε **ΠΡΟΣΘΗΚΗ** για να συνεχίσετε.

   Το Bitdefender πρέπει να επικυρώσει αυτόν τον λογαριασμό πριν εμφανίσει ιδιωτικές πληροφορίες. Επομένως, αποστέλλεται ένα email με κωδικό επικύρωσης στη email διεύθυνση που ορίστηκε.

   Ελέγξτε τα εισερχόμενά σας και, στη συνέχεια, πληκτρολογήστε τον κωδικό που λάβατε στην περιοχή **Απόρρητο λογαριασμού** της εφαρμογής

σας. Εάν δεν μπορείτε να βρείτε το email επικύρωσης στο φάκελο Εισερχόμενα, ελέγξτε το φάκελο Spam.

Εμφανίζεται η κατάσταση απορρήτου του επικυρωμένου λογαριασμού.

Αν διαπιστώσετε διαρροές σε οποιονδήποτε από τους λογαριασμούς σας, σας συνιστούμε να αλλάξετε τον κωδικό πρόσβασής σας το συντομότερο δυνατό. Για να δημιουργήσετε έναν ισχυρό και ασφαλή κωδικό πρόσβασης, λάβετε υπόψη σας τις παρακάτω συμβουλές:

- Φροντίστε να είναι τουλάχιστον 8 χαρακτήρες.
- Να περιλαμβάνετε μικρούς και μεγάλους χαρακτήρες.
- Προσθέστε τουλάχιστον έναν αριθμό ή σύμβολο όπως #, @, % or !.

Μόλις έχετε ασφαλίσει έναν λογαριασμό που ήταν μέρος μιας παραβίασης της ιδιωτικής ζωής, μπορείτε να επιβεβαιώσετε τις αλλαγές, επισημαίνοντας τις αναγνωρισμένες διαρροές ως **Επιλυμένες** . Για να το κάνετε αυτό:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Απόρρητο λογαριασμού**.
3. Επιλέξτε τον λογαριασμό που μόλις ασφαλίσατε.
4. Πατήστε την παραβίαση για την οποία ασφαλίσατε τον λογαριασμό.
5. Επιλέξτε **ΕΠΙΛΥΘΗΚΕ** για να ορίσετε ότι ο λογαριασμός είναι ασφαλής.

Όταν όλες οι διαρροές που ανιχνεύτηταν επισημανθούν ως **Επιλυμένες** , ο λογαριασμός δεν θα εμφανίζεται πλέον να έχει διαρρεύσει, τουλάχιστον έως ότου εντοπιστεί νέα διαρροή.

Για να σταματήσετε να ενημερώνεστε κάθε φορά που γίνεται αυτόματη σάρωση:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Ρυθμίσεις**.
3. Απενεργοποιήστε τον αντίστοιχο διακόπτη στην περιοχή Απόρρητο λογαριασμού.

27. ΚΛΕΊΔΩΜΑ ΕΦΑΡΜΟΓΏΝ

Εγκατεστημένες εφαρμογές όπως e-mail, φωτογραφίες, ή μηνύματα, μπορεί να περιέχουν προσωπικά δεδομένα που θα θέλατε να παραμείνουν προσωπικά περιορίζοντας επιλεκτικά την πρόσβαση σε αυτά.

Το App Lock σας βοηθά να μπλοκάρετε την ανεπιθύμητη πρόσβαση σε εφαρμογές με τον καθορισμό ενός κωδικού πρόσβασης ασφαλείας PIN. Ο κωδικός PIN που θα βάλετε πρέπει να αποτελείται τουλάχιστον από 4 ψηφία, αλλά όχι περισσότερα από 8, και είναι απαραίτητος κάθε φορά που θέλετε να αποκτήσετε πρόσβαση στις επιλεγμένες κλειστές εφαρμογές.

Εναλλακτικά σε συσκευές που υποστηρίζουν την επαλήθευση δακτυλικών αποτυπωμάτων, μπορεί να χρησιμοποιηθεί επιβεβαίωση δακτυλικών αποτυπωμάτων αντί του επιλεγμένου κωδικού PIN.

Ενεργοποίηση του App Lock

Για να περιορίσετε την πρόσβαση σε επιλεγμένες εφαρμογές, ρυθμίστε το App Lock από την κάρτα που εμφανίζεται στην επιφάνεια μετά την ενεργοποίηση του Anti-Theft.

Εναλλακτικά, μπορείτε να ενεργοποιήσετε το App Lock ακολουθώντας τα παρακάτω βήματα:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Κλείδωμα εφαρμογής**.
3. Πατήστε **ΕΝΕΡΓΟΠΟΙΗΣΗ**.
4. Να επιτρέπεται η πρόσβαση σε δεδομένα χρήσης για Bitdefender Ασφάλεια.
5. Να επιτρέπεται η **σχεδίαση πάνω από άλλες εφαρμογές** .
6. Πηγαίνετε πίσω στην εφαρμογή, διαμορφώστε τον κωδικό πρόσβασης και, στη συνέχεια, πιέστε **SET PIN**.

Σημείωση

Αυτό το βήμα είναι διαθέσιμο μόνο αν δεν έχετε ρυθμίσει προηγουμένως τον κωδικό PIN στο Anti-Theft.

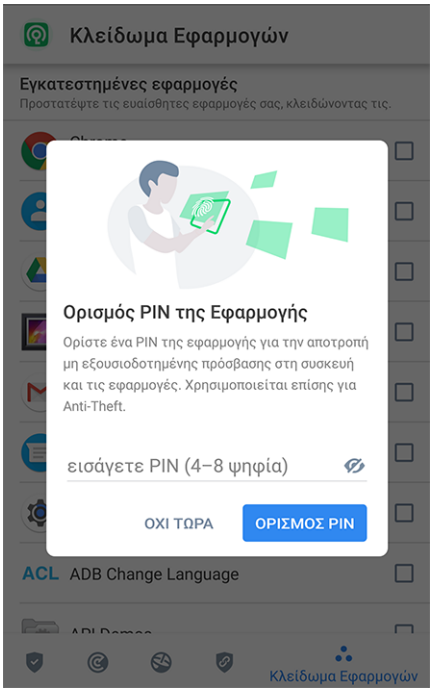
7. Ενεργοποιήστε την επιλογή Στιγμιαία Φωτογράφιση για να εντοπίσετε κάθε εισβολέα που θα προσπαθήσει να αποκτήσει πρόσβαση στα ιδιωτικά σας δεδομένα.

Σημείωση
Πρόσθετα δικαιώματα απαιτούνται για το Android 6 για τη λειτουργία στιγμιαίας φωτογραφίας.
Για να την ενεργοποιήσετε, επιτρέψτε το **Antivirus** να παίρνει φωτογραφίες και βίντεο.

8. Επιλέξτε τις εφαρμογές που θέλετε να προστατεύσετε.

Χρησιμοποιώντας το λανθασμένο PIN ή το δακτυλικό αποτύπωμα πέντε φορές στη σειρά, θα ενεργοποιηθεί μια περίοδος αναμονής 30 δευτερολέπτων. Με αυτόν τον τρόπο, οποιαδήποτε απόπειρα εισβολής στις προστατευμένες εφαρμογές θα αποκλειστεί.

Σημείωση
Ο ίδιος κωδικός PIN χρησιμοποιείται από το Anti-Theft για να σας βοηθήσει να εντοπίσετε τη συσκευή σας.



Κλείδωμα Εφαρμογών

ΛΕΙΤΟΥΡΓΙΑ ΚΕΙΔΩΜΑΤΟΣ

Την πρώτη φορά που προσθέτετε μια εφαρμογή στο Κλείδωμα εφαρμογής, Από εδώ μπορείτε να επιλέξετε πότε η λειτουργία Κλείδωμα εφαρμογής θα πρέπει να προστατεύει τις εφαρμογές που είναι εγκατεστημένες στη συσκευή σας.

Μπορείτε να επιλέξετε από μία από τις παρακάτω επιλογές:

- **Απαιτείται ξεκλείδωμα κάθε φορά** - κάθε φορά που έχετε πρόσβαση στις κλειδωμένες εφαρμογές, θα χρησιμοποιηθεί ο κωδικός PIN ή το αποτύπωμα σας.
- **Ξεκλείδωμα έως ότου η σβήσει οθόνη** - η πρόσβαση στις εφαρμογές σας θα είναι ενεργή μέχρι να απενεργοποιηθεί η οθόνη.

- **Κλείδωμα μετά από 30 δευτερόλεπτα** - μπορείτε να πραγματοποιήσετε έξοδο και να αποκτήσετε πρόσβαση στις ξεκλειδωμένες εφαρμογές σας εντός 30 δευτερολέπτων.

Αν θέλετε να αλλάξετε την επιλεγμένη ρύθμιση:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Ρυθμίσεις**.
3. Πατήστε **Απαιτείται ξεκλείδωμα κάθε φορά** στην περιοχή Κλείδωμα εφαρμογής.
4. Επιλέξτε την επιθυμητή ρύθμιση

Ρυθμίσεις Κλειδώματος Εφαρμογών

Για μια προηγμένη διαμόρφωση του Κλειδώματος Εφαρμογών:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Ρυθμίσεις**.

Στην περιοχή Κλείδωμα Εφαρμογής μπορείτε να διαμορφώσετε τις παρακάτω επιλογές:

- **Σύσταση ευαίσθητης εφαρμογής.** - λαμβάνετε μια ειδοποίηση κλειδώματος κάθε φορά που εγκαθιστάτε μια ευαίσθητη εφαρμογή.
- **Απαιτείται ξεκλείδωμα κάθε φορά** - επιλέξτε μία από τις διαθέσιμες επιλογές κλειδώματος και ξεκλειδώματος.
- **Έξυπνο ξεκλείδωμα** - διατηρεί τις εφαρμογές ξεκλείδωτες ενώ είστε συνδεδεμένοι σε αξιόπιστα Wi-Fi δίκτυα .
- **Τυχαίο πληκτρολόγιο** - αποτρέψτε την ανάγνωση του PIN μέσω των τυχαιοποιημένων θέσεων αριθμών.

Στιγμιαία Φωτογραφία

Με την Bitdefender Στιγμιαία φωτογραφία, μπορείτε να ξαφνιάσετε τους φίλους ή τους συγγενείς σας. Με αυτό τον τρόπο μπορείτε να εκπαιδεύσετε τα περίεργα μάτια τους να μην βλέπουν τα προσωπικά αρχεία σας ή τις εφαρμογές που χρησιμοποιείτε.

Αυτό το χαρακτηριστικό λειτουργεί εύκολα: κάθε φορά που ο κωδικός PIN που έχετε ορίσει για την προστασία εφαρμογές σας εισαχθεί λάθος τρεις φορές στη σειρά, μια φωτογραφία λαμβάνεται χρησιμοποιώντας την μπροστινή κάμερα. Η φωτογραφία αποθηκεύεται μαζί με χρονική σήμανση και την ενέργεια, και μπορεί να δει κανείς όταν ανοίγετε το Bitdefender Mobile Security και κάνετε πρόσβαση στη λειτουργία App Lock.

Σημείωση
Αυτό το χαρακτηριστικό είναι διαθέσιμο μόνο για τα τηλέφωνα που έχουν μια μπροστινή κάμερα.

Για να ρυθμίσετε τις παραμέτρους της λειτουργίας Snap Photo για την εφαρμογή Κλείδωμα Εφαρμογών:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Ρυθμίσεις**.
3. Ενεργοποιήστε τον αντίστοιχο διακόπτη στην περιοχή Snap Photo.

Οι στιγμιαίες φωτογραφίες που τραβήχτηκαν όταν έγινε εσφαλμένη εισαγωγή PIN, εμφανίζονται στο μενού Κλείδωμα Εφαρμογών και μπορούν να προβληθούν σε πλήρη οθόνη.

Εναλλακτικά, μπορούν να προβληθούν στον Bitdefender λογαριασμό:

1. Μετάβαση σε: https://central.bitdefender.com.
2. Συνδεθείτε στο λογαριασμό σας
3. Πατήστε στο εικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι συσκευές μου**.
4. Επιλέξτε τη συσκευή σας Android και, στη συνέχεια, την καρτέλα **Anti-Theft** .
5. Επιλέξτε δίπλα στο **Ελέγξτε τα στιγμιότυπα σας** για να δείτε τις πιο πρόσφατες ληφθείσες φωτογραφίες.

Αποθηκεύονται μόνο οι δύο πιο πρόσφατες φωτογραφίες.

Για να διακόψετε το ανέβασμα φωτογραφιών στο Bitdefender λογαριασμό σας:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.

2. Επιλέξτε **Ρυθμίσεις**.
3. Απενεργοποιήστε **Ανέβασμα φωτογραφίας** στην περιοχή Snap Photo.

Smart Unlock

Ένας εύκολος τρόπος για να σταματήσει η λειτουργία App Lock να ζητά να εισάγετε τον κωδικό PIN ή την επιβεβαίωση δακτυλικών αποτυπωμάτων για τις προστατευόμενες εφαρμογές κάθε φορά που θα έχουν πρόσβαση σε αυτά είναι για να ενεργοποιήσετε το Smart Unlock.

