Νομική σημείωση
Με την επιφύλαξη κάθε νόμιμου δικαιώματος. Δεν επιτρέπεται η αναπαραγωγή ή αναμετάδοση κανενός τμήματος αυτού του εγχειρίδιου σε οποιοδήποτε μορφή ή από οποιοδήποτε μέσο, ηλεκτρονικό ή μηχανικό, συμπεριλαμβανομένης της ψωτοαντιγραφής και της εγγραφής, ή από οποιοδήποτε σύστημα αποθήκευσης πληροφοριών και ανάκτησης, χωρίς την έγγραφη σύγφυση ή επιτροποποίηση από αντιπρόσωπο της Bitdefender. Η συμπερίληψη σύντομων εδαφίων σε αναθεωρήσεις μπορεί να γίνει μόνον με αναφορά της πηγής προέλευσης. Δεν είναι δυνατή η τροποποίηση του περιεχομένου με κανέναν τρόπο.

Προεδροποίηση και κείμενο αποποίησης ευθυνών.
Αυτό το προϊόν και τα έγγραφα που το συνοδεύουν προστατεύονται από τον νόμο περί πνευματικών δικαιωμάτων. Οι πληροφορίες σε αυτό το έγγραφο παρέχονται "ώς έχουν", χωρίς εγγύηση. Παρά το γεγονός ότι έχει ληφθεί κάθε μέτρο προφύλαξης κατά την προετοιμασία αυτού του εγγράφου, οι συγγραφείς δεν αναλαμβάνουν οιαδήποτε ευθύνη έναντι οιαδήποτε φυσικού ή νομικού προσώπου όσον αφορά οιανήποτε απώλεια ή βλάβη φερόμενη ως προκληθείσα εμμέσως ή αμέσως από τις παρεχόμενες στο παρόν πόνημα πληροφορίες.

Αυτό το βιβλίο περιέχει τις συνδέσεις σε ιστοχώρους τρίτων που δεν είναι υπό έλεγχο της Bitdefender, οποιασδήποτε από τις παρεχόμενές σε αυτό το έγγραφο συνδέσεις ή από τις παρεχόμενες στο παρόν πόνημα πληροφορίες θα θεωρηθούν εμμέσως από τη Bitdefender, κατόπιν προετοιμασίας της συνδέσεως. Το Bitdefender προϊόν δεν επικρατεί ή δέχεται οποιασδήποτε ευθύνη για την προετοιμασία του τρίτου site.

Εμπορικά σήματα.
Σε αυτό το βιβλίο ενδέχεται να εμφανίζονται ονόματα εμπορικών σημάτων. Όλα τα καταχωρημένα και μη καταχωρημένα εμπορικά σήματα σε αυτό το έγγραφο αποτελούν την αποκλειστική ιδιοκτησία των αντίστοιχων κατάχων τους και αναγνωρίζονται ανάλογα.
Πίνακας Περιεχομένων

Σχετικά με τον οδηγό ............................................................... vii
  1. Σκοπός και κοινό στο οποίο απευθύνεται ........................................ vii
  2. Πώς να χρησιμοποιήσετε αυτό τον οδηγό ........................................ vii

Total Security για PC .......................................................... 1

1. Εγκατάσταση ........................................................................... 2
  1.1. Προετοιμασία εγκατάστασης .................................................. 2
  1.2. Απαιτήσεις συστήματος ......................................................... 3
  1.3. Εγκατάσταση του Bitdefender προϊόντος σας ......................... 4

2. Έναρξη .................................................................................. 12
  2.1. Τα βασικά ............................................................................ 12
  2.2. Βασικό περιβάλλον του Bitdefender ...................................... 22
  2.3. Bitdefender Central ............................................................... 39
  2.4. Διατηρώντας το Bitdefender ενημερωμένο με τις πιο πρόσφατες ενημερώσεις ................................................................. 48

3. Πώς μπορείτε να .................................................................. 54
  3.1. Εγκατάσταση ........................................................................ 54
  3.2. Συνδρομές ......................................................................... 62
  3.3. Bitdefender Central ............................................................... 63
  3.4. Έλεγχος με το Bitdefender .................................................... 66
  3.5. ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ ............................................................. 72
  3.6. Έλεγχος Απορρήτου ............................................................ 80
  3.7. Εργαλεία βελτιστοποίησης ..................................................... 85
  3.8. Χρήσιμες πληροφορίες .......................................................... 87

4. Διαχείριση της ασφάλειας σας ................................................. 97
  4.1. Antivirus Προστασία .............................................................. 97
  4.2. Advanced Threat Defense ................................................... 122
  4.3. ΠΡΟΣΤΑΣΙΑ Web ................................................................. 124
  4.4. Antispam ............................................................................. 126
  4.5. ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ (Firewall) ...................................... 137
  4.6. ΕΥΠΑΘΕΙΑ ..................................................................... 143
  4.7. Προστασία για webcam ......................................................... 152
  4.8. Ασφαλή Αρχεία ................................................................. 154
  4.9. Κρυπτογράφηση Αρχείων ..................................................... 158
  4.10. Προστασία των κωδικών σας με το Διαχειριστή Κωδικών Ασφαλείας ................................................................. 164
  4.11. Ασφάλεια SafePay για online συναλλαγές ............................. 172
  4.12. Προστασία Δεδομένων ....................................................... 178
  4.13. ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ ............................................................. 179
  4.14. Κατά της κλοπής συσκευής (Anti-Theft) ............................ 193
  4.15. USB Immunizer ............................................................... 195

5. Βελτιστοποίηση συστήματος .................................................. 197
  5.1. Εργαλεία ................................................................. 197
  5.2. Προφίλ ............................................................... 201
6. Αντιμετώπιση Προβλημάτων .......................................................... 210
6.1. Επίλυση κοινών ζητημάτων ......................................................... 210
   6.1.1. Το σύστημά μου φαίνεται να είναι αργό ................................ 211
   6.1.2. Η Σάρωση δεν ξεκινάει ....................................................... 212
   6.1.3. Δεν μπορώ πλέον να χρησιμοποιήσω μια εφαρμογή ................. 215
   6.1.4. Τι να κάνετε όταν το Bitdefender εμποδίζει μια ασφαλή ιστοσελίδα ή μια διαδικτυακή εφαρμογή .................................................. 216
   6.1.5. Τι να κάνετε αν το Bitdefender εντοπίζει μια ασφαλή εφαρμογή ως ransomware .......................................................... 217
   6.1.6. Δεν μπορώ να συνδεθώ στο Διαδίκτυο ..................................... 218
   6.1.7. Δεν μπορώ να αποκτήσω πρόσβαση σε μια συσκευή στο δίκτυό μου . 218
   6.1.8. Η σύνδεση μου στο Internet είναι αργή .................................. 221
   6.1.9. Πώς να ενημερώσετε το Bitdefender σε μια αργή σύνδεση στο Internet ................................................................. 222
   6.1.10. Οι Υπηρεσίες του Bitdefender δεν ανταποκρίνονται .................. 223
   6.1.11. Το Antispam φίλτρο δεν λειτουργεί σωστά .................................. 224
   6.1.12. Η λειτουργία αυτόματης συμπλήρωσης στο Πορτοφόλι μου δεν λειτουργεί ................................................................. 229
   6.1.13. Η αφαίρεση του Bitdefender απέτυχε .................................... 231
   6.1.14. Το σύστημά μου δεν ξεκινάει μετά την εγκατάσταση του Bitdefender ............................................................... 232
6.2. Αφαίρεση κακόβουλου λογισμικού από το σύστημά σας .................. 236
   6.2.1. Bitdefender Λειτουργία διάσωσης (Περιβάλλον διάσωσης στα Windows 10) ................................................................. 237
   6.2.2. Τι να κάνετε όταν το Bitdefender βρίσκει ιούς στον υπολογιστή σας; ... 241
   6.2.3. Πώς μπορώ να καθαρίσω έναν ιό σε ένα αρχείο; ......................... 243
   6.2.4. Πώς μπορώ να καθαρίσω έναν ιό σε ένα αρχείο archive e-mail; ...... 244
   6.2.5. Τι πρέπει να κάνω αν υποπτεύομαι ένα αρχείο ως επικίνδυνο; ...... 245
   6.2.6. Ποια είναι τα αρχεία που προστατεύονται με κωδικό πρόσβασης στο αρχείο καταγραφής της σάρωσης; .................. 246
   6.2.7. Ποια είναι τα στοιχεία που έχουν παραλειφθεί στο αρχείο καταγραφής της σάρωσης; .................................................. 246
   6.2.8. Ποια είναι τα υπερ-συμπιεσμένα αρχεία στο αρχείο καταγραφής της σάρωσης; .................................................. 247
   6.2.9. Γιατί το Bitdefender διέγραψε αυτόματα ένα μολυσμένο αρχείο; ...... 247

Antivirus για Mac ............................................................. 248
7. Εγκατάσταση και αφαίρεση ......................................................... 249
   7.1. Απαιτήσεις συστήματος ......................................................... 249
   7.2. Εγκατάσταση του Bitdefender Antivirus for Mac ......................... 249
      7.2.1. Βήματα εγκατάστασης ...................................................... 250
   7.3. Αφαίρεση Bitdefender Antivirus for Mac .................................. 254