Με το Smart Unlock μπορείτε να ορίσετε ως αξιόπιστα τα δίκτυα Wi-Fi που συνήθως συνδέεστε και όταν συνδέεται με αυτά, το Lock App θα απενεργοποιηθεί για τις προστατευόμενες εφαρμογές.

Για να διαμορφώσετε τη δυνατότητα Έξυπνο Ξεκλείδωμα:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Κλείδωμα εφαρμογής**.
3. Πατήστε το κουμπί .
4. Πατήστε το διακόπτη δίπλα στο **Έξυπνο ξεκλείδωμα**, εάν η λειτουργία δεν είναι ακόμη ενεργοποιημένη.

   Επικυρώστε χρησιμοποιώντας το δακτυλικό σας αποτύπωμα ή το PIN σας.

   Την πρώτη φορά που θα ενεργοποιήσετε τη λειτουργία, θα πρέπει να ενεργοποιήσετε την άδεια τοποθεσίας. Επιλέξτε το κουμπί **ΕΠΙΤΡΕΠΩ**, και στη συνέχεια ξανεπιλέξτε το κουμπί **ΕΠΙΤΡΕΠΩ**.
5. Επιλέξτε **ΠΡΟΣΘΗΚΗ** για να ρυθμίσετε τη σύνδεση Wi-Fi που χρησιμοποιείτε αυτήν τη στιγμή ως αξιόπιστη.

Κάθε φορά που αλλάζετε γνώμη, απενεργοποιήστε αυτή την δυνατότητα και τα δίκτυα Wi-Fi που έχετε θέσει ως αξιόπιστα θα αντιμετωπίζονται ως μη αξιόπιστα.

28. ΑΝΑΦΟΡΕΣ

Η λειτουργία Αναφορές διατηρεί ένα λεπτομερές αρχείο καταγραφής των γεγονότων που αφορούν τη δραστηριότητα σάρωσης στη συσκευή σας.

Κάθε φορά που συμβαίνει κάτι σχετικό με την ασφάλεια της συσκευής σας, ένα νέο μήνυμα, προστίθεται στις Αναφορές.

Για να αποκτήσετε πρόσβαση στην ενότητα Αναφορές:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Αναφορές**.

Οι ακόλουθες καρτέλες είναι διαθέσιμες στο παράθυρο Αναφορές:

- **ΕΒΔΟΜΑΔΙΑΙΑ ΑΝΑΦΟΡΑ** - εδώ έχετε πρόσβαση στην κατάσταση ασφαλείας και τις εκτελούμενες εργασίες από την τρέχουσα και την προηγούμενη εβδομάδα. Η έκθεση της τρέχουσας εβδομάδας παράγεται κάθε Κυριακή και θα λάβετε μια ειδοποίηση που σας ενημερώνει όταν γίνει διαθέσιμη.

  Κάθε εβδομάδα μια νέα συμβουλή θα εμφανιστεί σε αυτή την ενότητα, οπότε φροντίστε να ελέγχετε τακτικά για να πάρετε το καλύτερο από την εφαρμογή.

  Για να σταματήσετε να λαμβάνετε ειδοποιήσεις κάθε φορά που δημιουργείται μία αναφορά:

  1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
  2. Επιλέξτε **Ρυθμίσεις**.
  3. Απενεργοποιήστε το διακόπτη **Νέα ειδοποίηση αναφοράς** στην περιοχή Αναφορές.
- **ΔΡΑΣΤΗΡΙΟΤΗΤΑ** - εδώ μπορείτε να ελέγξετε λεπτομερείς πληροφορίες σχετικά με τη δραστηριότητα της εφαρμογής σας Bitdefender Mobile Security από τότε που εγκαταστάθηκε στη συσκευή σας Android.

  Για να διαγράψετε το διαθέσιμο αρχείο καταγραφής δραστηριοτήτων:

  1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
  2. Επιλέξτε **Ρυθμίσεις**.

3. Επιλέξτε **Εκκαθάριση αρχείου δραστηριοτήτων** και στη συνέχεια πιέστε **ΚΑΘΑΡΙΣΜΟΣ**.

29. WEARON

Με το Bitdefender WearON μπορείτε εύκολα να βρείτε το smartphone σας είτε αν το έχετε αφήσει στο γραφείο σε μια αίθουσα συσκέψεων ή κάτω από ένα μαξιλάρι στον καναπέ σας. Η συσκευή μπορεί να βρεθεί ακόμη και αν έχει ενεργοποιηθεί η λειτουργία σίγασης.

Κρατήστε αυτή τη λειτουργία ενεργοποιημένη για να βεβαιωθείτε ότι έχετε πάντα το smartphone σας κοντά σας.

Σημείωση
Η λειτουργία είναι συμβατή με Android 4.3 και Android Wear.

Ενεργοποίηση του WearON

Για να χρησιμοποιήσετε το WearON, δεν έχετε παρά να συνδέσετε το SmartWatch σας με το Bitdefender Mobile Security και να ενεργοποιήσετε τη δυνατότητα με την ακόλουθη φωνητική εντολή:

Start:<Where is my phone>

Bitdefender WearON έχει δύο εντολές:

1. **Phone Alert**

   Με τη λειτουργία Phone Alert μπορείτε να βρείτε γρήγορα το smartphone σας κάθε φορά που θα απομακρύνεστε πολύ από αυτό.

   Αν έχετε μαζί σας το smartwatch σας, ανιχνεύει αυτόματα την εφαρμογή στο τηλέφωνό σας και δονείται όταν είναι πολύ μακριά από το ρολόι σας και οι συσκευές χάνουν τη σύνδεση Bluetooth.

   Για να ενεργοποιήσετε αυτή τη λειτουργία, ανοίξτε το Bitdefender Mobile Security, πατήστε **Γενικές Ρυθμίσεις** στο μενού και επιλέξτε το αντίστοιχο διακόπτη κάτω από την ενότητα WearON.

2. **Συναγερμός Κραυγής**

   Το να βρείτε το τηλέφωνό σας δεν ήταν ποτέ ευκολότερο. Κάθε φορά που θα ξεχάσετε πού αφήσατε το τηλέφωνό σας, επιλέξτε την εντολή Scream στο ρολόι σας για να κάνετε το τηλέφωνό σας να φωνάξει.

30. ΣΧΕΤΙΚΆ

Για να βρείτε πληροφορίες για την Bitdefender Mobile Security έκδοση που έχετε εγκαταστήσει για να δείτε τη Συμφωνία Συνδρομής, την Πολιτική Απορρήτου και Άδειες ανοιχτού κώδικα:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Ρυθμίσεις**.
3. Επιλέξτε την επιθυμητή επιλογή στην περιοχή Πληροφορίες.

31. BITDEFENDER CENTRAL

Bitdefender Central είναι η διαδικτυακή πλατφόρμα όπου μπορείτε να έχετε πρόσβαση σε online υπηρεσίες και χαρακτηριστικά του προϊόντος αυτού και μπορείτε να εκτελέσετε από απόσταση σημαντικές εργασίες σε συσκευές όπου το Bitdefender είναι εγκατεστημένο. Μπορείτε να συνδεθείτε στον Bitdefender λογαριασμό από οποιονδήποτε υπολογιστή ή κινητή συσκευή που συνδέεται στο Internet μέσω του https://central.bitdefender.com, ή απευθείας μέσω της Bitdefender Central εφαρμογής για Android και iOS συσκευές.

Για να εγκαταστήσετε την Bitdefender Centralεφαρμογή στις συσκευές σας:

- **Σε Android** - αναζητήστε Bitdefender Central στο Google Play και στη συνέχεια κατεβάστε και εγκαταστήστε την εφαρμογή. Ακολουθήστε τα απαιτούμενα βήματα για να ολοκληρώσετε την εγκατάσταση.
- **Σε iOS** - αναζητήστε Bitdefender Central στο App Store και στη συνέχεια κάντε λήψη και εγκατάσταση της εφαρμογής. Ακολουθήστε τα απαιτούμενα βήματα για να ολοκληρώσετε την εγκατάσταση.

Μόλις έχετε πρόσβαση, μπορείτε να αρχίσετε να κάνετε τα εξής:

- Λήψη και εγκατάσταση του Bitdefender σε Windows, macOS, iOS και σε Android λειτουργικά συστήματα. Τα προϊόντα που διατίθενται για λήψη είναι:
  - Bitdefender Mobile Security
  - Bitdefender Mobile Security για iOS
  - Bitdefender Antivirus για Mac
  - Η σειρά προϊόντων Bitdefender για Windows
- Διαχειριστείτε και ανανεώστε τις Bitdefender συνδρομές σας.
- Προσθέστε νέες συσκευές στο δίκτυό σας και διαχειριστείτε τις από όπου κι αν βρίσκεστε.
- Προστατέψτε τις συσκευές δικτύου και τα δεδομένα τους από κλοπή ή απώλεια με το Anti-Theft.

Πρόσβαση στον Bitdefender λογαριασμό σας

Υπάρχουν διάφοροι τρόποι για να αποκτήσετε πρόσβαση στο Bitdefender Central:

- Από τον πλοηγό σας:
  1. Ανοίξτε ένα πρόγραμμα περιήγησης σε οποιαδήποτε συσκευή με πρόσβαση στο Διαδίκτυο.
  2. Μετάβαση σε: https://central.bitdefender.com.
  3. Συνδεθείτε στο λογαριασμό σας χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
- Από την συσκευή σας Android ή iOS:

  Ανοίξτε την Bitdefender Central εφαρμογή που έχετε εγκαταστήσει.

Σημείωση
Σε αυτό το υλικό παρέχονται οι επιλογές και οι οδηγίες που διατίθενται στην πλατφόρμα web.

2-Factor Authentication

Η μέθοδος 2-Factor Authentication προσθέτει ένα πρόσθετο επίπεδο ασφαλείας στον Bitdefenderλογαριασμό σας, απαιτώντας έναν κωδικό επαλήθευσης εκτός από τα διαπιστευτήριά σας σύνδεσης. Έτσι θα αποτρέψετε την υποκλοπή του λογαριασμού σας και θα προστατευτείτε από επιθέσεις.

Ενεργοποίηση 2-Factor Authentication

Ενεργοποιώντας το 2-Factor Authentication, ο Bitdefender λογαριασμός σας θα είναι πολύ πιο ασφαλής. Η ταυτότητά σας θα επαληθεύεται κάθε φορά που θα συνδεθείτε από διαφορετικές συσκευές,για να εγκαταστήσετε ένα από τα Bitdefender προϊόντα, να ελέγξτε την κατάσταση της συνδρομής σας ή να εκτελέστε απομακρυσμένα εργασίες στις συσκευές σας.

Για να ενεργοποιήσετε το 2-Factor Authentication:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο 👤 στην επάνω δεξιά γωνία της οθόνης.
3. Κάντε κλικ στο **Ο Bitdefender Λογαριασμός μου** στο μενού.

4. Επιλέξτε την καρτέλα **Κωδικός και ασφάλεια**
5. Επιλέξτε **2-Factor Authentication**.
6. Επιλέξτε **ΕΝΑΡΞΗ**.

   Επιλέξτε μία από τις ακόλουθες μεθόδους:

   - **Εφαρμογή Authenticator** - χρησιμοποιήστε μια εφαρμογή ελέγχου ταυτότητας για να δημιουργήσετε έναν κωδικό κάθε φορά που θέλετε να συνδεθείτε στον Bitdefender λογαριασμό σας.

     Εάν θέλετε να χρησιμοποιήσετε μια εφαρμογή ελέγχου ταυτότητας, αλλά δεν είστε σίγουροι για το τι θα επιλέξετε, υπάρχει διαθέσιμη μια λίστα με τις εφαρμογές ελέγχου ταυτότητας που συστήνουμε.

     a. Επιλέξτε **ΧΡΗΣΙΜΟΠΟΙΗΣΤΕ AUTHENTICATOR ΕΦΑΡΜΟΓΗ** για να ξεκινήσετε.

     b. Για να συνδεθείτε σε μια συσκευή Android ή iOS, χρησιμοποιήστε τη συσκευή σας για να σαρώσετε τον QR κωδικό .

        Για να συνδεθείτε σε laptop ή επιτραπέζιο υπολογιστή, μπορείτε να προσθέσετε χειροκίνητα τον εμφανιζόμενο κώδικα.

        Επιλέξτε **ΣΥΝΕΧΕΙΑ**.

     c. Εισάγετε τον κωδικό που παρέχεται από την εφαρμογή ή αυτόν που εμφανίζεται στο προηγούμενο βήμα και στη συνέχεια πατήστε **ΕΝΕΡΓΟΠΟΙΗΣΗ** .

   - **E-mail** - κάθε φορά που συνδέεστε στο Bitdefender λογαριασμό σας, θα σταλεί στο εισερχόμενό σας email ένας κωδικός επαλήθευσης. στη συνέχεια πληκτρολογήστε τον κωδικό που λάβατε.

     a. Επιλέξτε **ΧΡΗΣΙΜΟΙΗΣΤΕ EMAIL** για να ξεκινήσετε.

     b. Ελέγξτε το email και πληκτρολογήστε τον παρεχόμενο κωδικό.