8. Ξεκινώντας ............................................................. 255
   8.1. Σχετικά με Bitdefender Antivirus for Mac ................................ 255
   8.2. Άνοιγμα Bitdefender Antivirus for Mac .................................. 255
   8.3. Κεντρικό Παράθυρο Εφαρμογή ................................................. 256
   8.4. Εικονίδιο Application Dock .................................................... 257
9. Προστασία από κακόβουλο λογισμικό .................................................. 259
  9.1. Βέλτιστες πρακτικές ................................................................. 259
  9.2. Σάρωση του Mac σας ............................................................... 260
  9.3. Ενεργοποίηση ή απενεργοποίηση του Autopilot ......................... 261
  9.4. Προστασία Time Machine ......................................................... 261
  9.5. Οδηγός Σάρωσης .................................................................. 263
  9.6. Διόρθωση θεμάτων ................................................................. 264
  9.7. ΠΡΟΣΤΑΣΙΑ Web ................................................................. 296
  9.8. ενημερώσεις ....................................................................... 267
    9.8.1. Ζητώντας ενημέρωση ......................................................... 267
    9.8.2. Παίρνοντας ενημερώσεις μέσω ενός Proxy Server .................. 268
    9.8.3. Αναβάθμιση σε νέα έκδοση .................................................. 268
10. Διαμόρφωση Προτιμήσεων ................................................................. 269
   10.1. Προτιμήσεις Πρόσβασης ......................................................... 269
   10.2. Πληροφορίες Λογαριασμού ....................................................... 269
   10.3. Προτιμήσεις Προστασίας ......................................................... 269
       10.3.1. Σάρωση Εξαιρέσεων ......................................................... 271
   10.4. Ασφαλή Αρχεία .................................................................. 272
       10.4.1. Διαχείριση εφαρμογών ................................................... 274
   10.5. Ιστορικό ............................................................................. 275
   10.6. Καραντίνα ......................................................................... 276
11. Bitdefender Central ................................................................. 277
   11.1. σχετικά με Bitdefender Central ................................................ 277
   11.2. Πρόσβαση στο Bitdefender Central .......................................... 277
   11.3. Οι Συνδρομές μου ................................................................. 278
       11.3.1. Ενεργοποίηση συνδρομής .................................................. 278
       11.3.2. Αγοράστε μια συνδρομή .................................................... 279
   11.4. Οι συσκευές μου ................................................................. 279
       11.4.1. Προσαρμόστε το προϊόν σας ............................................. 279
       11.4.2. Ενέργειες εξ αποστάσεως .................................................. 280
12. Συχνές Ερωτήσεις ................................................................. 281

Mobile Security για Android ................................................................. 286
13. Χαρακτηριστικά Προστασίας ................................................................. 287
14. Ξεκινώντας ........................................................................... 288
15. Σαρωτής Κακόβουλου Λογισμικού .................................................. 293
16. Web Security ............................................................................ 296
17. Ιδιωτικότητα του λογαριασμού .................................................. 298
18. Χαρακτηριστικά Anti-Theft .............................................................. 300
19. Κλείδωμα Εφαρμογών ................................................................. 306
20. Privacy Advisor ........................................................................ 312
<table>
<thead>
<tr>
<th>Νο.</th>
<th>Τίτλος</th>
<th>Παράγραφος</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>ΑΝΑΦΟΡΕΣ</td>
<td>314</td>
</tr>
<tr>
<td>22</td>
<td>WearON</td>
<td>315</td>
</tr>
<tr>
<td>23</td>
<td>Bitdefender Central</td>
<td>316</td>
</tr>
<tr>
<td>24</td>
<td>Συχνές Ερωτήσεις</td>
<td>320</td>
</tr>
<tr>
<td>25</td>
<td>Ζητήσετε βοήθεια</td>
<td>327</td>
</tr>
<tr>
<td>26</td>
<td>Online πηγές</td>
<td>329</td>
</tr>
<tr>
<td>26.1</td>
<td>Κέντρο Υποστήριξης του Bitdefender</td>
<td>329</td>
</tr>
<tr>
<td>26.2</td>
<td>Φόρουμ Υποστήριξης του Bitdefender</td>
<td>330</td>
</tr>
<tr>
<td>26.3</td>
<td>HOTforSecurity Portal</td>
<td>330</td>
</tr>
<tr>
<td>27</td>
<td>Πληροφορίες επικοινωνίας</td>
<td>331</td>
</tr>
<tr>
<td>27.1</td>
<td>Διευθύνσεις Web</td>
<td>331</td>
</tr>
<tr>
<td>27.2</td>
<td>Τοπικοί διανομείς</td>
<td>331</td>
</tr>
<tr>
<td>27.3</td>
<td>Γραφεία Bitdefender</td>
<td>332</td>
</tr>
<tr>
<td>Συνολο</td>
<td>Στείλτε μας τα σχόλιά σας</td>
<td>326</td>
</tr>
<tr>
<td>26</td>
<td>Εργασίες ισχυρής</td>
<td>329</td>
</tr>
<tr>
<td>26.1</td>
<td>Κέντρο Υποστήριξης του Bitdefender</td>
<td>329</td>
</tr>
<tr>
<td>26.2</td>
<td>Φόρουμ Υποστήριξης του Bitdefender</td>
<td>330</td>
</tr>
<tr>
<td>26.3</td>
<td>HOTforSecurity Portal</td>
<td>330</td>
</tr>
</tbody>
</table>
Σχετικά με τον οδηγό

1. Σκοπός και κοινό στο οποίο απευθύνεται

Η συνδρομή σας του Bitdefender Total Security 2018 μπορεί να προστατεύσει έως και 10 διαφορετικά PC, Mac, 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.


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 τρία προϊόντα που περιλαμβάνονται στο Bitdefender Total Security 2018:

- “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. 248)
  Μάθετε πώς να χρησιμοποιείτε το προϊόν στον Mac σας.

- “Mobile Security για Android” (p. 286)
  Μάθετε πώς μπορείτε να χρησιμοποιήσετε το προϊόν για τα Android smartphones και tablets σας.

- “Στείλτε μας τα σχόλιά σας” (p. 326)
  Μάθετε πού θα ψάξετε για βοήθεια αν κάτι αναπάντεχο προκύψει.
TOTAL SECURITY ΓΙΑ PC
1. ΕΓΚΑΤΑΣΤΑΣΗ

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 ο Ηλεκτρονικός Υπολογιστής στον οποίο πρόκειται να εγκαταστήσετε το Bitdefender ικανοποιεί τουλάχιστον τις ελάχιστες απαιτήσεις συστήματος. Εάν ο Ηλεκτρονικός Υπολογιστής δεν ικανοποιεί όλες τις ελάχιστες απαιτήσεις συστήματος, το Bitdefender δεν θα εγκατασταθεί, ή ακόμη και αν εγκατασταθεί θα προκαλέσει επιβραδύνσεις και αστάθεια στο σύστημα. Για τον πλήρη κατάλογο απαιτήσεων συστήματος παρακαλούμε αναφερθείτε στο “Απαιτήσεις συστήματος” (p. 3).

● Συνδεθείτε στον Η/Υ (log-on) χρησιμοποιώντας ένα λογαριασμό διαχειριστή (Administrator).

● Απεγκαταστείστε οποιοδήποτε παρόμοιο λογισμικό από τον Ηλεκτρονικό Υπολογιστή. 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 αφαιρέστε οποιοδήποτε πρόγραμμα τείχους προστασίας που ενδέχεται να εκτελούνται στον υπολογιστή. Η παράλληλη λειτουργία δύο εφαρμογών ασφαλείας μπορεί να επηρεάσει την λειτουργία τους και να δημιουργήσει σημαντικά προβλήματα στο σύστημα. Ο Windows Firewall θα απενεργοποιηθεί κατά την διάρκεια της εγκατάστασης.

● Συνιστάται ιδιαίτερα ο Ηλεκτρονικός σας Υπολογιστής να είναι συνδεδεμένος στο Διαδίκτυο ακόμη και όταν κάνετε εγκάτασταση του λογισμικού από το 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 Ηλεκτρονικό Υπολογιστή ο οποίος λειτουργεί με κάποιο από τα παρακάτω Λειτουργικά Συστήματα:

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

Πριν από την εγκατάσταση, βεβαιωθείτε ότι ο Ηλεκτρονικός σας Υπολογιστής ικανοποιεί τουλάχιστον τις ελάχιστες προδιαγραφές συστήματος

Σημείωση

Για να βρείτε το Λειτουργικό Σύστημα των Windows και πληροφορίες για το hardware του Υπολογιστή σας:

- 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.

Ελάχιστες απαιτήσεις συστήματος

- 1.5 GB ελεύθερος χώρος στον δίσκο
- Επεξεργαστής Dual core 1.6 GHz
- 1 GB μνήμης (RAM)
Προτεινόμενη σύνθεση συστήματος

- Τουλάχιστον 2 GB ελεύθερος χώρος στο σκληρό δίσκο (τουλάχιστον 800 MB στο δίσκο εκκίνησης του συστήματος)
- CPU: Intel CORE 2 Duo (2 GHz) ή ισοδύναμος επεξεργαστής
- 2 GB μνήμης (RAM)

Απαιτήσεις λογισμικού

Για να είναι δυνατή η χρήση του Bitdefender και όλων των δυνατοτήτων του, ο Υπολογιστής σας θα πρέπει να ικανοποιεί όλες τις παρακάτω απαιτήσεις λογισμικού:

- Microsoft Edge 40 και άνω
- Internet Explorer 10 και μεταγενέστερος
- Mozilla Firefox 51 ή μεταγενέστερος
- Google Chrome 34 ή μεταγενέστερο
- Skype version 6.3 ή μεταγενέστερος

1.3. Εγκατάσταση του Bitdefender προϊόντος σας

Μπορείτε να εγκαταστήσετε το Bitdefender από το δίσκο εγκατάστασης ή από το πρόγραμμα εγκατάστασης που κατεβάσατε στον υπολογιστή σας από το Bitdefender Central.