        Σημειώστε ότι έχετε πέντε λεπτά για να ελέγξετε τον email λογαριασμό και να πληκτρολογήσετε τον παραγόμενο κώδικα. Εάν λήξει ο χρόνος, θα πρέπει να δημιουργήσετε έναν νέο κωδικό ακολουθώντας τα ίδια βήματα.

     c. Επιλέξτε **ΕΝΕΡΓΟΠΟΙΗΣΗ**.

     d. Σας παρέχονται δέκα κωδικοί ενεργοποίησης. Μπορείτε να τους αντιγράψετε, να τους κατεβάσετε ή να εκτυπώσετε τη λίστα και να την χρησιμοποιήσετε σε περίπτωση που χάσετε το email ή δεν

θα μπορείτε να συνδεθείτε. Κάθε κωδικός μπορεί να χρησιμοποιηθεί μόνο μία φορά.

e. Επιλέξτε **ΕΤΟΙΜΟ**.

Σε περίπτωση που θέλετε να σταματήσετε να χρησιμοποιείτε το 2-Factor Authentication:

1. Επιλέξτε **ΑΠΕΝΕΡΓΟΠΟΙΗΣΗ 2-FACTOR AUTHENTICATION**.
2. Ελέγξτε την εφαρμογή ή το email σας και πληκτρολογήστε τον κωδικό που λάβατε.

   Σημειώστε ότι έχετε πέντε λεπτά για να ελέγξετε τον email λογαριασμό σας και πληκτρολογήσετε τον παραγόμενο κώδικα. Εάν λήξει ο χρόνος, θα πρέπει να δημιουργήσετε έναν νέο κωδικό ακολουθώντας τα ίδια βήματα.
3. Επιβεβαιώστε την επιλογή σας.

Προσθήκη έμπιστης συσκευής

Για να βεβαιωθείτε ότι μόνο εσείς μπορείτε να αποκτήσετε πρόσβαση στο Bitdefender λογαριασμό σας, ίσως χρειαστεί πρώτα έναν κωδικό ασφαλείας. Εάν θέλετε να παραλείψετε αυτό το βήμα κάθε φορά που συνδέεστε από την ίδια συσκευή, σας συνιστούμε να την ορίσετε ως αξιόπιστη συσκευή.

Για να δηλώσετε συσκευές ως αξιόπιστες:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο 👤 στην επάνω δεξιά γωνία της οθόνης.
3. Κάντε κλικ στο **Ο Bitdefender Λογαριασμός μου** στο μενού.
4. Επιλέξτε την καρτέλα **Κωδικός και ασφάλεια**
5. Επιλέξτε **Αξιόπιστες συσκευές**.
6. Εμφανίζεται η λίστα με τις συσκευές όπου το Bitdefender που είναι εγκατεστημένο. Επιλέξτε την επιθυμητή συσκευή.

Μπορείτε να προσθέσετε όσες συσκευές επιθυμείτε, υπό την προϋπόθεση ότι έχει εγκατασταθεί το Bitdefender και η συνδρομή σας είναι έγκυρη.

Οι συσκευές μου

Η περιοχή **MY DEVICES** στον Bitdefender λογαριασμό σας, σας δίνει τη δυνατότητα να εγκαταστήσετε, να διαχειριστείτε και να ολοκληρώσετε ενέργειες εξ αποστάσεως στο Bitdefender προϊόν σας σε οποιαδήποτε συσκευή, υπό την προϋπόθεση ότι είναι ενεργοποιημένη και συνδεδεμένη στο Internet. Οι κάρτες συσκευής εμφανίζουν το όνομα της συσκευής, την κατάσταση προστασίας και αν υπάρχουν κίνδυνοι ασφαλείας που επηρεάζουν την προστασία των συσκευών σας.

Για να εντοπίσετε εύκολα τις συσκευές σας, μπορείτε να προσαρμόσετε το όνομα της συσκευής:

1. Πρόσβαση στο Bitdefender Central.
2. Πατήστε στο ☰ εικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι συσκευές μου**.
3. Πατήστε την επιθυμητή κάρτα συσκευής και, στη συνέχεια, το εικονίδιο ⋮ στην επάνω δεξιά γωνία της οθόνης.
4. Επιλέξτε **Ρυθμίσεις**.
5. Πληκτρολογήστε ένα νέο όνομα στο πεδίο **Όνομα συσκευής** και, στη συνέχεια, επιλέξτε **Αποθήκευση** .

Μπορείτε να δημιουργήσετε και να ορίσετε έναν ιδιοκτήτη σε κάθε μία από τις συσκευές σας για καλύτερη διαχείριση:

1. Πρόσβαση στο Bitdefender Central.
2. Πατήστε στο ☰ εικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι συσκευές μου**.
3. Πατήστε την επιθυμητή κάρτα συσκευής και, στη συνέχεια, το εικονίδιο ⋮ στην επάνω δεξιά γωνία της οθόνης.
4. Επιλέξτε **Προφίλ**.
5. Κάντε κλικ στο **Προσθήκη κατόχου** και στη συνέχεια συμπληρώστε τα αντίστοιχα πεδία. Προσαρμόστε το προφίλ προσθέτοντας μια φωτογραφία και επιλέγοντας μια ημερομηνία γέννησης.
6. Κάντε κλικ στο **ADD** για να αποθηκεύσετε ένα προφίλ.
7. Επλέξτε τον επιθυμητό ιδιοκτήτη από τη λίστα **Device owner** και στη συνέχεια κάντε κλικ στο **ASSIGN**.

Για περισσότερες ενέργειες εξ αποστάσεως και πληροφορίες σχετικά με το Bitdefender προϊόν σας σε μια συγκεκριμένη συσκευή, κάντε κλικ στην επιθυμητή κάρτα συσκευής.

Μόλις κάνετε κλικ σε μια κάρτα συσκευής, οι ακόλουθες καρτέλες είναι διαθέσιμες:

- **Ταμπλώ**. Σε αυτό το παράθυρο μπορείτε να δείτε λεπτομέρειες σχετικά με την επιλεγμένη συσκευή, να ελέγξετε την κατάσταση προστασίας, την κατάσταση του Bitdefender VPN και πόσες απειλές έχουν αποκλειστεί τις τελευταίες επτά ημέρες. Η κατάσταση προστασίας μπορεί να είναι πράσινη, όταν δεν υπάρχει κανένα πρόβλημα που να επηρεάζει τη συσκευή σας, κίτρινη όταν η συσκευή σας χρειαστεί την προσοχή σας ή κόκκινη όταν η συσκευή κινδυνεύει. Όταν υπάρχουν ζητήματα που επηρεάζουν τη συσκευή σας, κάντε πατήσετε στο αναπτυσσόμενο βέλος στην επάνω περιοχή κατάστασης για να μάθετε περισσότερες λεπτομέρειες. Από εδώ μπορείτε να διορθώσετε χειροκίνητα ζητήματα που επηρεάζουν την ασφάλεια των συσκευών σας.
- **ΠΡΟΣΤΑΣΙΑ**. Από αυτό το παράθυρο μπορείτε να εκτελέσετε μια Σάρωση εξ αποστάσεως στη συσκευή σας. Κάντε κλικ στο κουμπί **ΣΑΡΩΣΗ** για να ξεκινήσει η διαδικασία. Μπορείτε επίσης να ελέγξετε πότε πραγματοποιήθηκε η τελευταία σάρωση στη συσκευή καθώς και μία διαθέσιμη αναφορά της τελευταίας σάρωσης με τις πιο σημαντικές πληροφορίες.
- **Anti-theft**. Σε περίπτωση που δεν θυμάστε που αφήσατε τη συσκευή σας, με τη λειτουργία Anti-Theft μπορείτε να την εντοπίσετε και να πραγματοποιήσετε ενέργειες εξ αποστάσεως. Κάντε κλικ στο **LOCATE** για να μάθετε τη θέση της συσκευής. Η τελευταία γνωστή θέση θα εμφανιστεί, μαζί με την ώρα και την ημερομηνία. Για περισσότερες λεπτομέρειες σχετικά με αυτή τη δυνατότητα, ανατρέξτε στο "*Χαρακτηριστικά Anti-Theft*" (p. 313).

Οι Συνδρομές μου

Η Bitdefender Central πλατφόρμα σας δίνει τη δυνατότητα να διαχειριστείτε εύκολα τις συνδρομές που έχετε για όλες τις συσκευές σας.

Ελέγξτε τις διαθέσιμες συνδρομές

Για να ελέγξετε τις διαθέσιμες συνδρομές σας:

1. Πρόσβαση στο Bitdefender Central.
2. Πατήστε στο ≡ εικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι συνδρομές μου**.

Εδώ έχετε πληροφορίες σχετικά με τη διαθεσιμότητα των συνδρομών που έχετε στην κατοχή σας και τον αριθμό των συσκευών που χρησιμοποιούν κάθε μία από αυτές.

Μπορείτε να προσθέσετε μια νέα συσκευή σε μια συνδρομή ή να την ανανεώσετε, επιλέγοντας μια κάρτα συνδρομής.

Προσθέστε μια νέα συσκευή

Εάν η συνδρομή σας καλύπτει περισσότερες από μία συσκευή, μπορείτε να προσθέσετε μια νέα συσκευή και να εγκαταστήσετε το Bitdefender Mobile Security σε αυτή, όπως περιγράφεται στο "Εγκατάσταση του Bitdefender Mobile Security" (p. 298).

Παράταση συνδρομής

Αν υπάρχουν λιγότερες από 30 ημέρες στην συνδρομή σας, και δεν έχετε επιλέξει για αυτόματη ανανέωση, μπορείτε να ανανεώσετε με μη αυτόματο τρόπο, ακολουθώντας τα παρακάτω βήματα:

1. Πρόσβαση στο Bitdefender Central.
2. Πατήστε στο ≡ εικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι συνδρομές μου**.
3. Επιλέξτε την επιθυμητή κάρτα συνδρομής.
4. Κάντε κλικ στο **RENEW** για να συνεχίσετε.

Μια ιστοσελίδα ανοίγει στο πρόγραμμα πλοήγησης σας, όπου μπορείτε να ανανεώσετε τη Bitdefender συνδρομή σας.

32. ΣΥΧΝΈΣ ΕΡΩΤΉΣΕΙΣ

Γιατί το Bitdefender Mobile Security απαιτεί σύνδεση στο Internet;.

Η εφαρμογή θα πρέπει να επικοινωνήσει με τους Bitdefender servers προκειμένου να καθορίσει το επίπεδο ασφάλειας των εφαρμογών που σαρώνει και τις ιστοσελίδες που επισκέπτεστε, καθώς επίσης και να λάβει εντολές από το Bitdefender λογαριασμό σας, όταν χρησιμοποιεί την λειτουργία Anti-Theft.

Για ποιο σκοπό χρειάζεται το Bitdefender Mobile Security την κάθε άδεια;.

- Η πρόσβαση στο Internet -> χρησιμοποιείται για την επικοινωνία με το Cloud
- Διαβάστε την κατάσταση και ταυτότητα -> του τηλεφώνου που χρησιμοποιήθηκε για να ανιχνεύσει αν η συσκευή είναι συνδεδεμένη στο Internet και για να αποσπάσει ορισμένες πληροφορίες συσκευής που απαιτούνται για να δημιουργήσουν ένα μοναδικό αναγνωριστικό επικοινωνίας με το Bitdefender cloud.
- Διαβάστε και γράψτε σελιδοδείκτες του προγράμματος περιήγησης -> Το Web Protection διαγράφει κακόβουλες ιστοσελίδες από το ιστορικό περιήγησης.
- Διαβάστε τα αρχεία καταγραφής -> Το Bitdefender Mobile Security εντοπίζει ίχνη δραστηριότητας κακόβουλου λογισμικού από τα Android logs.
- Τοποθεσία -> απαιτείται για απομακρυσμένη τοποθεσία.
- Κάμερα -> απαιτείτε για στιγμιαία φωτογραφία.
- Αποθήκευση -> χρησιμεύει για να επιτρέψει το Malware Scanner για να ελέγξετε την κάρτα SD.

Πώς μπορώ να σταματήσω την υποβολή Bitdefender πληροφοριών σχετικά με ύποπτες εφαρμογές;.

Από προεπιλογή, το Bitdefender Mobile Security αποστέλλει αναφορές στους Bitdefender servers για το θέμα αυτής της εφαρμογής. Αυτές οι πληροφορίες είναι απαραίτητες για την καλύτερη κατανόηση της εφαρμογής. Σε περίπτωση που θέλετε να μας στείλετε πληροφορίες σχετικά με ύποπτες εφαρμογές:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.

2. Επιλέξτε **Ρυθμίσεις**.
3. Απενεργοποιήστε το **Ανίχνευση σε cloud** στην περιοχή Σαρωτής κακόβουλου λογισμικού.

Πού μπορώ να δω λεπτομέρειες σχετικά με τη δραστηριότητα της εφαρμογής;.

Το Bitdefender Mobile Security διατηρεί ένα αρχείο καταγραφής όλων των σημαντικών ενεργειών, αλλαγών κατάστασης και άλλων κρίσιμων μηνυμάτων που σχετίζονται με την δραστηριότητα του. Για να αποκτήσετε πρόσβαση στη δραστηριότητα της εφαρμογής:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Αναφορές**.

   Στο παράθυρο ΕΒΔΟΜΑΔΙΑΙΕΣ ΑΝΑΦΟΡΕΣ μπορείτε να έχετε πρόσβαση στα αποτελέσματα της εβδομαδιαίας δραστηριότητάς της εφαρμογής και στο παράθυρο ACTIVITY LOG μπορείτε να δείτε πληροφορίες σχετικά με τη δραστηριότητα της Bitdefender εφαρμογής σας

Ξέχασα τον κωδικό PIN που όρισα για την προστασία της εφαρμογής μου. Τι μπορώ να κάνω;.

1. Πρόσβαση στο Bitdefender Central.
2. Πατήστε στο εικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε **Οι συσκευές μου**.
3. Πατήστε την επιθυμητή κάρτα συσκευής και, στη συνέχεια, το εικονίδιο στην επάνω δεξιά γωνία της οθόνης.
4. Επιλέξτε **Ρυθμίσεις**.
5. Ανακτήστε τον κωδικό PIN από το πεδίο **PIN Εφαρμογής**

Πώς μπορώ να αλλάξω τον κωδικό PIN που έχω ρυθμίσει για το Κλείδωμα Εφαρμογών και Anti-Theft;.

Αν θέλετε να αλλάξετε τον κωδικό PIN που έχετε ρυθμίσει για το Κλείδωμα Εφαρμογών και Anti-Theft:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Ρυθμίσεις**.

3. Επιλέξτε Ασφάλεια **ΚΩΔΙΚΟΣ PIN** στην περιοχή Anti-Theft.
4. Πληκτρολογήστε τον τρέχοντα κωδικό PIN.
5. Πληκτρολογήστε τον νέο κωδικό PIN που θέλετε να ορίσετε.

Πώς μπορώ να απενεργοποιήσω τη λειτουργία Κλείδωμα εφαρμογής;.

Δεν υπάρχει επιλογή απενεργοποίησης για τη λειτουργία "Κλείδωμα εφαρμογής", αλλά μπορείτε να την απενεργοποιήσετε εύκολα, διαγράφοντας τα πλαίσια ελέγχου δίπλα στις επιλεγμένες εφαρμογές, αφού επικυρώσετε το PIN ή το δακτυλικό αποτύπωμα που έχετε ορίσει.

Πώς μπορώ να ορίσω ένα άλλο ασύρματο δίκτυο ως αξιόπιστο;.

Πρώτον, πρέπει να συνδέσετε τη συσκευή σας στο ασύρματο δίκτυο που θέλετε να ορίσετε ως έμπιστο. Ακολουθήστε τα παρακάτω βήματα:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Επιλέξτε **Κλείδωμα εφαρμογής**.
3. Επιλέξτε στην πάνω δεξιά γωνία.
4. Πατήστε **ΠΡΟΣΘΗΚΗ** δίπλα στο δίκτυο που θέλετε να ορίσετε ως αξιόπιστο.

Πώς μπορώ να σταματήσω να βλέπω στιγμιαίες φωτογραφίες που ελήφθησαν στην συσκευές μου;.

Για να σταματήσετε να βλέπετε τις στιγμιαίες φωτογραφίες που ελήφθησαν στις συσκευές σας:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στην επάνω δεξιά γωνία της οθόνης.
3. Κάντε κλικ στο **Ο Λογαριασμός μου** στο μενού.
4. Επιλέξτε την καρτέλα **Settings**.
5. Απενεργοποιήστε την επιλογή **Show/don't show snap photos taken on your devices**.

Πώς μπορώ να διατηρήσω ασφαλείς τις ηλεκτρονικές μου αγορές;.

Οι αγορές στο διαδίκτυο γίνονται υψηλού κινδύνου όταν αγνοούνται κάποιες λεπτομέρειες. Για να μην γίνετε θύμα απάτης, σας συνιστούμε τα εξής:

- Διατηρήστε την εφαρμογή ασφαλείας σας ενημερωμένη.
- Υποβάλετε τις ηλεκτρονικές πληρωμές μόνο σε προστατευμένο περιβάλλον.
- Χρησιμοποιήστε το VPN όταν συνδέεστε στο Internet από δημόσια και μη ασφαλή ασύρματα δίκτυα.
- Δώστε προσοχή στους κωδικούς πρόσβασης που έχετε αντιστοιχίσει στους λογαριασμούς σας στο διαδίκτυο. Πρέπει να είναι ισχυροί, συμπεριλαμβανομένων κεφαλαίων και πεζών γραμμάτων, αριθμών και συμβόλων (@,!,%, #, κλπ.).
- Βεβαιωθείτε ότι οι πληροφορίες που στέλνετε είναι πάνω από ασφαλείς συνδέσεις. Η επέκταση διαδικτυακού ιστότοπου πρέπει να είναι HTTPS:// και όχι HTTP://.

Πότε πρέπει να χρησιμοποιήσω το Bitdefender VPN;.

Πρέπει να είστε προσεκτικοί κατά την πρόσβαση, κατά το upload ή download περιεχόμενου στο Internet. Για να είστε ασφαλείς κατά την περιήγηση στον ιστό, σας συνιστούμε να χρησιμοποιήσετε το VPN Bitdefender όταν:

- θέλετε να συνδεθείτε με δημόσια ασύρματα δίκτυα
- θέλετε να αποκτήσετε πρόσβαση σε περιεχόμενο που κανονικά είναι περιορισμένο σε συγκεκριμένες περιοχές, ανεξάρτητα από το αν είστε στο εσωτερικό ή στο εξωτερικό
- θέλετε να διατηρήσετε τα προσωπικά σας δεδομένα ιδιωτικά (ονόματα χρήστη, κωδικοί πρόσβασης, πληροφορίες πιστωτικής κάρτας κ.λπ.)
- θέλετε να αποκρύψετε τη IP διεύθυνση σας

Θα επηρεάσει αρνητικά το Bitdefender VPN τη διάρκεια ζωής της μπαταρίας της συσκευής μου;.

Το Bitdefender VPN έχει σχεδιαστεί για να προστατεύει τα προσωπικά σας δεδομένα, να αποκρύπτει την IP διεύθυνση σας ενώ είναι συνδεδεμένο σε μη ασφαλή ασύρματα δίκτυα και να έχει πρόσβαση σε περιορισμένο περιεχόμενο σε ορισμένες χώρες. Συστήνουμε να χρησιμοποιήσετε το VPN μόνο όταν το χρειάζεστε καινα το αποσυνδέετε όταν είστε εκτός σύνδεσης.

Γιατί αντιμετωπίζω την επιβράδυνση του Διαδικτύου όταν συνδέεται με το Bitdefender VPN;.

Το Bitdefender VPN έχει σχεδιαστεί για να σας προσφέρει μια ελαφριά εμπειρία κατά την πλοήγηση στο διαδίκτυο, Παρόλα αυτά, η σύνδεση στο διαδίκτυο ή η απόσταση από τον server στον οποίο συνδέεστε μπορεί να προκαλέσει επιβράδυνση. για να συνδεθείτε από τη θέση σας σε έναν απομακρυσμένο φιλοξενούμενο server (π.χ. από την Αμερική στην Κίνα), σας συνιστούμε να επιτρέψετε στο Bitdefender VPN να σας συνδέσει αυτόματα στον πλησιέστερο διακομιστή ή να βρείτε ένα server πιο κοντά στην τρέχουσα τοποθεσία σας.

Μπορώ να αλλάξω τον λογαριασμό Bitdefender που συνδέεται με τη συσκευή μου;.

Ναι, μπορείτε να αλλάξετε εύκολα τον Bitdefender λογαριασμό που συνδέετε με τη συσκευή σας ακολουθώντας τα παρακάτω βήματα:

1. Επιλέξτε **Περισσότερα** στην κάτω γραμμή πλοήγησης.
2. Εισάγετε τη διεύθυνση e-mail σας.
3. Επιλέξτε **Αποσύνδεση του λογαριασμού σας** . Αν έχετε κωδικό PIN, θα σας ζητηθεί να τον πληκτρολογήσετε.
4. Επιβεβαιώστε την επιλογή σας.
5. Πληκτρολογήστε τη διεύθυνση e-mail και τον κωδικό πρόσβασης του λογαριασμού σας στα αντίστοιχα πεδία και στη συνέχεια κάντε κλικ στο **ΣΥΝΔΕΣΗ**.

Πώς το Bitdefender Mobile Security θα επηρεάσει την απόδοση και αυτονομία της μπαταρίας της συσκευής μου;.

Κρατάμε την επίπτωση πολύ χαμηλά. Η εφαρμογή τρέχει μόνο όταν είναι απαραίτητη - αφού εγκαταστήσετε μια εφαρμογή, όταν περιηγηθείτε στη διεπαφή της εφαρμογής ή όταν θέλετε έλεγχο ασφαλείας. Το Bitdefender Mobile Security δεν εκτελείται στο παρασκήνιο όταν καλείτε τους φίλους σας, πληκτρολογείτε ένα μήνυμα ή όταν παίζετε ένα παιχνίδι.

Τι είναι ο Device Administrator;.

Ο Device Administrator είναι μία λειτουργία Android που δίνει στο Bitdefender Mobile Security τα δικαιώματα που απαιτούνται για την εκτέλεση ορισμένων εργασιών από απόσταση. Χωρίς αυτά τα δικαιώματα, το απομακρυσμένο κλείδωμα δεν θα μπορούσε να λειτουργήσει και η διαγραφή δεν θα ήταν σε θέση να σβήσει εντελώς τα δεδομένα σας. Αν θέλετε να αφαιρέσετε την εφαρμογή, φροντίστε να ανακαλέσετε τα

προνόμια πριν προσπαθήσετε να καταργήσετε την εγκατάσταση από **Ρυθμίσεις > Ασφάλεια > Επιλέξτε διαχειριστή συσκευής**.

Πως να διορθώσω το σφάλμα "No Google Token" το οποίο εμφανίζεται όταν συνδέομαι στο Bitdefender Mobile Security.

Αυτό το σφάλμα παρουσιάζεται όταν η συσκευή δεν συνδέεται με έναν λογαριασμό Google, ή όταν η συσκευή είναι συνδεδεμένη με ένα λογαριασμό, αλλά ένα προσωρινό πρόβλημα εμποδίζει τη σύνδεση με το Google. Δοκιμάστε μία από τις παρακάτω λύσεις:

- Πηγαίνετε στο Ρυθμίσεις > Εφαρμογές > Διαχείριση Εφαρμογών > Bitdefender Mobile Security και πατήστε **Εκκαθάριση δεδομένων**. Στη συνέχεια, προσπαθήστε να συνδεθείτε ξανά.
- Βεβαιωθείτε ότι η συσκευή σας συσχετίζεται με ένα λογαριασμό Google.

  Για να το ελέγξετε αυτό, μεταβείτε στο Ρυθμίσεις > Λογαριασμοί & Συγχρονισμός και δείτε αν ένας λογαριασμός Google είναι μέρος της λίστας **Διαχείριση Λογαριασμών**. Προσθέστε τον λογαριασμό σας, αν δεν είναι στη λίστα, επανεκκινήσετε τη συσκευή σας και, στη συνέχεια, προσπαθήστε να συνδεθείτε στο Bitdefender Mobile Security.
- Επανεκκινήστε τη συσκευή σας, στη συνέχεια, προσπαθήστε να συνδεθείτε ξανά.

Σε ποιες γλώσσες είναι διαθέσιμο το Bitdefender Mobile Security;.

Το Bitdefender Mobile Security είναι αυτή τη στιγμή διαθέσιμο στις ακόλουθες γλώσσες:

- Βραζιλία
- Czech
- Ολλανδία
- Αγγλικά
- Γαλλικά
- Γερμανικά
- Ελληνικά
- Hungarian
- Ιταλικά
- Ιαπωνικά
- Κορεάτικα
- Πολωνικά
- Πορτογαλία

- Ρουμανικά
- Ρωσικά
- Ισπανικά
- Σουηδικά
- Ταϊλανδικά
- Τουρκικά
- Βιετναμέζικα

Επιπλέον γλώσσες θα προστεθούν σε μελλοντικές εκδόσεις. Για να αλλάξετε τη γλώσσα της πλατφόρμας τουBitdefender Mobile Security, μεταβείτε στη συσκευή σας στη ρύθμιση **Γλώσσα & πληκτρολογίου** και ρυθμίστε τη συσκευή στη γλώσσα που θέλετε να χρησιμοποιήσετε.