Αν την αγορά σας καλύπτει περισσότερους από έναν υπολογιστές, επαναλάβετε τη διαδικασία εγκατάστασης και ενεργοποιήστε το προϊόν σας με τον ίδιο λογαριασμό σε κάθε υπολογιστή. Ο λογαριασμός που πρέπει να χρησιμοποιήσετε είναι αυτός που περιέχει την ενεργή Bitdefender συνδρομή σας.

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 από το Bitdefender Central:

1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το Οι συσκευές μου.
3. Στο παράθυρο MY DEVICES κάντε κλικ στο INSTALL Bitdefender.

4. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:

   ● ΛΗΨΗ
     Κάντε κλικ στο κουμπί και αποθηκεύσετε το αρχείο εγκατάστασης.

   ● Σε άλλη συσκευή
     Επιλέξτε Windows να κατεβάσετε Bitdefender προϊόν σας και, στη συνέχεια, κάντε κλικ στο κουμπί ΣΥΝΕΧΕΙΑ. Πληκτρολογήστε μια διεύθυνση e-mail στο αντίστοιχο πεδίο, και κάντε κλικ στο ΑΠΟΣΤΟΛΗ.

5. 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 προϊόντος Bitdefender, θα ενημερωθείτε για τα σημεία εκείνα που χρήζουν βελτίωσης πριν προχωρήσετε.

Εάν εντοπιστεί κάποιο ασύμβατο πρόγραμμα antivirus ή κάποια παλιότερη έκδοση του Bitdefender, θα ερωτηθείτε για την αφαίρεσή του από το σύστημα σας. Παρακαλούμε ακολουθείτε τις οδηγίες για την απομάκρυνση του λογισμικού από το σύστημα σας προκειμένου να αποφύγετε προβλήματα που θα εμφανιστούν αργότερα. Μπορεί να χρειαστεί να επανεκκινήσετε τον υπολογιστή σας για να ολοκληρωθεί η απομάκρυνση εντοπισμένου antivirus λογισμικού.

Το πακέτο εγκατάστασης του Bitdefender Total Security επικαιροποιείται διαρκώς.

Σημείωση

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

Αφού επικυρωθεί η εγκατάσταση, θα εμφανιστεί ο βοηθός εγκατάστασης. Ακολουθείτε τα βήματα για να εγκαταστήσετε το Bitdefender Total Security.
Βήμα 1 - Εγκατάσταση Bitdefender

Στην οθόνη εγκατάστασης του Bitdefender, κάντε κλικ στο κουμπί **Εγκατάσταση** για να ξεκινήσετε τη διαδικασία εγκατάστασης του Bitdefender.

Τρεις επιπρόσθετες εργασίες μπορούν να υλοποιηθούν στο βήμα αυτό:

- **Διαβάστε την Άδεια χρήσης τελικού χρήστη πριν προχωρήσετε με την εγκατάσταση.** Η συμφωνία αδειοδότησης περιέχει τους όρους και τις προϋποθέσεις υπό τις οποίες αποκτάτε δικαίωμα χρήσης του Bitdefender Total Security. Εάν δεν συμφωνείτε με τους όρους αυτούς, κλείστε το παράθυρο αυτό. Η διαδικασία εγκατάστασης θα διακοπεί και η εγκατάσταση θα τερματιστεί.

- **Κρατήστε την επιλογή Send anonymous reports ενεργοποιημένη.** Επιτρέπει 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 προϊόντος και θα βοηθήσουν να έχετε καλύτερη εμπειρία χρήσης στο μέλλον. Παρακαλούμε 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.**

Βήμα 2 - Εγκατάσταση σε εξέλιξη

Παρακαλούμε περιμένετε για την ολοκλήρωση της εγκατάστασης. Εμφανίζονται λεπτομερείς πληροφορίες για την πρόοδο της εγκατάστασης και οι πολύ σημαντικοί τομείς του συστήματός σας σκανάρονται για ιούς, οι τελευταίες εκδόσεις των αρχείων της εφαρμογής λαμβάνονται και εγκαθίστανται και και οι υπηρεσίες του προϊόντος Bitdefender ξεκινούν. Αυτό το βήμα μπορεί να διαρκέσει μερικά λεπτά.

Βήμα 3 - Η εγκατάσταση ολοκληρώθηκε

Το Bitdefender προϊόν σας έχει εγκατασταθεί με επιτυχία.

Εμφανίζεται σύνοψη της εγκατάστασης. Εάν κάποια ενεργά κακόβουλα προγράμματα (malware) εντοπίστηκαν και αφαιρέθηκαν κατά την διάρκεια...
της εγκατάστασης, το σύστημα ίσως χρειαστεί επανεκκίνηση. Κάντε κλικ στο **START USING Bitdefender** για να συνεχίσετε.

### Βήμα 4 - Έναρξη

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

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

### 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 πλοήγησείτε 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 προϊόντος Bitdefender, θα ενημερωθείτε για τα σημεία εκείνα που χρήζουν βελτίωσης πριν προχωρήσετε.

Εαν εντοπιστεί κάποιο ασύμβατο πρόγραμμα antivirus ή κάποια παλιότερη έκδοση του Bitdefender, θα ερωτηθείτε για την αφαίρεσή του από το σύστημα σας. Παρακαλούμε ακολουθείστε τις οδηγίες για την απομακρύνση του λογισμικού από το σύστημα σας προκειμένου να αποφύγετε προβλήματα που θα εμφανιστούν αργότερα. Μπορεί να χρειαστεί να
επανεκκινήσετε τον υπολογιστή σας για να ολοκληρωθεί η απομάκρυνση εντοπισμένου antivirus λογισμικού.

**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. Ακολουθείτε τα βήματα για να εγκαταστήσετε το Bitdefender Total Security.

**Βήμα 1 - Εγκατάσταση Bitdefender**

Στην οθόνη εγκατάστασης του Bitdefender, κάντε κλικ στο κουμπί **Εγκατάσταση** για να ξεκινήσετε τη διαδικασία εγκατάστασης του Bitdefender.

Τρεις επιπρόσθετες εργασίες μπορούν να υλοποιηθούν στο βήμα αυτό:

- **Διαβάστε την Άδεια χρήσης τελικού χρήστη πριν προχωρήσετε με την εγκατάσταση.** Η συμφωνία αδειοδότησης περιέχει τους όρους και τις προυποθέσεις υπό τις οποίες αποκτάτε δικαίωμα χρήσης του Bitdefender Total Security.

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

- **Κρατήστε την επιλογή Send anonymous reports ενεργοποιημένη.** Επιτρέπουντας 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 προϊόντος και θα βοηθήσουν να έχετε 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.

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

**Βήμα 2 - Εγκατάσταση σε εξέλιξη**

Παρακαλούμε περιμένετε για την ολοκλήρωση της εγκατάστασης. Εμφανίζονται λεπτομερείς πληροφορίες για την πρόοδο της εγκατάστασης.
Κρίσιμες περιοχές του συστήματός σας σαρώνονται και οι υπηρεσίες του Bitdefender ξεκινούν. Αυτό το βήμα μπορεί να διαρκέσει μερικά λεπτά.

**Βήμα 3 - Η εγκατάσταση ολοκληρώθηκε**

Εμφανίζεται σύνωση της εγκατάστασης. Εάν κάποια ενεργά κακόβουλα προγράμματα (malware) εντοπίστηκαν και αφαιρέθηκαν κατά την διάρκεια της εγκατάστασης, το σύστημα ίσως χρειαστεί επανεκκίνηση. Κάντε κλικ στο **START USING Bitdefender** για να συνεχίσετε.

**Step 4 - Λογαριασμός Bitdefender**

Αφού ολοκληρώσετε την αρχική ρύθμιση, εμφανίζεται το παράθυρο του Bitdefender λογαριασμού. Ένας Bitdefender λογαριασμός απαιτείται προκειμένου να ενεργοποιήσετε το προϊόν και να χρησιμοποιήσετε τις online δυνατότητές του. Για περισσότερες πληροφορίες αναφέρθείτε στο "**Bitdefender Central**" (p. 39).

Συνεχίστε ανάλογα την περίπτωσή σας.

**Θέλω να δημιουργήσω ένα λογαριασμό Bitdefender**

Πληκτρολογήστε τις απαιτούμενες πληροφορίες στα αντίστοιχα πεδία, και στη συνέχεια κάντε κλικ στο κουμπί **CREATE ACCOUNT**.

Τα δεδομένα που εισαγάγατε εδώ παραμένουν εμπιστευτικά.

Ο κωδικός πρόσβασης πρέπει να αποτελείται από τουλάχιστον 8 χαρακτήρες και να περιλαμβάνει ένα ψηφίο.

Πριν προχωρήσετε διαβάστε τους Όρους Χρήσης της Bitdefender.

**Σημείωση**

Μετά την δημιουργία του λογαριασμού μπορείτε να χρησιμοποιήσετε την διεύθυνση ηλεκτρονικού ταχυδρομείου που δώσατε και τον κωδικό πρόσβασης για να συνδεθείτε στο λογαριασμό σας στο https://central.bitdefender.com.