ΕΠΙΚΟΙΝΩΝΉΣΤΕ ΜΑΖΊ ΜΑΣ

33. ΖΗΤΉΣΕΤΕ ΒΟΉΘΕΙΑ

Το Bitdefender παρέχει στους πελάτες της ένα απαράμιλλο επίπεδο γρήγορης και ακριβούς υποστήριξης. Εάν αντιμετωπίσετε οποιοδήποτε πρόβλημα ή εάν έχετε οποιαδήποτε ερώτηση σχετικά με το Bitdefender σας, μπορείτε να χρησιμοποιήσετε διάφορες online πηγές για να βρείτε μία λύση ή μια απάντηση. Την ίδια στιγμή, μπορείτε να επικοινωνήσετε με την ομάδα Εξυπηρέτησης Πελατών του Bitdefender. Αντιπρόσωποί μας θα απαντήσουν στις ερωτήσεις σας εγκαίρως και θα σας δώσουν τη βοήθεια που χρειάζεστε.

Το *"Επίλυση κοινών ζητημάτων"* (p. 193) τμήμα παρέχει τις απαραίτητες πληροφορίες σχετικά με τα πιο σημαντικά ζητήματα που ενδέχεται να αντιμετωπίσετε όταν χρησιμοποιείτε αυτό το προϊόν.

Εάν δεν μπορείτε να βρείτε την απάντηση στην ερώτησή σας στις παρεχόμενες απαντήσεις, μπορείτε να επικοινωνήσετε άμεσα μαζί μας:

- "Επικοινωνήστε απευθείας μαζί μας από το Bitdefender Total Security" (p. 345)
- "Επικοινωνήστε μαζί μας μέσω του online Κέντρου Υποστήριξης" (p. 346)

Επικοινωνήστε απευθείας μαζί μας από το Bitdefender Total Security

Εάν έχετε μια ενεργή σύνδεση στο Internet, μπορείτε να επικοινωνήσετε με το Bitdefender για απευθείας βοήθεια από το περιβάλλον του προϊόντος.

Ακολουθείστε αυτά τα βήματα:

1. Επιλέξτε**Υποστήριξη** στο μενού πλοήγησης του Bitdefender περιβάλλοντος.
2. Έχετε τις εξής επιλογές:
   - **ΟΔΗΓΙΕΣ ΧΡΗΣΗΣ**

     Αποκτήστε πρόσβαση στις βάσεις δεδομένων μας και ψάξτε τις απαραίτητες πληροφορίες.
   - **ΚΕΝΤΡΟ ΥΠΟΣΤΗΡΙΞΗΣ**

     Αποκτήστε πρόσβαση στα ηλεκτρονικά μας άρθρα και βίντεο.
   - **ΕΠΙΚΟΙΝΩΝΙΑ**

Χρησιμοποιήστε το κουμπί **ΕΠΙΚΟΙΝΩΝΗΣΤΕ ΜΕ ΤΗΝ ΥΠΟΣΤΗΡΙΞΗ** για την έναρξη του Εργαλείου Υποστήριξης του Bitdefender και επικοινωνήστε με το Τμήμα Εξυπηρέτησης Πελατών.

a. Συμπληρώστε τη φόρμα υποβολής με τα απαραίτητα στοιχεία:

   i. Επιλέξτε την κατηγορία του προβλήματος που έχετε αντιμετωπίζετε.

   ii. Πληκτρολογήστε μια περιγραφή του προβλήματος που αντιμετωπίσατε.

   iii. Επιλέξτε**ΔΟΚΙΜΑΣΤΕ ΝΑ ΑΝΑΠΑΡΑΓΕΤΕ ΤΟ ΠΡΟΒΛΗΜΑ** σε περίπτωση που αντιμετωπίζετε κάποιο θέμα με το προϊόν. Αναπαράγετε το πρόβλημα και, στη συνέχεια, επιλέξτε **ΤΕΛΟΣ** στο πλαίσιο ΑΝΑΠΑΡΑΓΩΓΗ ΠΡΟΒΛΗΜΑΤΟΣ.

   iv. Επιλέξτε **ΕΠΙΒΕΒΑΙΩΣΗ ΠΡΟΒΛΗΜΑΤΟΣ**.

b. Συνεχίστε να συμπληρώνετε τη φόρμα υποβολής με τα απαραίτητα δεδομένα:

   i. Εισάγετε το πλήρες όνομά σας.

   ii. Εισάγετε τη διεύθυνση e-mail σας.

   iii. Επιλέξτε το check box της αποδοχής.

   iv. Επιλέξτε **ΔΗΜΙΟΥΡΓΙΑ DEBUG ΠΑΚΕΤΟΥ** .

   Παρακαλώ περιμένετε για λίγα λεπτά, ενώ το Bitdefender συγκεντρώνει σχετικές πληροφορίες για το προϊόν. Αυτές οι πληροφορίες θα βοηθήσουν τους μηχανικούς μας να βρουν μια λύση στο πρόβλημά σας.

c. Επιλέξτε **ΚΛΕΙΣΙΜΟ** για να βγείτε από τον οδηγό. Θα επικοινωνήσει μαζί σας το συντομότερο δυνατό ένας εκπρόσωπός μας.

Επικοινωνήστε μαζί μας μέσω του online Κέντρου Υποστήριξης

Εάν δεν μπορείτε να έχετε πρόσβαση στις απαραίτητες πληροφορίες με τη χρήση του Bitdefender, ανατρέξτε στο online Κέντρο Υποστήριξης μας:

1. Μετάβαση σε https://www.bitdefender.com/support/consumer.html.

   Το Κέντρο Υποστήριξης του Bitdefender φιλοξενεί πολυάριθμα άρθρα που περιέχουν λύσεις σε θέματα που σχετίζονται με το Bitdefender.

2. Χρησιμοποιήστε τη γραμμή αναζήτησης στο πάνω μέρος του παραθύρου για να βρείτε άρθρα που μπορούν να δώσουν λύση στο πρόβλημά σας. Για την αναζήτηση, απλά πληκτρολογήστε έναν όρο στη γραμμή αναζήτησης και κάντε κλικ στο **Αναζήτηση**.
3. Διαβάστε τα σχετικά άρθρα ή τα έγγραφα και δοκιμάστε τις προτεινόμενες λύσεις.
4. Αν η λύση δεν λύνει το πρόβλημά σας, πηγαίνετε στο

   https://www.bitdefender.com/support/contact-us.htmlκαι να επικοινωνήσετε με τους εκπροσώπους υποστήριξής μας.

34. ONLINE ΠΗΓΈΣ

Πολλές online πηγές είναι διαθέσιμες για να σας βοηθήσουν να λύσετε τα προβλήματα και τις ερωτήσεις σας που σχετίζονται με το Bitdefender.

- Κέντρο Υποστήριξης του Bitdefender:

  https://www.bitdefender.com/support/consumer.html

- Φόρουμ Υποστήριξης του Bitdefender:

  https://forum.bitdefender.com

- Το portal HOTforSecurity για την ασφάλεια του υπολογιστή:

  https://www.hotforsecurity.com

Μπορείτε επίσης να χρησιμοποιήσετε την αγαπημένη σας μηχανή αναζήτησης για να μάθετε περισσότερες πληροφορίες σχετικά με την ασφάλεια των υπολογιστών, τα Bitdefender προϊόντα και την εταιρεία.

34.1. Κέντρο Υποστήριξης του Bitdefender

Το Κέντρο Υποστήριξης του Bitdefender είναι ένα online αρχείο καταγραφής πληροφοριών σχετικά με τα Bitdefender προϊόντα. Αποθηκεύει, σε μια εύκολα προσβάσιμη μορφή, αναφορές σχετικά με τα αποτελέσματα της συνεχιζόμενης τεχνικής υποστήριξης και τις ενέργειες διόρθωσης λαθών από τις ομάδες υποστήριξης και ανάπτυξης του Bitdefender, καθώς και περισσότερα γενικά άρθρα σχετικά με την πρόληψη απειλών, τη διαχείριση λύσεων του Bitdefender με λεπτομερείς εξηγήσεις, και πολλά άλλα άρθρα.

Το Κέντρο Υποστήριξης του Bitdefender είναι ανοικτό για το κοινό και ελεύθερο αναζήτησης. Οι εκτεταμένες πληροφορίες που περιέχει είναι ένα ακόμη μέσο για την παροχή στους πελάτες του Bitdefender με την τεχνική γνώση και τη διορατικότητα που χρειάζονται. Όλες οι έγκυρες αιτήσεις παροχής πληροφοριών ή αναφορές σφαλμάτων που προέρχονται από πελάτες του Bitdefender βρίσκουν τελικά τη λύση τους στο Κέντρο Υποστήριξης του Bitdefender, ως αναφορές bugfix, workaround cheatsheets ή ενημερωτικά άρθρα για τη συμπλήρωση των αρχείων βοήθειας του προϊόντος.

Το Κέντρο Υποστήριξης του Bitdefender είναι διαθέσιμο ανά πάσα στιγμή

https://www.bitdefender.com/support/consumer.html.

34.2. Φόρουμ Υποστήριξης του Bitdefender

Το Φόρουμ Υποστήριξης του Bitdefender παρέχει στους χρήστες του Bitdefender έναν εύκολο τρόπο για να λάβετε βοήθεια και να βοηθήσει άλλους.

Εάν το Bitdefender προϊόν σας δεν λειτουργεί καλά, αν δεν μπορεί να αφαιρέσει συγκεκριμένες απειλές από τον υπολογιστή σας ή αν έχετε ερωτήσεις σχετικά με τον τρόπο που λειτουργεί, δημοσιεύστε το πρόβλημά ή την ερώτησή σας στο φόρουμ.

Οι τεχνικοί υποστήριξης του Bitdefender παρακολουθούν το φόρουμ για νέες δημοδιεύσεις προκειμένου να σας βοηθήσουν. Μπορείτε επίσης να πάρετε μια απάντηση ή μια λύση από έναν πιο έμπειρο χρήστη του Bitdefender.

Πριν δημοσιεύσετε το πρόβλημα ή την ερώτησή σας, μπορείτε να αναζητήσετε στο φόρουμ για παρόμοια ή συσχετιζόμενα θέματα.

Το Φόρουμ Υποστήριξης του Bitdefender είναι διαθέσιμο https://forum.bitdefender.com, σε 5 διαφορετικές γλώσσες: Αγγλικά, Γερμανικά, Γαλλικά, Ισπανικά και Ρουμάνικα. Κάντε κλικ στο σύνδεσμο **Home & Home Office Protection** για να αποκτήσετε πρόσβαση στην ενότητα αφιερωμένη στα καταναλωτικά προϊόντα.

34.3. HOTforSecurity Portal

Το HOTforSecurity είναι μια πλούσια πηγή πληροφοριών για την ασφάλεια του υπολογιστή. Εδώ μπορείτε να μάθετε για τις διάφορες απειλές που είναι εκτεθειμένος ο υπολογιστή σας όταν είστε συνδεδεμένοι στο Internet (malware, phishing, spam, cyber-criminals).

Τα νέα άρθρα δημοσιεύονται τακτικά για να σας κρατήσουν ενημερωμένους με τις πιο πρόσφατες απειλές που ανακαλύφθηκαν, τις τρέχουσες τάσεις ασφαλείας καθώς και άλλες πληροφορίες σχετικά με τον κλάδο της ασφάλειας του υπολογιστή.

Η ιστοσελίδα HOTforSecurity είναι https://www.hotforsecurity.com.

35. CONTACT INFORMATION

Η αποτελεσματική επικοινωνία είναι το κλειδί για μια επιτυχημένη επιχείρηση. Κατά τη διάρκεια των τελευταίων 16 χρόνων το BITDEFENDER έχει δημιουργήσει μια αδιαμφισβήτητη φήμη με τη συνεχή προσπάθεια για καλύτερη επικοινωνία, έτσι ώστε να υπερβαίνουμε τις προσδοκίες των πελατών και των συνεργατών μας. Εάν έχετε απορίες, μην διστάσετε να επικοινωνήσετε μαζί μας.

35.1. Διευθύνσεις Web

Τμήμα πωλήσεων: sales@bitdefender.com
Κέντρο Υποστήριξης:https://www.bitdefender.com/support/consumer.html
Τεκμηρίωση: documentation@bitdefender.com
Τοπικοί διανομείς:https://www.bitdefender.com/partners
Πρόγραμμα συνεργατών: partners@bitdefender.com
Δημόσιες σχέσεις: pr@bitdefender.com
Καριέρα: jobs@bitdefender.com
Υποβολή Απειλών: virus_submission@bitdefender.com
Υποβολή Spam: spam_submission@bitdefender.com
Αναφορά κατάχρησης: abuse@bitdefender.com
Website:https://www.bitdefender.com

35.2. Τοπικοί διανομείς

Οι τοπικοί διανομείς του Bitdefender είναι έτοιμοι να ανταποκριθούν σε οποιαδήποτε ερώτηση σχετικά με τους τομείς λειτουργίας τους, τόσο σε εμπορικά όσο και σε γενικότερα θέματα.