**Έχω ήδη ένα λογαριασμό Bitdefender.**

Κάντε κλικ στο **Sign In**, και στη συνέχεια πληκτρολογήστε το e-mail και το password του Bitdefender λογαριασμού.

Κάντε κλικ στο **SIGN IN** για να συνεχίσετε.

Εάν έχετε ξεχάσει τον κωδικό πρόσβασης για το λογαριασμό σας ή αν απλά θέλετε να επαναφέρετε αυτόν που ήδη έχετε ορίσει, κάντε κλικ...
Στο σύνδεσμο Forgot my password. Πληκτρολογήστε την διεύθυνση e-mail, στη συνέχεια, κάντε κλικ στο κουμπί FORGOT PASSWORD. Ελέγξτε το λογαριασμό e-mail σας και ακολουθήστε τις οδηγίες που παρέχονται για να ορίσετε έναν νέο κωδικό πρόσβασης για το Bitdefender λογαριασμό.

Σημείωση
Αν έχετε ήδη ένα λογαριασμό MyBitdefender, μπορείτε να το χρησιμοποιήσετε για να συνδεθείτε στο Bitdefender λογαριασμό. Εάν έχετε ξεχάσει τον κωδικό πρόσβασης 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 λογαριασμό.

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 μεταφέρθετε 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 5 - 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 έναν 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 I have an activation code και, στη συνέχεια, κάντε κλικ στο κουμπί CONTINUE.

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 προϊόν για 30 ημέρες. Για να ξεκινήσετε τη δοκιμαστική περίοδο, επιλέξτε I don't have a subscription, I want to try the product for free, και στη συνέχεια κάντε κλικ στο κουμπί CONTINUE.

Βήμα 6 - Έναρξη
Στο παράθυρο Get started μπορείτε να δείτε λεπτομέρειες για την ενεργή συνδρομή σας.
Κάντε κλικ στο FINISH για να αποκτήσετε πρόσβαση στο Bitdefender Total Security.
2. ΈΝΑΡΞΗ

2.1. Τα βασικά

Αφού έχετε εγκαταστήσει το Bitdefender Total Security, ο υπολογιστής σας προστατεύεται από κάθε είδους κακόβουλο λογισμικό (όπως ιούς, spyware και trojans) και απειλές του Internet (όπως χάκερ, phishing και ανεπιθύμητη αλληλογραφία).

Η εφαρμογή χρησιμοποιεί την τεχνολογία Photon για να αυξήσει την ταχύτητα και απόδοση της διαδικασίας ανίχνευσης και αναχαίτισης κακόβουλου λογισμικού. 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.

Μπορείτε να παρακολουθείτε τους κωδικούς πρόσβασης και τους λογαριασμούς σας στο διαδίκτυο, αποθηκεύοντάς τα με “Προστασία κωδικών πρόσβασης με το Διαχειριστή Κωδικών Ασφαλείας” (p. 164) σε ένα wallet. Με ένα μοναδικό κύριο κωδικό πρόσβασης είστε σε θέση να προστατεύσετε το απόρρητό σας από εισβολές και σκέφτεστε να κλέψουν χρήματα.

"Προστασία για webcam" (p. 152) Διατηρεί μακριά τις μη αξιόπιστες εφαρμογές από την πρόσβαση στην βιντεοκάμερα σας, αποφεύγοντας έτσι οποιαδήποτε προσπάθεια να παραβιάσετε. Με βάση την επιλογή των χρηστών του Bitdefender, η πρόσβαση σε δημοφιλείς εφαρμογές στην κάμερα σας θα επιτρέπεται ή θα εμποδίζεται.

Για να σας προστατέψουμε από πιθανές ενοχλήσεις και κατασκόπους όταν η συσκευή σας είναι συνδεδεμένη σε μια ασφαλή οικογένεια 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. 148).

Τα προσωπικά σας αρχεία που είναι αποθηκευμένα σε τοπικό επίπεδο, όπως έγγραφα, φωτογραφίες ή ταινίες, καθώς και αυτά που έχουν αποθηκευτεί στο cloud, μπορούν να παραμείνουν τώρα μακριά από το πιο επικίνδυνο κακόβουλο λογισμικό του σήμερα, δηλαδή το ransomware. Για
πληροφορίες σχετικά με τον τρόπο ασφάλισης των προσωπικών αρχείων, ανατρέξτε στο "Ασφαλή Αρχεία" (p. 154).

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 "Προφιλ" (p. 201).

Το Bitdefender θα πάρει για λογαριασμό σας τις περισσότερες σχετιζόμενες με την ασφάλεια αποφάσεις και σπάνια θα σας δείξει pop-up για συναγερμό. Λειτουργεί για τις ενέργειες που εκτελέστηκαν και πληροφορίες για την λειτουργία εφαρμογών είναι διαθέσιμες στο παράθυρο Ειδοποιήσεων. Για περισσότερες πληροφορίες παρακολούθησης αναφερθείτε στο "Ειδοποιήσεις" (p. 16).

Από καιρό σε καιρό, θα πρέπει να ανοίξετε το Bitdefender και να διορθώσετε τυχόν υφιστάμενα προβλήματα. Ισως χρειαστεί να ρυθμίσετε συγκεκριμένα στοιχεία του Bitdefender ή να λάβετε προληπτικά μέτρα για να προστατεύετε τον υπολογιστή σας και τα δεδομένα σας.

Για να χρησιμοποιήσετε τα διαδικτυακά χαρακτηριστικά του Bitdefender ήταν για διαχείριση των συνδρομές και τις συσκευές σας, μπείτε στον Bitdefender λογαριασμό σας. Για περισσότερες πληροφορίες παρακολούθησης αναφερθείτε στο "Bitdefender Central" (p. 39).

Το "Πως μπορείτε να" (p. 54) 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. 210) τμήμα για πιθανές λύσεις των πλέον συνηθισμένων προβλημάτων.

Άνοιγμα παραθύρου του Bitdefender

Για να αποκτήσετε πρόσβαση στο βασικό περιβάλλον του Bitdefender Total Security, ακολουθήστε τα παρακάτω βήματα:

● Στα Windows 7:

1. Κάντε κλικ στην Έναρξη και οδηγηθείτε στο Όλα τα προγράμματα.
2. Κάντε κλικ στο Bitdefender 2018.
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 Total Security από το μενού έναρξης των Windows (για παράδειγμα, μπορείτε να ξεκινήσετε την πληκτρολόγηση "Bitdefender" απευθείας στο μενού Έναρξης) και στη συνέχεια κάντε κλικ στο εικονίδιο 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. 22).

**Διόρθωση θεμάτων**

To Bitdefender χρησιμοποιεί ένα σύστημα παρακολούθησης για να ανιχνεύει και να σας ενημερώνει σχετικά με τα ζητήματα που ενδέχεται να επηρεάσουν την ασφάλεια του υπολογιστή και των δεδομένων σας. Από προεπιλογή θα παρακολουθεί μόνο μια σειρά από ζητήματα που θεωρούνται πολύ σημαντικά. Ωστόσο, μπορείτε να το διαμορφώσετε ανάλογα με τις ανάγκες σας, επιλέγοντας για ποια συγκεκριμένα θέματα επιθυμείτε να λαμβάνετε ειδοποιήσεις.

Κάποια εντοπισμένα ζητήματα περιλαμβάνουν σημαντικές ρυθμίσεις προστασίας που είναι απενεργοποιημένες και άλλες καταστάσεις που μπορεί να αποτελέσουν κίνδυνο για την ασφάλεια. Ομαδοποιούνται σε δύο κατηγορίες:

- **Κρίσιμα ζητήματα** - εμποδίζουν το Bitdefender στην προστασία σας ενάντια σε κακόβουλο λογισμικό ή αποτελούν σημαντικό κίνδυνο για την ασφάλεια.

- **Μικρά (μη-κρίσιμα) ζητήματα** - μπορούν να επηρεάσουν την προστασία σας στο άμεσο μέλλον.
Το εικονίδιο του Bitdefender στην περιοχή ειδοποιήσεων υποδεικνύει εκκρεμότητες με την αλλαγή χρώματος του ως εξής:

- Τα κρίσιμα ζητήματα επηρεάζουν την ασφάλεια του συστήματος σας. Απαιτούν την άμεση προσοχή σας και πρέπει να διορθωθούν το συντομότερο δυνατόν.
- Μη κρίσιμα ζητήματα επηρεάζουν την ασφάλεια του συστήματος σας. Θα πρέπει να τα ελέγξετε και να τα διορθώσετε όταν έχετε το χρόνο.

Επίσης, εάν μετακινήσετε τον κέρσο του ποντικιού πάνω από το εικονίδιο, ένα αναδυόμενο παράθυρο θα επιβεβαίωσει την ύπαρξη των ζητημάτων που εκκρεμούν.

Όταν ανοίξετε την Bitdefender πλατφόρμα, η περιοχή της κατάστασης ασφαλείας στην επάνω γραμμή εργαλείων θα αναφέρει τη φύση των ζητημάτων που επηρεάζουν το σύστημα σας.

Οδηγός για θέματα ασφαλείας

Για να διορθώσετε τα ζητήματα που έχουν εντοπιστεί ακολουθήστε τον οδηγό Security Issues.

1. Για να ανοίξετε τον οδηγό, κάντε ένα από τα παρακάτω:
   - Κάντε δεξί κλικ στο εικονίδιο του Bitdefender στην περιοχή ειδοποιήσεων και επιλέξτε Προβολή θεμάτων ασφάλειας.
   - Ανοίξτε το Bitdefender και κάντε κλικ οπουδήποτε μέσα στην Περιοχή Κατάστασης Ασφαλείας στην επάνω γραμμή εργαλείων.

2. Μπορείτε να δείτε τα θέματα που επηρεάζουν την ασφάλεια του υπολογιστή και των δεδομένων σας. Όλα τα τρέχοντα ζητήματα έχουν επιλεχθεί για να διορθωθούν.

   Αν δεν επιθυμείτε να διορθώσετε ένα συγκεκριμένο ζήτημα αμέσως, αποποιηθείτε το αντίστοιχο κουτάκι επιλογής. Θα σας ζητηθεί να καθορίσετε για πόσο χρονικό διάστημα θα αναβληθεί η διόρθωση του ζητήματος. Επιλέξτε την επιθυμητή επιλογή από το μενού και κάντε κλικ στο OK. Για να σταματήσετε την παρακολούθηση της κατηγορίας για το αντίστοιχο ζήτημα, επιλέξτε Μόνιμα.

   Η κατάσταση του ζητήματος θα αλλάξει σε Αναβλήθηκε και καμία ενέργεια δεν θα ληφθεί για να διορθωθεί το πρόβλημα.
3. Για να διορθώσετε τα επιλεγμένα ζητήματα, κάντε κλικ στο Διόρθωση. Ορισμένα ζητήματα διορθώνονται αμέσως. Για άλλα, ένας οδηγός σας βοηθάει να τα διορθώσετε.

Τα ζητήματα, που αυτός ο οδηγός σας βοηθά να διορθώσετε, μπορούν να ομαδοποιηθούν σε αυτές τις κύριες κατηγορίες:

- **Απενεργοποιημένες ρυθμίσεις ασφαλείας.** Τέτοια ζητήματα διορθώνονται αμέσως, ενεργοποιώντας τις αντίστοιχες ρυθμίσεις ασφαλείας.

- **Προληπτικές εργασίες ασφαλείας που χρειάζεται να εκτελέσετε.** Κατά την διόρθωση αυτών των ζητημάτων, ένας οδηγός σας βοηθάει να ολοκληρώσετε με επιτυχία την εργασία.

**Διαμόρφωση Κατάστασης Ειδοποιήσεων**

Το Bitdefender μπορεί να σας ενημερώσει όταν εμφανιστούν θέματα στην λειτουργία των παρακάτω υποσυστημάτων του προγράμματος:

- **Antivirus**
- **ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ (Firewall)**
- **Ενημέρωση**
- **Ασφάλεια Πλοήγησης**

Μπορείτε να ρυθμίσετε το σύστημα προειδοποίησης, για να εξυπηρετεί καλύτερα τις ανάγκες ασφαλείας σας, επιλέγοντας ποια συγκεκριμένα ζητήματα πρέπει να ενημερώνονται. Ακολουθείστε αυτά τα βήματα:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Advanced.
3. Κάντε κλικ στον σύνδεσμο Διαμόρφωση κατάστασης ειδοποιήσεων.
4. Κάντε κλικ στις επιλογές για να ενεργοποιήσετε ή να απενεργοποιήσετε τις ειδοποιήσεις κατάστασης σύμφωνα με τις προτιμήσεις σας.

**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 Ενημερώσεις 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 βρέθηκε κακόβουλο λογισμικό 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 εικονίδιο στην αριστερή μπάρα του Bitdefender interface. Κάθε φορά που συμβαίνει κάποιο γεγονός, ένας μετρητής μπορεί να παρατηρήθει στο 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 αναγνωσμένη των γεγονότων σας αυτό το τμήμα.

**Autopilot**

Για όλους τους χρήστες που θέλουν από τη λύση της ασφάλειάς τους απλά να προστατεύονται χωρίς να ενοχλούνται, το Bitdefender Total Security έχει σχεδιαστεί με μία ενσωματωμένη λειτουργία αυτόματου πιλότου.
Κατά την λειτουργία αυτόματου πιλότου, το Bitdefender εφαρμόζει τη βέλτιστη ρύθμιση παραμέτρων ασφαλείας και λαμβάνει όλες τις σχετικές με την ασφάλεια αποφάσεις για εσάς. Αυτό σημαίνει ότι σπάνια θα βλέπετε αναδυόμενα παράθυρα και δεν θα χρειαστεί να προχωρήσετε σε καμία ρύθμιση.

Στη λειτουργία του Αυτόματου Πιλότου, το Bitdefender διορθώνει αυτόματα κρίσιμα ζητήματα, επιτρέπει και αθόρυβα διαχειρίζεται:

- Αntivirus προστασία, που παρέχεται από σάρωση κατά την πρόσβαση αλλά και τη συνεχή σάρωση.
- Προστασία Firewall.
- Προστασία Web.
- Αυτόματες ενημερώσεις.

Για να ενεργοποιήσετε ή να απενεργοποιήσετε τον αυτόματο πιλότο, κάντε κλικ στην επιλογή Αυτόματος πιλότος που βρίσκεται στην επάνω γραμμή εργαλείων του Bitdefender interface.

Για όσο διάστημα ο Αυτόματος Πιλότος είναι ενεργοποιημένος, το εικονίδιο του Bitdefender στην περιοχή ειδοποιήσεων αλλάζει σε 📴.

Σημαντικό
Ενώ ο Αυτόματος Πιλότος είναι ενεργοποιημένος, τροποποιώντας οποιαδήποτε από τις ρυθμίσεις που διαχειρίζεται θα έχει ως αποτέλεσμα να απενεργοποιηθεί.

Για να δείτε το ιστορικό των ενεργειών που εκτελέστηκαν από το Bitdefender, ενώ το Autopilot εχει ενεργοποιηθεί, ανοίξτε το παράθυρο Notifications.

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 αναβληθούν 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 δραστηριότητες 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.

Για να επιτρέψετε στο Bitdefender να διαχειριστεί τα προφίλ:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Profiles.
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 ON/OFF. Μόνο ένα προφίλ μπορεί να ενεργοποιηθεί χειροκίνητα ταυτόχρονα.

Για περισσότερες πληροφορίες σχετικά με τα Προφίλ, παρακαλούμε ανατρέξτε στο “Προφίλ” (p. 201)

Ρυθμίσεις προστασίας του Κωδικού πρόσβασης του Bitdefender

Εάν δεν είστε το μόνο πρόσωπο με δικαιώματα διαχειριστή χρήσης αυτού του υπολογιστή, συνιστάται να προστατεύσετε τις προσωπικές ρυθμίσεις του Bitdefender σας με κωδικό πρόσβασης.

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

1. Κάντε κλικ στο εικονίδιο α στην αριστερή μπάρα του Bitdefender interface.
2. Στο παράθυρο του Γενικά, ενεργοποιήστε το Προστασία με κωδικό πατώντας τον αντίστοιχο διακόπτη.
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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Στο παράθυρο του Πρόσβασης, απενεργοποιήστε την προστασία με κωδικό πατώντας τον αντίστοιχο διακόπτη.

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 στον σύνδεσμο Αλλαγή κωδικού. Πληκτρολογήστε τον τρέχοντα κωδικό πρόσβασης και στη συνέχεια κάντε κλικ στο κουμπί 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.

### Αναφορές Ανώνυμης Χρήσης

Από προεπιλογή, το Bitdefender στέλνει εκθέσεις που περιέχουν πληροφορίες σχετικά με το χρησιμοποιείτε το προϊόν στους Bitdefender servers. Οι πληροφορίες αυτές είναι απαραίτητες για την βελτίωση του προϊόντος και μπορούν να μας βοηθήσουν να σας προσφέρουμε μια καλύτερη εμπειρία χρήσης στο μέλλον. Παρακαλώ σημειώστε ότι οι αναφορές αυτές θα περιέχουν μη εμπιστευτικά δεδομένα, όπως το όνομα ή η διεύθυνση IP, και ότι δεν θα χρησιμοποιηθούν για εμπορικούς σκοπούς.

Σε περίπτωση που θέλετε να σταματήσετε την αποστολή Ανώνυμων αναφορών χρήσης:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Advanced.
3. Κάντε κλικ στους αντίστοιχους διακόπτες ON/OFF.

### 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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα 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 **ΣΥΝΕΧΕΙΑ** για να συνεχίσετε με τις οδηγίες, ή **Παράλειψη περιήγησης** για να κλείσετε τον οδηγό.

Για να δείτε την κατάσταση του προϊόντος και να εκτελείτε βασικές εργασίες, το εικονίδιο του Bitdefender στην περιοχή ειδοποιήσεων είναι διαθέσιμο οποιαδήποτε στιγμή.

Το main window σας επιτρέπει να διαχειριστείτε τη συμπεριφορά του προϊόντος με τη χρήση Autopilot, σας δίνει πρόσβαση σε σημαντικές πληροφορίες για το προϊόν και σας επιτρέπει να εκτελέσετε συνήθεις εργασίες. Από την αριστερή μπάρα μπορείτε να έχετε πρόσβαση στο Bitdefender λογαρισμό και το Bitdefender sections για λεπτομερείς ρυθμίσεις και προχωρημένη διαχείριση.