Για να βρείτε ένα διανομέα Bitdefender στη χώρα σας:

1. Μετάβαση σε https://www.bitdefender.com/partners/partner-locator.html.
2. Επιλέξτε τη χώρα και την πόλη σας, χρησιμοποιώντας τις αντίστοιχες επιλογές.
3. Εάν δεν μπορείτε να βρείτε ένα διανομέα Bitdefender στη χώρα σας, μη διστάσετε να επικοινωνήσετε μαζί μας μέσω email στη διεύθυνση sales@bitdefender.com. Παρακαλούμε γράψτε το email σας στα αγγλικά, προκειμένου να είμαστε σε θέση να σας βοηθήσουμε άμεσα.

35.3. Γραφεία Bitdefender

Τα γραφεία του Bitdefender είναι έτοιμα να ανταποκριθούν σε οποιαδήποτε ερώτηση σχετικά με τους τομείς λειτουργίας τους, τόσο σε εμπορικά όσο και σε γενικότερα θέματα. Οι αντίστοιχες διευθύνσεις και επαφές βρίσκονται παρακάτω.

Η.Π.Α.

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Τηλέφωνο (γραφείο&πωλήσεις): 1-954-776-6262
Πωλήσεις: sales@bitdefender.com
Τεχνική Υποστήριξη: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

ΗΒ και Ιρλανδία

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
Email: info@bitdefender.co.uk
Τηλέφωνο: (+44) 2036 080 456
Πωλήσεις: sales@bitdefender.co.uk
Τεχνική Υποστήριξη: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

Γερμανία

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Γραφείο: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Πωλήσεις: vertrieb@bitdefender.de
Τεχνική Υποστήριξη: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Δανία

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Γραφείο: +45 7020 2282
Τεχνική Υποστήριξη: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

Ισπανία:

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Τηλέφωνο: +34 902 19 07 65
Πωλήσεις: comercial@bitdefender.es
Τεχνική Υποστήριξη: https://www.bitdefender.es/support/consumer.html
Website: https://www.bitdefender.es

Ρουμανία

BITDEFENDER SRL
Orhideea Towers, 15A Orhideelor Street, Sector 6
Bucharest
Fax: +40 21 2641799
Τηλέφωνο Πωλήσεων: +40 21 2063470
Email Πωλήσεων: sales@bitdefender.ro
Τεχνική Υποστήριξη: https://www.bitdefender.ro/support/consumer.html
Website: https://www.bitdefender.ro

Ηνωμένα Αραβικά Εμιράτα

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Τηλέφωνο Πωλήσεων: 00971-4-4588935 / 00971-4-4589186
Email Πωλήσεων: mena-sales@bitdefender.com
Τεχνική Υποστήριξη: https://www.bitdefender.com/support/consumer.html
Website: https://www.bitdefender.com

Γλωσσάρι

ActiveX

Το ActiveX είναι ένα μοντέλο για την ανάπτυξη προγραμμάτων, έτσι ώστε άλλα προγράμματα και το λειτουργικό σύστημα μπορεί να επικοινωνήσει. Η τεχνολογία ActiveX χρησιμοποιείται με τον Microsoft Internet Explorer για να κάνετε διαδραστικές ιστοσελίδες που μοιάζουν και συμπεριφέρονται σαν προγράμματα ηλεκτρονικών υπολογιστών, και όχι στατικές σελίδες. Με το ActiveX, οι χρήστες μπορούν να ζητήσουν ή να απαντήσουν στις ερωτήσεις, χρησιμοποιήστε τα κουμπιά και αλληλεπιδράσετε με πολλούς τρόπους με την ιστοσελίδα. Τα ActiveX controls συνήθως έχουν αναπτυχθεί με Visual Basic.

Τα Active X διακρίνονται για την ολοκληρωτική έλλειψη ασφάλειας? Ειδικοί σε θέματα ασφάλειας υπολογιστών αποθαρρύνει τη χρήση τους μέσω του Διαδικτύου.

Adware

Το Adware συνδυάζεται συχνά με μια εφαρμογή υπολογιστή η οποια παρέχεται χωρίς χρέωση για όσο διάστημα ο χρήστης συμφωνεί να δεχθεί το adware. Επειδή οι adware εφαρμογές εγκαθίστανται συνήθως αφού ο χρήστης συμφωνήσει με μία σύμβαση αδείας εκμεταλλεύσεως, η οποια δηλώνει το σκοπό της εφαργμογής με αποτέλεσμα να μην διαπράττεται κανένα αδίκημα.

Ωστόσο, οι αναδυόμενες διαφημίσεις μπορούν να γίνουν ενοχλητικές και σε ορισμένες περιπτώσεις να υποβαθμίσουν την απόδοση του συστήματος. Επίσης, οι πληροφορίες που κάποιες από αυτές τις εφαρμογές συλλέγουν, ενδέχεται να προκαλέσουν ανησυχίες για την ιδιωτική ζωή των χρηστών που δεν είχαν πλήρη γνώση των όρων της άδειας χρήσης.

Backdoor

Μια τρύπα ασφάλειας ενός συστήματος η οποια αφέθηκε επίτηδες από τους σχεδιαστές ή τους συντηρητές. Το κίνητρο για τέτοιες τρύπες δεν είναι πάντα κακόβουλο? Μερικά λειτουργικά συστήματα, για παράδειγμα, βγαίνουν στην παραγωγή με προνομιούχους λογαριασμούς που προορίζονται για χρήση από τους τεχνικούς στον τομέα των υπηρεσιών ή προγραμματιστές συντήρησης του πωλητή.

Boot sector

Ένας τομέας στην αρχή κάθε δίσκου που προσδιορίζει την αρχιτεκτονική του δίσκου (μέγεθος τομέα, το μέγεθος του cluster, και ούτω καθεξής). Για δίσκους εκκίνησης, ο τομέας εκκίνησης περιέχει επίσης ένα πρόγραμμα που φορτώνει το λειτουργικό σύστημα.

Botnet

Ο όρος "botnet" αποτελείται από τις λέξεις "ρομπότ" και "δίκτυο". Τα bootnets είναι συσκευές συνδεδεμένες στο διαδίκτυο που έχουν μολυνθεί από κακόβουλο λογισμικό και μπορούν να χρησιμοποιηθούν για την αποστολή ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου, την κλοπή δεδομένων, την απομακρυσμένη παρακολούθηση ευάλωτων συσκευών ή την εξάπλωση λογισμικού υποκλοπής spyware, ransomware και άλλων μορφών κακόβουλου λογισμικού. Στόχος τους είναι να μολύνουν όσο το δυνατόν περισσότερες συνδεδεμένες συσκευές, όπως υπολογιστές, servers, κινητές συσκευές ή συσκευές IoT που ανήκουν σε μεγάλες εταιρείες ή βιομηχανίες.

Browser

Συντομογραφία για το πρόγραμμα περιήγησης στο Web, μια εφαρμογή λογισμικού που χρησιμοποιείται για να εντοπίσει και να εμφανίσει ιστοσελίδες. Δημοφιλή φυλλομετρητές περιλαμβάνουν τον Microsoft Internet Explorer, Mozilla Firefox and Google Chrome. Αυτά είναι περιηγητές γραφικών, πράγμα που σημαίνει ότι μπορούν να εμφανίσουν γραφικά καθώς και το κείμενο. Επιπλέον, τα περισσότερα σύγχρονα προγράμματα περιήγησης μπορεί να παρουσιάσουν πληροφορίες πολυμέσων, συμπεριλαμβανομένων ήχου και βίντεο, που όμως απαιτούν plug-ins για ορισμένες μορφές.

Brute Force Attack

Η επίθεση μέσω μαζικής εισαγωγής κωδικών χρησιμοποιείται για να διασπάσει την ασφάλεια εισάγοντας πιθανούς συνδυασμούς κωδικών πρόσβασης, ξεκινώντας συνήθως με τον ευκολότερο κωδικό πρόσβασης.

Cookie

Εντός της βιομηχανίας του Διαδικτύου, τα cookies περιγράφονται ως μικρά αρχεία που περιέχουν πληροφορίες σχετικά με μεμονωμένους υπολογιστές που μπορούν να αναλυθούν και να χρησιμοποιηθούν από

τους διαφημιστές για να παρακολοθούν τα online ενδιαφέροντα και τις προτιμήσεις σας. Σε αυτό το βασίλειο, η τεχνολογία των cookies εξακολουθεί να αναπτύσσεται και η πρόθεση είναι να στοχεύουν τις διαφημίσεις άμεσα σε ότι έχετε δήλωσει ότι σας ενδιαφέρει Είναι δίκοπο μαχαίρι για πολλούς ανθρώπους γιατί από τη μία πλευρά, είναι αποτελεσματική και πάντα επίκαιρη, καθώς βλέπετε διαφημίσεις μόνο για ότι σας ενδιαφέρει. Από την άλλη , πρόκειται στην πραγματικότητα για "παρακολούθηση" και "ανίχνευση" που πάτε και σε τι κάνετε κλικ. Δικαιολογημένα λοιπόν, υπάρχει μια συζήτηση για την ιδιωτική ζωή και πολλοί άνθρωποι αισθάνονται προσβεβλημένοι από την ιδέα ότι θεωρούνται ως "αριθμός SKU" (το bar code στο πίσω μέρος των συσκευασιών που σκανάρεται στο ταμείο του παντοπωλείου). Ενώ αυτή η άποψη μπορεί να είναι ακραία, σε ορισμένες περιπτώσεις είναι ακριβής.

Cyberbullying

Όταν οι συμμαθητές ή οι ξένοι διαπράττουν βίαιες ενέργειες εναντίον παιδιών με σκοπό να τα βλάψουν σωματικά. Για να προκαλέσουν συναισθηματική ζημιά, οι επιτιθέμενοι στέλνουν μηνύματα ή ανεπιθύμητες φωτογραφίες, απομονώνοντας έτσι τα θύματά τους από τους άλλους ή για να τους κάνουν να αισθάνονται απογοητευμένοι.

Dictionary Attack

Οι επιθέσεις μαζικής εισαγωγής κωδικών χρησιμοποιούνται για να διασπάσουν την ασφάλεια υπολογιστή εισάγοντας έναν συνδυασμό κοινών λέξεων για τη δημιουργία πιθανών κωδικών πρόσβασης. Η ίδια μέθοδος χρησιμοποιείται για να μαντέψει τα κλειδιά αποκρυπτογράφησης κρυπτογραφημένων μηνυμάτων ή εγγράφων. Οι Dictionary Επιθέσεις επιτυγχάνουν επειδή πολλοί άνθρωποι προτιμούν να επιλέγουν κωδικούς πρόσβασης μικρών και μεμονωμένων λέξεων που είναι εύκολο να βρεθούν.

E-mail

Το ηλεκτρονικό ταχυδρομείο. Μια υπηρεσία που στέλνει μηνύματα σε υπολογιστές μέσω τοπικών ή παγκόσμιων δικτύων

Exploits

Ένας τρόπος να εκμεταλλευτείτε τα διαφορετικά σφάλματα ή τρωτά σημεία που υπάρχουν σε έναν υπολογιστή (λογισμικό ή υλικό). Έτσι,

οι χάκερ μπορούν να αποκτήσουν τον έλεγχο των υπολογιστών ή των δικτύων.

Εφαρμογή -πελάτης ηλεκτρονικού ταχυδρομείου (mail client)

Ένας e-mail client είναι μια εφαρμογή που σας επιτρέπει να στέλνετε και να λαμβάνετε ηλεκτρονικό ταχυδρομείο

Honeypot

Ένα δόλωμα σύστημα υπολογιστή για να προσελκύει τους hackers, προκειμένου να μελετήσουμε τον τρόπο που ενεργούν και να εντοπίσουμε τις αιρετικές μεθόδους που χρησιμοποιούν για τη συλλογή πληροφοριών του συστήματος. Εταιρείες και οι οργανισμοί ενδιαφέρονται περισσότερο για την εφαρμογή και χρήση honeypots για να βελτιώσουν τη γενική κατάσταση της ασφάλειας τους.

IP

Πρωτόκολλο Διαδικτύου - ενα πρωτόκολλο με δυνατότητα δρομολόγησης στην οικογένεια πρωτοκόλλων TCP / IP που είναι υπεύθυνο για την διευθυνσιοδότηση IP, δρομολόγηση, και τον κατακερματισμό και επανασυναρμολόγηση των πακέτων IP.

Keylogger (καταγραφέας πληκτρολογήσεων)

Ένας keylogger είναι μια εφαρμογή που καταγράφει οτιδήποτε πληκτρολογείτε.

Τα Keyloggers δεν είναι κακόβουλου χαρακτήρα. Μπορούν να χρησιμοποιηθούν για νόμιμους σκοπούς, όπως την παρακολούθηση των εργαζομένων ή τη δραστηριότητα των παιδιών. Ωστόσο, χρησιμοποιούνται ολοένα και περισσότερο από κυβερνο-εγκληματίες για δόλιους σκοπούς (για παράδειγμα, ώστε να συλλέξουν ιδιωτικά δεδομένα, όπως συνθηματικά σύνδεσης σε συστήματα και αριθμούς κοινωνικής ασφάλισης).

Macro ιός

Ένας τύπος απειλής υπολογιστών που κωδικοποιείται ως μακροεντολή ενσωματωμένη σε ένα έγγραφο. Πολλές εφαρμογές, όπως το Microsoft Word και το Excel, υποστηρίζουν ισχυρές γλώσσες μακροεντολών.