Αν θέλετε να παρακολουθείτε σταθερά τις βασικές πληροφορίες για την ασφάλεια και να έχετε γρήγορη πρόσβαση σε βασικές ρυθμίσεις, προσθέστε το Οδηγό Ασφαλείας στην επιφάνεια εργασίας σας.

**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 ειδοποίησεων.

3. Επιλέξτε Εικονίδια και ειδοποίησεις για το εικονίδιο του Bitdefender Agent.

   ● Στα Windows 10:
     1. Κάντε δεξί κλικ στη γραμμή εργασιών και επιλέξτε Ιδιότητες.
     2. Κάντε κλικ στο Προσαρμογή στο παράθυρο της γραμμής εργασιών.
     3. Κάντε κλικ και επιλέξτε τα εικονίδια τα οποία θα εμφανίζονται στη γραμμή εργασιών. από το παράθυρο Επιλογή των εικονιδίων και των ειδοποίησεων & που εμφανίζονται στη γραμμή εργασιών.
     4. 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.

● Εμφάνιση - ανοίγει το κύριο παράθυρο του Bitdefender.

● Σχετικά - Ανοίγει ένα παράθυρο όπου μπορείτε να δείτε πληροφορίες σχετικά με το Bitdefender και πού να ψάξετε για βοήθεια σε περίπτωση που κάτι απροσδόκητο εμφανιστεί.

● Εμφάνιση θεμάτων ασφάλειας - σας βοηθά να καταργήσετε τα τρέχοντα τρωτά σημεία της ασφάλειας. Εάν η επιλογή δεν είναι διαθέσιμη, δεν υπάρχουν ζητήματα που πρέπει να διοικηθούν. Για λεπτομερείς πληροφορίες πληροφορίες, παρακαλούμε ανατρέξτε στο “Διόρθωση θεμάτων” (p. 14).

● Απόκρυψη / Εμφάνιση Οδηγού Ασφαλείας - ενεργοποιεί / απενεργοποιεί το Οδηγός Ασφάλειας.

● Ενημέρωση Τώρα - ξεκινά μια άμεση ενημέρωση. Μπορείτε να παρακολουθείτε την κατάσταση ενημέρωσης στον πίνακα Ενημέρωση στο βασικό παράθυρο Bitdefender.

● Εμφάνιση Αναφοράς Ασφαλείας - Ανοίγει ένα παράθυρο όπου μπορείτε να δείτε μια εβδομαδιαία κατάσταση και συστάσεις για το σύστημά σας. Μπορείτε να ακολουθήσετε τις συστάσεις για να βελτιώσετε την ασφάλεια του συστήματός σας.
Το Bitdefender εικονίδιο στην περιοχή ειδοποιήσεων σας ενημερώνει όταν υπάρχουν θέματα τα οποία επηρεάζουν τον υπολογιστή σας ή το πώς το προϊόν λειτουργεί, εμφανίζοντας ένα ειδικό σύμβολο, ως εξής:

zą Ζητήματα επηρεάζουν την ασφάλεια του συστήματός σας. Απαιτείται η άμεση προσοχή σας και πρέπει να διορθωθούν το συντομότερο δυνατόν.

monds Ζητήματα επηρεάζουν την ασφάλεια του συστήματός σας. Θα πρέπει να τα ελέγξετε και να τα διορθώσετε όταν έχετε το χρόνο.

zą Ο Αυτόματος Πιλότος του Bitdefender δραστηριοποιείται.

Εάν το Bitdefender δεν λειτουργεί, το εικονίδιο στην περιοχή ειδοποιήσεων εμφανίζεται σε γκρίζο φόντο: Ε. Αυτό συμβαίνει συχνά 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.

Κύριο Παράθυρο

Το κύριο παράθυρο του Bitdefender 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 χωρισμένο σε τέσσερις βασικούς τομείς:

1. Περιοχή κατάστασης
   Εδώ μπορείτε να ελέγξετε την κατάσταση ασφάλειας του υπολογιστή σας, να ξεκινήσετε μια ενημέρωση και να ρυθμίσετε το Autopilot.

2. Αριστερή μπάρα
   Αυτό το μενού σας επιτρέπει να περιήχεστε στο εβδομαδιαίο Security Report, στις Γενικές ρυθμίσεις και στο Help & Support.

3. Κουμπιά δράσης και πρόσβαση στην περιοχή λειτουργιών
   Εδώ μπορείτε να εκτελέσετε διάφορες εργασίες για να διατηρήσετε προστατευμένο το σύστημά σας και για να λειτουργεί σε βέλτιστη ταχύτητα. Επίσης, μπορείτε να έχετε πρόσβαση στις ενότητες του Bitdefender για να ρυθμίσετε το προϊόν μόνος σας.
Κάτω μπάρα

Εδώ μπορείτε πολύ εύκολα να εγκαταστήσετε το Bitdefender σε άλλες συσκευές, με την προϋπόθεση ότι η συνδρομή σας τον ικανό αριθμό συσκευών.

Περιοχή κατάστασης

Η περιοχή κατάστασης περιέχει τα ακόλουθα στοιχεία:

- Το Security Status στην αριστερή πλευρά της γραμμής εργαλείων, σας ενημερώνει αν υπάρχουν οποιαδήποτε ζητήματα που επηρεάζουν την ασφάλεια του υπολογιστή σας και σας βοηθά να τα διορθώσετε.

- Το χρώμα στην περιοχή κατάστασης της ασφάλειας αλλάζει ανάλογα με τα ζητήματα που έχουν εντοπιστεί και εμφανίζονται διαφορετικά μηνύματα:
  - Η περιοχή έχει πράσινο χρώμα. Δεν υπάρχουν ζητήματα για διόρθωση. Ο υπολογιστής και τα δεδομένα σας είναι προστατευμένα.
  - Η περιοχή έχει κίτρινο χρώμα. Μη κρίσιμα ζητήματα επηρεάζουν την ασφάλεια του συστήματός σας. Θα πρέπει να τα ελέγξετε και να τα διορθώσετε όταν έχετε το χρόνο.
  - Η περιοχή έχει κόκκινο χρώμα. Τα κρίσιμα ζητήματα επηρεάζουν την ασφάλεια του συστήματός σας. Θα πρέπει να αντιμετωπίσετε αμέσως αυτά τα ζητήματα.

- Κάνοντας κλικ σε οποιοδήποτε σημείο μέσα στην περιοχή κατάστασης ασφαλείας, μπορείτε να αποκτήσετε πρόσβαση σε έναν οδηγό που θα σας βοηθήσει να απομακρύνετε εύκολα τυχόν απειλές από τον υπολογιστή σας. Για λεπτομερείς πληροφορίες, παρακαλούμε ανατρέξτε στο “Διόρθωση θεμάτων” (p. 14).

- Το Autopilot σας δίνει τη δυνατότητα να αποκτήσετε βέλτιστη προστασία και να απολαύσετε εντελώς αθόρυβη ασφάλεια. Για λεπτομερείς πληροφορίες, παρακαλούμε ανατρέξτε στο “Autopilot” (p. 17).

- Το UPDATE NOW σας επιτρέπει να εκτελέσετε μια ενημερωμένη του προϊόντος κάθε φορά που θέλετε να βεβαιωθείτε ότι έχετε τις πιο πρόσφατες υπογραφές malware. Για λεπτομερείς πληροφορίες, παρακαλούμε ανατρέξτε στο “Διατηρώντας το Bitdefender ενημερωμένο με τις πιο πρόσφατες ενημερώσεις” (p. 48).
Το Active Profile εμφανίζει το τρέχον ενεργοποιημένο προφίλ του Bitdefender. Για λεπτομερείς πληροφορίες, παρακαλούμε ανατρέξτε στο “Προφίλ” (p. 201).

Αριστερή μπάρα

Εικονίδια υπόδειξης είναι διαθέσιμα στην αριστερή μπάρα που σας δίνουν πρόσβαση στο Bitdefender λογαρισμό, τα τμήματα του προϊόντος, έκθεση πεπραγμένων, ειδοποιήσεις, γενικές ρυθμίσεις και υποστήριξη.

Τα ονόματα των εικονιδίων είναι ορατά κάνοντας κλικ στο εικονίδιο ☐, ως εξής:

● ☐ Protection. Τα ενεργά κουμπιά Quick Scan και Vulnerability Scan γίνονται ορατά στην κάτω αριστερή γωνία του Bitdefender interface. Επίσης, γίνονται ορατές πληροφορίες σχετικά με εφαρμογές που έχουν μπλοκάριστε και απειλές και επιθέσεις που εχουν ανιχνευθεί. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΕΝΟΤΗΤΩΝ για να αποκτήσετε πρόσβαση στην περιοχή διαμόρφωσης.

● ☐ Privacy. Τα κουμπιά επιλογών Safepay και Parental Advisor γίνονται ορατά στην κάτω αριστερή γωνία του Bitdefender interface. Επίσης, εμφανίζονται πληροφορίες σχετικά με τα wallets και τα vaults αρχεία. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΕΝΟΤΗΤΩΝ για να αποκτήσετε πρόσβαση στην περιοχή διαμόρφωσης.

● ☞ Εργαλεία. Τα κουμπιά επιλογών OneClick Optimizer και Startup Optimizer γίνονται ορατά στην κάτω αριστερή γωνία του Bitdefender interface. Επίσης, εμφανίζονται πληροφορίες σχετικά με το βελτιστοποιημένο χώρο και το Disk Cleanup μπορεί να ξεκινήσει για να κάνει χώρο με τα νέα δεδομένα, διαγράφοντας μεγάλα αρχεία και φακέλους που δεν χρησιμοποιείτε πια. Επιπλέον, μπορεί να προσεγγιστεί η λειτουργία Anti-Theft.