Οι εφαρμογές αυτές σας επιτρέπουν να ενσωματώσετε μια μακροεντολή σε ένα έγγραφο, η οποία μακροεντολή εκτελείται κάθε φορά που το έγγραφο ανοίγει.

Non-heuristic (μη- ευρετικό)

Αυτή η μέθοδος σάρωσης βασίζεται σε συγκεκριμένη βάση δεδομένων πληροφοριών απειλών. Το πλεονέκτημα της non-heuristic σάρωσης είναι ότι δεν ξεγελιέται από ό,τι φαίνεται ότι θα μπορούσε να είναι απειλή, και δεν παράγει ψευδείς συναγερμούς.

Online predators

Άτομα που επιδιώκουν να προσελκύσουν ανηλίκους ή εφήβους σε συζητήσεις με σκοπό να τους εμπλέξουν σε παράνομες σεξουαλικές δραστηριότητες. Τα κοινωνικά δίκτυα είναι ο ιδανικός χώρος όπου τα ευάλωτα παιδιά μπορούν εύκολα να κυνηγηθούν και να παρασυρθούν να διαπράξουν σεξουαλικές δραστηριότητες, διαδικτυακά ή πρόσωπο με πρόσωπο.

phishing

Η αποστολή ενός e-mail σε ένα χρήστη με τον ψευδή ισχυρισμό ότι πρόκειται για μια καθιερωμένη νόμιμη επιχείρηση, σε μια προσπάθεια εξαπάτησης του χρήστη με σκοπό να παραδοθούν ιδιωτικές πληροφορίες που θα χρησιμοποιηθούν για κλοπή ταυτότητας. Το e-mail κατευθύνει το χρήστη να επισκεφτεί μια τοποθεσία Web, όπου καλείται να ενημερώσει προσωπικές πληροφορίες, όπως κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών, κοινωνικής ασφάλισης και τραπεζικών λογαριασμών, τους οποίος ο νόμιμος Φορέας ήδη κατέχει. Η τοποθεσία Web, ωστόσο, είναι ψεύτικη και έχει συσταθεί μόνο για την κλοπή πληροφοριών του χρήστη.

Photon (φωτόνιο)

Το Photon είναι μία καινοτόμος μη παρεμβατική τεχνολογία της Bitdefender, που αποσκοπεί στην ελαχιστοποίηση της επίδρασης στην απόδοση του υπολογιστή εξαιτίας της λειτουργίας προστασίας από απειλές. Με την παρακολούθηση της δραστηριότητας του υπολογιστή σας στο παρασκήνιο, δημιουργεί πρότυπα χρήσης που βοηθούν στην βελτιστοποίηση των διαδικασιών εκκίνησης και σάρωσης.

Ransomware

Το Ransomware είναι ένα κακόβουλο πρόγραμμα που προσπαθεί να κερδίσει χρήματα από τους χρήστες κλειδώνοντας τα ευπαθή συστήματά τους. Το CryptoLocker, CryptoWall, και το TeslaWall είναι μόνο μερικές παραλλαγές που κυνηγούν ιδιωτικά συστήματα χρηστών.

Η μόλυνση μπορεί να μεταδοθεί με την πρόσβαση σε ανεπιθύμητων e-mail, τη λήψη συνημμένων ηλεκτρονικού ταχυδρομείου, ή με την εγκατάσταση εφαρμογών, χωρίς ο χρήστης να ξέρει το τι συμβαίνει στο σύστημά του. Οι καθημερινοί χρήστες και εταιρείες στοχεύονται από ransomware χάκερ.

Rootkit

Το rootkit είναι ένα σύνολο εργαλείων λογισμικού που προσφέρουν επίπεδο πρόσβασης διαχειριστή σε ένα σύστημα. Ο όρος χρησιμοποιήθηκε για πρώτη φορά στα λειτουργικά συστήματα UNIX αναφέρομενος σε εκ νέου μεταγλωττισμένα (recompiled) εργαλεία που παρέχουν σε εισβολείς δικαιώματα διαχειριστή, επιτρέποντάς τους να κρύψουν την παρουσία τους, ούτως ώστε να μην είναι ορατοί από τους διαχειριστές του συστήματος.

Ο κύριος ρόλος των rootkits είναι να κρύψουν τις διαδικασίες, τα αρχεία, συνδέσεις και τα αρχεία καταγραφής. Μπορούν επίσης να υποκλέψουν δεδομένα από τους τερματικούς σταθμούς, συνδέσεις δικτύου ή περιφερειακά, εάν ενσωματώσουν το κατάλληλο λογισμικό.

Τα Rootkits δεν είναι φύσει κακόβουλα. Για παράδειγμα, συστήματα και ακόμη και μερικές εφαρμογές κρύβουν κρίσιμα αρχεία χρησιμοποιώντας rootkits. Ωστόσο, χρησιμοποιούνται κατά κύριο λόγο για να κρύψουν κακόβουλο λογισμικό ή να αποκρύψουν την παρουσία ενός εισβολέα στο σύστημα. Όταν συνδυάζονται με απειλές, τα rootkits αποτελούν σοβαρή απειλή για την ακεραιότητα και την ασφάλεια του συστήματος. Μπορούν να παρακολουθούν την κυκλοφορία, να δημιουργήσουν κερκόπορτες (backdoors) στο σύστημα, να τροποποιήσουν αρχεία και αρχεία καταγραφής και να αποφύγουν τον εντοπισμό.

Spam

Το ηλεκτρονικό ταχυδρομείο junk (σαβούρας) ή ποσταρίσματα junk ομάδων ειδήσεων. Ευρύτερα γνωστό ως οποιοδήποτε ανεπιθύμητο ηλεκτρονικό ταχυδρομείο.

Spyware

Οποιοδήποτε λογισμικό συγκεντρώνει κρυφά πληροφορίες για το χρήστη μέσω της σύνδεσης Internet του χρήστη χωρίς τη γνώση του, συνήθως για διαφημιστικούς σκοπούς. Οι εφαρμογές Spyware συνήθως ομαδοποιούνται ως κρυφό στοιχείο της δωρέαν (freeware) ή με δωρεάν

δοκιμαστική χρήση (shareware) προγράμματα που μπορείτε να κατεβάσετε από το Διαδίκτυο. Ωστόσο, θα πρέπει να σημειωθεί ότι η πλειοψηφία των shareware και freeware εφαρμογών δεν περιέχουν spyware. Μόλις εγκατασταθεί, το spyware παρακολουθεί τη δραστηριότητα του χρήστη στο διαδίκτυο και μεταδίδει τις πληροφορίες στο παρασκήνιο σε κάποιον άλλο. Το Spyware μπορεί επίσης να συλλέξει πληροφορίες σχετικά με τις διευθύνσεις e-mail, ακόμα και κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών.

Η ομοιότητα του Spyware με ένα Trojan Horse είναι το γεγονός ότι οι χρήστες εγκαθιστούν άθελά τους το προϊόν κατά την εγκατάσταση μιάς άλλης εφαρμογής. Ένας κοινός τρόπος για να γίνει κανείς θύμα του spyware είναι να κατεβάσει ορισμένα προϊόντα ανταλλαγής αρχείων σε ομότιμο δίκτυο (peer - to peer) από τα διαθέσιμα σήμερα.

Εκτός από τα ζητήματα της ηθικής και της ιδιωτικότητας, το spyware κλέβει από το χρήστη με τη χρήση του υπολογιστή του, πόρους μνήμης και επίσης καταναλώνει εύρος ζώνης επικοινωνίας (bandwidth), στέλνοντας τις πληροφορίες πίσω στην έδρα του spyware μέσω της σύνδεσης στο Internet του χρήστη. Επειδή το spyware χρησιμοποιεί μνήμη και πόρους του συστήματος, οι εφαρμογές που τρέχουν στο παρασκήνιο μπορεί να οδηγήσουν σε επιβραδύνσεις ή κόλλημα σύστηματο ή και τη γενική αστάθεια του συστήματος.

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) : Πρωτόκολλο Ελέγχου Μετάδοσης / Πρωτόκολλο Διαδικτύου - Ένα σύνολο από πρωτόκολλα που χρησιμοποιούνται ευρέως στο διαδίκτυο που παρέχουν επικοινωνίες ανάμεσα σε διασυνδεδεμένα δικτύα υπολογιστών με διαφορετικές αρχιτεκτονικές υλικού και διάφορα λειτουργικά συστήματα. TCP / IP περιλαμβάνει πρότυπα για το πώς επικοινωνούν οι υπολογιστές και συμβάσεις για τη σύνδεση δικτύων και τη δρομολόγηση της κυκλοφορίας.

Trojan

Ένα καταστροφικό πρόγραμμα το οποίο μεταμφιέζεται ο καλοήθης εφαρμογή. Σε αντίθεση με τα προγράμματα κακόβουλου λογισμικού και τα worms, τα Trojans δεν αντιγράφουν τον εαυτό τους αλλά μπορούν να είναι εξίσου καταστρεπτικά. Ένας από τους πιο ύπουλους τύπους Trojan horse είναι ένα πρόγραμμα που ισχυρίζεται ότι θα

απαλλάξει τον υπολογιστή σας από απειλές, αλλά αντ' αυτού εισάγει τις απειλές στον υπολογιστή σας.

Ο όρος προέρχεται από μια ιστορία στην Ιλιάδα του Ομήρου, στην οποία οι Έλληνες δίνουν ένα τεράστιο ξύλινο άλογο στους εχθρούς, τους Τρώες, φαινομενικά ως προσφορά ειρήνης. Αλλά αφού οι Τρώες έσυραν το άλογο εντός των τειχών της πόλης τους, οι Έλληνες στρατιώτες γλίστρησαν έξω από την κούφια κοιλιά του αλόγου και άνοιξαν τις πύλες της πόλης, επιτρέποντας τους συμπατριώτες τους να μπουν μέσα και να κατακτήσουν την Τροία.

Virtual Private Network (VPN)

Είναι μια τεχνολογία που επιτρέπει την προσωρινή και κρυπτογραφημένη άμεση σύνδεση με ένα συγκεκριμένο δίκτυο πάνω από ένα λιγότερο ασφαλές δίκτυο. Με αυτό τον τρόπο, η αποστολή και λήψη δεδομένων είναι ασφαλής και κρυπτογραφημένη, και είναι δύσκολο να κλεφτούν.. Μια απόδειξη της ασφάλειας είναι ο έλεγχος ταυτότητας, η οποία μπορεί να γίνει μόνο με ένα όνομα χρήστη και κωδικό πρόσβασης.

Worm

Ένα πρόγραμμα που διαδίδεται μέσω ενός δικτύου, αναπαράγει τον ίδιο του τον εαυτό καθώς περνά. Δεν μπορεί να συνδεθεί με άλλα προγράμματα.

Απειλή

Ένα πρόγραμμα ή ένα κομμάτι του κώδικα που έχει φορτωθεί στον υπολογιστή σας χωρίς τη γνώση σας και εκτελείται ενάντια στη θέλησή σας. Οι περισσότερες απειλές μπορούν επίσης να αναπαράγουν τον εαυτό τους. Όλες οι απειλές υπολογιστών δημιουργήθηκαν από ανθρώπους. Ένας απλή απειλή που μπορεί να αντιγράψει το ίδιο της τον εαυτό ξανά και ξανά είναι σχετικά εύκολο να παραχθεί. Ακόμη και ένας τέτοιος απλή απειλή είναι επικίνδυνη επειδή θα χρησιμοποιήσει γρήγορα όλη τη διαθέσιμη μνήμη και να φέρει το σύστημα σε αδιέξοδο. Ένα ακόμη πιο επικίνδυνη απειλή είναι αυτή που είναι ικανή να μεταφέρεται η ίδια σε όλα τα δίκτυα και παρακάμπτοντας τα συστήματα ασφάλειας.

Αρχείο

Ένας δίσκος, ταινία, ή φάκελος, οπου περιέχει τα αρχεία με τα αντίγραφα ασφαλείας.

Ένα αρχείο που περιέχει ένα ή περισσότερα αρχεία σε συμπιεσμένη μορφή.

Αρχείο αναφοράς

Ένα αρχείο που απαριθμεί τις ενέργειες που έχουν συμβεί. Το Bitdefender διατηρεί ένα αρχείο αναφοράς που απαριθμεί τη διαδρομή που σαρώθηκε, τους φακέλους, τον αριθμό των συμπιεσμένων αρχείων και τα αρχεία που σαρώθηκαν, πόσα μολυσμένα και ύποπτα αρχεία βρέθηκαν .

Γραμμή εντολών

Σε μια γραμμή εντολών, ο χρήστης πληκτρολογεί εντολές στο χώρο που παρέχεται απευθείας στην οθόνη χρησιμοποιώντας γλώσσα εντολών.

Δέσμη ενεργειών

Ένας άλλος όρος για τη μακροεντολή (macro) ή αρχείο δέσμης (batch file), το σενάριο (script) είναι μια λίστα με τις εντολές που μπορούν να εκτελεστούν χωρίς αλληλεπίδραση του χρήστη.