● ☁ Δραστηριότητα. Από εδώ, μπορείτε να δείτε τη δραστηριότητα του προϊόντος κατά τις τελευταίες 30 ημέρες και πρόσβαση στην έκθεση ασφαλείας που παράγεται κάθε επτά ημέρες.

● ☕ Notifications. Από εδώ, έχετε πρόσβαση στις παραγώμενες ειδοποιήσεις.
Λογαριασμός

Λεπτομέρειες σχετικά με το Bitdefender λογαρισμό και τη συνδρομή που χρησιμοποιείτε είναι διαθέσιμες. Αποκτήστε πρόσβαση στον Bitdefender λογαρισμό σας για να επαληθεύσετε τις συνδρομές σας και την εκτέλεση των εργασιών ασφαλείας στις συσκευές που διαχειρίζεστε.

Ρυθμίσεις

Από εδώ έχετε πρόσβαση στις γενικές ρυθμίσεις.

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.

Κουμπιά δράσης και πρόσβαση στην περιοχή λειτουργιών

Χρησιμοποιώντας τα κουμπιά ενεργειών μπορείτε να ξεκινήσετε γρήγορα την εκτέλεση σημαντικών εργασιών. Τα κουμπιά ενεργειών γίνονται ορατά στην κάτω αριστερή γωνία του Bitdefender interface όταν επιλέγετε ένα από τα τρία τμήματα: Protection, Privacy ή Tools από την αριστερή μπάρα.

Ανάλογα με το τμήμα που θα επιλέξετε, τα ορατά κουμπιά ενεργειών σε αυτόν τον τομέα μπορεί να είναι:

Γρήγορη Σάρωση

Εκτελέστε μια γρήγορη σάρωση για να βεβαιωθείτε ότι ο υπολογιστής σας είναι καθαρό από κακόβουλο λογισμικό.

Σάρωση για ευπάθειες

Σαρώστε τον υπολογιστή σας για τρωτά σημεία για να βεβαιωθείτε ότι όλες οι εγκατεστημένες εφαρμογές, μαζί με το λειτουργικό σύστημα, ενημερώνονται και λειτουργούν σωστά.

Safepay

Ανοίξτε το Bitdefender Safepay™ για την προστασία των ευαίσθητων δεδομένων σας, ενώ πραγματοποιείτε διαδικτυακές συναλλαγές.

Γονικός Έλεγχος

Μπείτε στο Bitdefender Parental Advisor για να είστε ενημερωμένοι σχετικά με τις δραστηριότητες των παιδιών σας.

OneClick Optimizer

Ελευθερώστε χώρο στο δίσκο, διορθώστε τα σφάλματα μητρώου και προστατεύστε τα προσωπικά σας δεδομένα διαγράφοντας τα αρχεία που δεν μπορούν πλέον να είναι χρήσιμα με ένα μόνο κλικ.

Startup Optimizer

Μειώστε το χρόνο εκκίνησης του συστήματος σας, αποκλείοντας τις περιττές εφαρμογές να εκτελεστούν κατά την εκκίνηση.
Κάτω μπάρα

Για να αρχίσετε να προστατεύετε επιπλέον συσκευές:

1. Επιλέξτε τον σύνδεσμο ΕΓΚΑΤΑΣΤΑΣΗ ΣΕ ΆΛΛΗ ΣΥΣΚΕΥΗ.

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

2. Στο παράθυρο που εμφανίζεται επιλέξτε το επιθυμητό λειτουργικό σύστημα και στη κατόπιν επιλέξτε ΣΥΝΕΧΕΙΑ.

3. Πληκτρολογήστε τη διεύθυνση e-mail που θα θέλατε λάβετε τον σύνδεσμο λήψης και εγκατάστασης της εφαρμογής για το επιλεγμένο λειτουργικό σύστημα.

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 iOS συσκευές.
- Bitdefender Γονικός Έλεγχος για macOS, iOS και συσκευές Android.

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 περιγραφεί 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 στην αριστερή μπάρα του Bitdefender interface:

- ΠΡΟΣΤΑΣΙΑ
- ΙΔΙΩΤΙΚΟΤΗΤΑ
- Εργαλεία
ΠΡΟΣΤΑΣΙΑ

Στην ενότητα Προστασία, μπορείτε να ρυθμίσετε το επίπεδο ασφαλείας σας, να διαχειριστείτε τους φίλους και τους spammers, να προβάλετε και να επεξεργαστείτε τις ρυθμίσεις σύνδεσης με το δίκτυο, να ρυθμίσετε την προστασία ransomware και των web χαρακτηριστικών, να ελέγξετε και να διορθώσετε πιθανά τρωτά σημεία του συστήματος και να αξιολογήσετε την ασφάλεια των ασύρματων δικτύων που 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 κακόβουλο λογισμικό, όπως οι ιοί, trojans, spyware, adware, κλπ.

Από την ενότητα Antivirus μπορείτε εύκολα να έχετε πρόσβαση στις ακόλουθες εργασίες σάρωσης:
- Γρήγορη Σάρωση
- Σάρωση Συστήματος
- Διαχείριση Σαρώσεων
- Λειτουργία διάσωσης (Περιβάλλον διάσωσης στα Windows 10)

Για περισσότερες πληροφορίες σχετικά με τις εργασίες σάρωσης και το πως να ρυθμίσετε την προστασία από ιούς, ανατρέξτε στο “Antivirus Προστασία” (p. 97).

ΠΡΟΣΤΑΣΙΑ WEB

Η προστασία Web 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 “ΠΡΟΣΤΑΣΙΑ Web” (p. 124).

FIREWALL

Το τείχος προστασίας σας προστατεύει, ενώ είστε συνδεδεμένοι με το δίκτυα και το Διαδίκτυο φιλτράροντας όλες τις προσπάθειες σύνδεσης.
Για περισσότερες πληροφορίες σχετικά με τη διαμόρφωση του τείχου προστασίας σας, παρακαλούμε ανατρέξτε στο “ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ (Firewall)” (p. 137).

ADVANCED THREAT DEFENSE
Το Advanced Threat Defense προστατεύει ενεργά το σύστημά σας από κακόβουλα προγράμματα, 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 κακόβουλο λογισμικό, ανατρέξτε στο “Advanced Threat Defense” (p. 122).

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. 126).

ΕΥΠΑΘΕΙΕΣ
Η λειτουργία Ευπάθειας σας βοηθά να διατηρείτε το λειτουργικό σύστημα και τις εφαρμογές που χρησιμοποιείτε τακτικά μέχρι σήμερα και να εντοπίσετε τα μη ασφαλή ασύρματα δίκτυα στα οποία συνδέεστε.

Κάντε κλικ στη Σάρωση ευπάθειας στην ενότητα ευπάθειας για να ξεκινήσει τον εντοπισμό κρίσιμων ενημερώσεων των Windows, ενημερώσεως εφαρμογών, αδύναμους κωδικούς πρόσβασης που ανήκουν σε λογαριασμούς των Windows και τα ασύρματα δίκτυα που δεν είναι ασφαλή.

Κάντε κλικ στο Wi-Fi Security Advisor για να δείτε τη λίστα με τα ασύρματα δίκτυα που συνδέεστε, μαζί με την εκτίμηση της αξιοπιστίας τους, και τις ενέργειες που μπορείτε να κάνετε για να παραμείνετε ασφαλείς.

Για περισσότερες πληροφορίες σχετικά με τη ρύθμιση της προστασίας των ευπαθειών, ανατρέξτε στο “ΕΥΠΑΘΕΙΑ” (p. 143).

ΑΣΦΑΛΗ ΑΡΧΕΙΑ
Η λειτουργία ασφαλών αρχείων διασφαλίζει ότι τα προσωπικά σας αρχεία παραμένουν προστατευμένα από επιθέσεις ransomware.
Για περισσότερες πληροφορίες σχετικά με τον τρόπο διαμόρφωσης των ασφαλών αρχείων για την προστασία των προσωπικών σας αρχείων από επιθέσεις ransomware, ανατρέξτε στο "Ασφαλή Αρχεία" (p. 154).

ΙΔΙΩΤΙΚΟΤΗΤΑ

Στην ενότητα Προστασία προσωπικών δεδομένων μπορείτε να κρυπτογραφήσετε τα προσωπικά σας δεδομένα, την προστασία των ηλεκτρονικών σας συναλλαγών, να κρατήσει την εμπειρία περιήγησής σας ασφαλές και να προστατεύσει τα παιδιά σας στην online δραστηριότητά τους.

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

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΟΥ

Δημιουργήστε κρυπτογραφημένα, προστατευόμενους από κωδικό πρόσβασης λογικούς δίσκους (ή θησαυροφυλάκια) στον υπολογιστή σας, όπου μπορείτε να αποθηκεύετε με ασφάλεια τα εμπιστευτικά και ευαίσθητα έγγραφά σας.

Για περισσότερες πληροφορίες σχετικά με το πώς να δημιουργήσετε κρυπτογραφημένες, προστατευόμενες με κωδικό λογικές μονάδες δίσκου (ή θησαυροφυλάκια) στον υπολογιστή σας, ανατρέξτε στο "Κρυπτογράφηση Αρχείου" (p. 158).