Διαδρομή

Οι ακριβείς οδηγίες προς ένα αρχείο σε έναν υπολογιστή. Αυτές οι κατευθύνσεις συνήθως περιγράφονται με τη βοήθεια του ιεραρχικού συστήματος αρχειοθέτησης από την κορυφή προς τα κάτω.

Η διαδρομή μεταξύ δύο σημείων, όπως το κανάλι επικοινωνίας μεταξύ δύο υπολογιστών.

Ενημέρωση

Μια νέα έκδοση του λογισμικού ή του υλικού ενός προϊόντος που προορίζεται να αντικαταστήσει μια παλαιότερη έκδοση του ίδιου προϊόντος. Επιπλέον, οι ρουτίνες εγκατάστασης για ενημερώσεις συχνά ελέγχουν για να είναι σίγουρο ότι μια παλαιότερη έκδοση είναι ήδη εγκατεστημένη στον υπολογιστή σας. Εάν όχι, δεν μπορείτε να εγκαταστήσετε την ενημερωμένη έκδοση.

Το Bitdefender έχει τη δική του δυνατότητα ενημέρωσης που σας επιτρέπει να ελέγχετε χειροκίνητα για ενημερώσεις, ή να το αφήσετε να ενημερώνει αυτόματα το προϊόν.

Ενημέρωση πληροφοριών απειλών

Το binary pattern μιας απειλής που χρησιμοποιείται από τη λύση ασφάλειας για την ανίχνευση και την εξάλειψη της απειλής.

Θύρα

Μια διασύνδεση σε έναν υπολογιστή στον οποίο μπορείτε να συνδέσετε μια συσκευή. Οι προσωπικοί υπολογιστές έχουν διάφορα είδη πορτών. Εσωτερικά, υπάρχουν αρκετές πόρτες για σύνδεση δίσκων, οθονών και πληκτρολόγιων. Εξωτερικά, οι προσωπικοί υπολογιστές έχουν θύρες για τη σύνδεση μόντεμ, εκτυπωτών, ποντικιών και άλλων περιφερειακών συσκευών.

Στα TCP/IP και UDP δίκτυα, ένα τελικό σημείο σε μια λογική σύνδεση. Ο αριθμός της πόρτας προσδιορίζει τι είδους πόρτα είναι. Για παράδειγμα, η πόρτα 80 χρησιμοποιείται για την κυκλοφορία HTTP.

Κωδικός ενεργοποίησης

Είναι ένας μοναδικός κωδικός που μπορεί να αγοραστεί από καταστήματα λιανικής και να χρησιμοποιηθεί για να ενεργοποιήσει ένα συγκεκριμένο προϊόν ή υπηρεσία. Ένας κωδικός ενεργοποίησης επιτρέπει την ενεργοποίηση μιας έγκυρης συνδρομής για ένα ορισμένο χρονικό διάστημα και αριθμό συσκευών και μπορεί επίσης να χρησιμοποιηθεί για την επέκταση μια συνδρομής με την προϋπόθεση να δημιουργηθεί για το ίδιο προϊόν ή υπηρεσία.

Λήψη

Για να αντιγράψετε τα δεδομένα (συνήθως ένα ολόκληρο αρχείο) από την κύρια πηγή σε μια περιφερειακή συσκευή. Ο όρος χρησιμοποιείται συχνά για να περιγράψει τη διαδικασία της αντιγραφής ενός αρχείου από μια ηλεκτρονική υπηρεσία στον υπολογιστή κάποιου. Η λήψη (μεταφόρτωση ή downloading) μπορεί επίσης να αναφέρεται σε αντιγραφή ενός αρχείου από ένα διακομιστή αρχείων δικτύου σε έναν υπολογιστή στο δίκτυο.

Μνήμη

Εσωτερικοί χώροι αποθήκευσης στον υπολογιστή. Ο όρος μνήμη (memory) προσδιορίζει χώρο αποθήκευσης δεδομένων που έρχεται με τη μορφή πλακιδίων (chips) , και ο όρος αποθηκευτικός χώρος (storage) χρησιμοποιείται για τη μνήμη που υπάρχει σε ταινίες ή δίσκους. Κάθε υπολογιστής έρχεται με ένα συγκεκριμένο ποσό φυσικής μνήμης, που συνήθως αναφέρεται ως κύρια μνήμη ή RAM.

Περιοχή ειδοποιήσεων

Καθιερώθηκε με τα Windows 95, η περιοχή ειδοποιήσεων βρίσκεται στη γραμμή εργασιών των Windows (συνήθως στο κάτω μέρος δίπλα στο ρολόι) και περιέχει μικρά εικονίδια για εύκολη πρόσβαση στις λειτουργίες του συστήματος, όπως φαξ, εκτυπωτή, modem, ένταση ήχου, και άλλα πολλά. Κάντε διπλό κλικ ή δεξί κλικ σε ένα εικονίδιο για να δείτε και να αποκτήσετε πρόσβαση στις λεπτομέρειες και τους ελέγχους.

Πολυμορφικός ιός.

Μία απειλή που αλλάζει μορφή με κάθε αρχείο που μολύνει. Δεδομένου ότι δεν διαθέτουν συνεπές δυαδικό μοτίβο (binary pattern), τέτοιες απειλές είναι δύσκολες στην ανίχνευση.

Προηγμένες Επίμονες Απειλές

Μια Προηγμένη Επίμονη Απειλή (APT) εκμεταλλεύεται τα τρωτά σημεία των συστημάτων για να κλέψει σημαντικές πληροφορίες και να τις παραδώσει στην πηγή. Μεγάλες ομάδες όπως οργανώσεις, εταιρείες, ή κυβερνήσεις, αποτελούν στόχο αυτής της απειλής.

Ο στόχος μιας προηγμένης επίμονης απειλής είναι να παραμείνει αδιάγνωστη για μεγάλο χρονικό διάστημα όντας σε θέση να παρακολουθεί και να συλλέξει σημαντικές πληροφορίες χωρίς να καταστρέφει τις στοχευμένες μηχανές. Η μέθοδος που χρησιμοποιείται για την έγχυση της απειλής στο δίκτυο είναι μέσω ενός αρχείου PDF ή ενός εγγράφου του Office που μοιάζει ακίνδυνο έτσι ώστε ο κάθε χρήστης να μπορέσει να ανοίξει τα αρχεία.

Στοιχεία εκκίνησης

Όλα τα αρχεία που τοποθετούνται σε αυτόν το φάκελο θα ανοίξουν, όταν ξεκινά ο υπολογιστής. Για παράδειγμα, μια οθόνη εκκίνησης, ένα αρχείο ήχου που θα αναπαράγεται κατά την πρώτη εκκίνηση του υπολογιστή, μια υπενθύμιση ημερολογίου, ή τα προγράμματα εφαρμογής μπορεί να είναι στοιχεία εκκίνησης. Κανονικά, ένα ψευδώνυμο ενός αρχείου τοποθετείται σε αυτόν το φάκελο και όχι το ίδιο το αρχείο.

Συμβάντα

Μια ενέργεια ή περιστατικό που ανιχνεύθηκε από ένα πρόγραμμα. Τα συμβάντα (events) μπορούν να είναι οι ενέργειες των χρηστών, όπως το πάτημα ενός κουμπιού του ποντικιού ή το πάτημα ενός πλήκτρου, ή γεγονότα του συστήματος, όπως η κατανάλωση όλης της μνήμης.

Συμπιεσμένα προγράμματα

Ένα αρχείο σε συμπιεσμένη μορφή Πολλά λειτουργικά συστήματα και εφαρμογές περιέχουν εντολές που σας επιτρέπουν να συμπιέσετε ένα αρχείο, έτσι ώστε να καταλαμβάνει λιγότερη μνήμη. Για παράδειγμα, ας υποθέσουμε ότι έχετε ένα αρχείο κειμένου που περιέχει δέκα διαδοχικούς χαρακτήρες κενού διαστήματος. Κανονικά, αυτό θα απαιτούσε δέκα bytes της αποθήκευσης.

Ωστόσο, ένα πρόγραμμα που συμπιέζει αρχεία θα αντικαταστήσει τους χαρακτήρες κενού διαστήματος με ένα ειδικό χαρακτήρα κενού διαστήματος ακολουθούμενο από τον αριθμό των κενών διαστημάτων που αντικαθίστανται. Στην περίπτωση αυτή, οι δέκα χαρακτήρες κενού διαστήματος θα απαιτήσουν μόνο δύο bytes. Αυτή είναι μόνο μία τεχνική συμπίεσης - υπάρχουν πολλές περισσότερες.

Συνδρομή

Συμφωνία αγοράς που δίνει στο χρήστη το δικαίωμα να χρησιμοποιήσει ένα συγκεκριμένο προϊόν ή υπηρεσία σε ένα συγκεκριμένο αριθμό συσκευών και για ένα ορισμένο χρονικό διάστημα. Μια συνδρομή που έχει λήξει μπορεί να ανανεωθεί αυτόματα, χρησιμοποιώντας τις πληροφορίες που παρέχονται από τον χρήστη κατά την πρώτη αγορά.

Τός τομέα εκκίνησης

Μία απειλή που μολύνει τον τομέα εκκίνησης ενός σταθερού δίσκου ή δισκέτας. Μια προσπάθεια να εκκινήσετε από μια δισκέτα που έχει μολυνθεί με την απειλή στον τομέα εκκίνησης θα καταλήξει στην ενεργοποίηση της στη μνήμη. Κάθε φορά που θα εκκινήσετε το σύστημά σας από το σημείο αυτό και μετά, θα έχετε την απειλή ενεργή στη μνήμη.

Ψευδώς θετικά

Συμβαίνει όταν ένας σαρωτής εντοπίζει ένα αρχείο ως μολυσμένο, ενώ στην πραγματικότητα δεν είναι.

επέκταση ονόματος αρχείου

Το τμήμα ενός όνοματος αρχείου, μετά την τελεία, το οποίο υποδεικνύει το είδος των δεδομένων που αποθηκεύονται στο αρχείο.

Πολλά λειτουργικά συστήματα χρησιμοποιούν επεκτάσεις, π. Χ. το Unix, το VMS, και MS-DOS. Συνήθως είναι από ένα έως τρία γράμματα (μερικά θλιβερά παλιά λειτουργικά δεν υποστηρίζουν περισσότερα

από τρία). Ενδεικτικά αναφέρουμε το «c» για τον πηγαίο κώδικα της γλώσσας C, "PS" για PostScript, το "txt" για αυθαίρετο κείμενο.

ευρετική

Μια βασισμένη σε κανόνες μέθοδος εντοπισμού απειλών. Αυτή η μέθοδος σάρωσης δεν βασίζεται σε συγκεκριμένη βάση δεδομένων πληροφοριών απειλών. Το πλεονέκτημα της heuristic σάρωσης είναι ότι δεν ξεγελιέται από μια νέα παραλλαγή μίας υπάρχουσας απειλής. Ωστόσο, σε ορισμένες περιπτώσεις ενδέχεται να αναφέρουν ύποπτο κώδικα σε κανονικά προγράμματα, δημιουργώντας το λεγόμενο «ψευδώς θετικό» (false positive))

μικροεφαρμογή (applet) Java

Ένα πρόγραμμα Java το οποίο είναι σχεδιασμένο να λειτουργεί μόνο σε ιστοσελίδα. Για να χρησιμοποιήσετε ένα applet σε μια ιστοσελίδα, πρέπει να καθορίσετε το όνομα της μικροεφαρμογής (applet) και το μέγεθος (μήκος και πλάτος, σε pixel) που το applet μπορεί να χρησιμοποιήσει. Κατά την πρόσβαση στην ιστοσελίδα, ο browser (περιγητής) κατεβάζει το applet από ένα διακομιστή και την τρέχει στο μηχάνημα του χρήστη (client). τα Applets διαφέρουν από τις εφαρμογές στο ότι διέπονται από ένα αυστηρό πρωτόκολλο ασφαλείας.

Για παράδειγμα, παρότι τα applets τρέχουν στον υπολογιστή -client (πελάτη), δεν μπορούν να διαβάσουν ή να γράψουν δεδομένα στο client μηχάνημα . Επιπλέον, οι μικροεφαρμογές περιορίζονταται περαιτέρω, έτσι ώστε να μπορούν να διαβάσουν και να γράψουν δεδομένα μόνο από τον ίδιο τομέα (Domain) που εξυπηρετούνται .

μονάδα δίσκου

Είναι μηχάνημα, το οποίο διαβάζει και γράφει δεδομένα σε ένα δίσκο.

Μία μονάδα σκληρού δίσκου διαβάζει και γράφει σκληρούς δίσκους.

Μία μονάδα δισκέττας διαβάζει και γράφει δισκέττες.

Μονάδες δίσκου μπορεί να είναι είτε εσωτερικοί (στεγασμένοι σε ένα υπολογιστή) ή εξωτερικοί (στεγασμένοι σε ένα ξεχωριστό πλαίσιο που συνδέεται με τον υπολογιστή).