ΠΡΟΣΤΑΣΙΑ ΓΙΑ WEBCAM

Η Προστασία Bitdefender Webcam κρατά την κάμερά σας εκτός κινδύνου, αποκλείοντας την πρόσβαση των μη αξιόπιστων εφαρμογών.

Για περισσότερες πληροφορίες σχετικά με τον τρόπο προστασίας της webcam από ανεπιθύμητη πρόσβαση, ανατρέξτε στο "Προστασία για webcam" (p. 152).

WALLET

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

Για περισσότερες πληροφορίες σχετικά με τη διαμόρφωση του Διαχειριστή Κωδικών Ασφαλείας, παρακαλούμε ανατρέξτε στο "Προστασία των κωδικών σας με το Διαχειριστή Κωδικών Ασφαλείας" (p. 164).
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.

Κάντε κλικ στο κουμπί Safepay από τη διεπαφή Bitdefender για να αρχίσετε τις online συναλλαγές σε ένα ασφαλές περιβάλλον.

Για περισσότερες πληροφορίες σχετικά με το Bitdefender Safepay™, παρακαλούμε ανατρέξτε στο “Ασφάλεια Safepay για online συναλλαγές” (p. 172).

ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ
Ο Γονικός Σύμβουλος Bitdefender σας επιτρέπει να παρακολουθείτε τι κάνει το παιδί σας στον υπολογιστή. Σε περίπτωση ακατάλληλου περιεχομένου, μπορείτε να αποφασίσετε να περιορίσετε την πρόσβασή του στο Διαδίκτυο ή σε συγκεκριμένες εφαρμογές.

Κάντε κλικ στο Διαμόρφωση στην μονάδα Γονικού Συμβουλίου 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 διαμόρφωση του Γονικού Συμβουλίου, παρακαλούμε ανατρέξτε στο “ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ” (p. 179).

ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ
Η ενότητα Προστασίας Δεδομένων σας επιτρέπει να διαγράψετε μόνιμα τα αρχεία σας.

Για περισσότερες πληροφορίες σχετικά με τη διαμόρφωση της Προστασίας των Δεδομένων, παρακαλούμε ανατρέξτε στο "Προστασία Δεδομένων" (p. 178).

Εργαλεία
Στα ενότητα εργαλεία μπορείτε να βελτιώσετε την ταχύτητα του συστήματος και να διαχειριστείτε τις συσκευές σας.

Tune-Up
Το Bitdefender Total Security δεν προσφέρει μόνο ασφάλεια, σας βοηθά επίσης να κρατήσετε την απόδοση του υπολογιστή σας σε φόρμα.
Στην ενότητα Tune-Up μπορείτε να αποκτήσετε πρόσβαση σε μια σειρά από χρήσιμα εργαλεία:
- OneClick Optimizer
- Startup Optimizer
- Disk Cleanup

Για περισσότερες πληροφορίες σχετικά με τα εργαλεία βελτιστοποίηση της επίδοσης, ανατρέξτε στο "Εργαλεία" (p. 197).

**Anti-Theft**

το Bitdefender Anti-Theft προστατεύει τον υπολογιστή και τα δεδομένα σας από κλοπή ή απώλεια. Σε περίπτωση τέτοιου συμβάντος, αυτό σας επιτρέπει να εντοπίσετε ή να κλειδώσετε τον υπολογιστή 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 σύστημα σας μακριά από τα λάθος χέρια, παρακαλούμε ανατρέξτε στο "Κατά της κλοπής συσκευής (Anti-Theft)" (p. 193).

**Widget Ασφαλείας**

Ο Οδηγός Ασφαλείας είναι ο γρήγορος και εύκολος τρόπος για να παρακολουθείτε και να ελέγχετε το Bitdefender Total Security. Η προσθήκη αυτού του μικρού και μη παρεμβατικού widget στην επιφάνεια εργασίας σας επιτρέπει να δείτε τις κρίσιμες πληροφορίες και να εκτελεί τα βασικά καθήκοντα, ανά πάσα στιγμή:
- ανοίξτε το κύριο παράθυρο του Bitdefender.
- παρακολουθήστε τη δραστηριότητα της σάρωσης σε πραγματικό χρόνο.
- παρακολουθήστε την κατάσταση ασφαλείας του συστήματός σας και διορθώστε τυχόν υπάρχοντα ζητήματα.
- δείτε όταν μια ενημέρωση είναι σε εξέλιξη.
- δείτε τις ειδοποιήσεις και αποκτήστε πρόσβαση στα τελευταία γεγονότα που αναφέρθηκαν από το Bitdefender.
σαρώσετε τα αρχεία ή τους φακέλους μέσω μεταφοράς και απόθεσης ενός ή πολλών αντικειμένων πάνω στο widget.

**Widget Ασφαλείας**

Η γενική κατάσταση της ασφάλειας του υπολογιστή σας εμφανίζεται στο κέντρο του widget. Η κατάσταση υποδεικνύεται από το χρώμα και το σχήμα του εικονιδίου που εμφανίζεται σε αυτή την περιοχή.

Τα κρίσιμα ζητήματα επηρεάζουν την ασφάλεια του συστήματός σας. Απαιτούν την άμεση προσοχή σας και πρέπει να διορθωθούν το συντομότερο δυνατόν. Κάντε κλικ στο εικονίδιο κατάστασης για να ξεκινήσετε την διόρθωση των ζητημάτων που αναφέρθηκαν.

Μη κρίσιμα ζητήματα επηρεάζουν την ασφάλεια του συστήματός σας. Θα πρέπει να τα ελέγξετε και να τα διορθώσετε όταν έχετε το χρόνο. Κάντε κλικ στο εικονίδιο κατάστασης για να ξεκινήσετε την διόρθωση των ζητημάτων που αναφέρθηκαν.

Το σύστημά σας είναι προστατευμένο.

Όταν μια on-demand εργασία σάρωσης βρίσκεται σε εξέλιξη, εμφανίζεται αυτό το κινούμενο εικονίδιο. Όταν τα ζητήματα αναφέρονται, κάντε κλικ στο εικονίδιο κατάστασης για να ξεκινήσει ο οδηγός Επίλυση Ζητημάτων.

Η κάτω πλευρά του οδηγού εμφανίζει το μετρητή μη αναγνωσμένων γεγονότων (ο αριθμός των εκκρεμών συμβάντων που αναφέρθηκαν από το Bitdefender, εάν υπάρχουν). Κάντε κλικ στο μετρητή γεγονότων, για παράδειγμα για ένα μη αναγνωσμένο γεγονός, για να ανοίξετε το παράθυρο Γεγονότα. Για περισσότερες πληροφορίες, παρακολούθησε αναφερθείτε στο “Ειδοποιήσεις” (p. 16).
Σάρωση αρχείων και φακέλων

Μπορείτε να χρησιμοποιήσετε τον Οδηγό Ασφαλείας για να σαρώσετε γρήγορα τα αρχεία και τους φακέλους. Σύρετε οποιοδήποτε αρχείο ή το φάκελο που θέλετε να σαρωθεί και αφήστε το στον Οδηγό Ασφαλείας.

Ο Antivirus Scan wizard θα εμφανιστεί και θα σας καθοδηγήσει στη διαδικασία σάρωσης. Οι επιλογές σάρωσης είναι ρυθμισμένος εκ των προτέρων για τα καλύτερα αποτελέσματα ανίχνευσης και δεν μπορούν να αλλάξουν. Εάν εντοπιστούν προσβεβλημένα αρχεία, το Bitdefender θα προσπαθήσει να τα απολυμάνει (να αφαιρέσει τον κώδικα του κακόβουλου λογισμικού). Εάν η απολύμανση αποτύχει, ο Antivirus Scan wizard θα σας επιτρέψει να καθορίσετε άλλες ενέργειες που πρέπει να ληφθούν για τα προσβεβλημένα αρχεία.

Απόκρυψη / εμφάνιση Widget Ασφαλείας

Όταν δεν επιθυμείτε πλέον να δείτε το widget, κάντε κλικ στο ☒.

Για να επαναφέρετε το Widget Ασφαλείας, χρησιμοποιήστε μία από τις ακόλουθες μεθόδους:

- Από την περιοχή ειδοποιήσεων:
  1. Κάντε δεξί κλικ στο εικονίδιο του Bitdefender στην περιοχή ειδοποιήσεων.
  2. Κάντε κλικ στο Εμφάνιση Widget Ασφαλείας στο αναδυόμενο μενού που εμφανίζεται.

- Από το περιβάλλον του Bitdefender:
  1. Κάντε κλικ στο εικονίδιο ☐ στην αριστερή μπάρα του Bitdefender interface.
  2. Επιλέξτε την καρτέλα Γενικά.
  3. Ενεργοποιήστε την Εμφάνιση Widget Ασφαλείας κάνοντας κλικ στον αντίστοιχο διακόπτη.

Το Bitdefender Security Widget είναι απενεργοποιημένο ως προεπιλογή.

Δραστηριότητα

Το παράθυρο Δραστηριότητα εμφανίζει πληροφορίες σχετικά με τις δράσεις που έχουν γίνει από το Bitdefender στη συσκευή σας τις τελευταίες
30 ημέρες. Εδώ μπορείτε να ελέγξετε ποιες εφαρμογές, απειλές και επιθέσεις μπλοκαρίστηκαν κατά τη διάρκεια αυτής της περιόδου, και αν τυχόν έγιναν προσπάθειες από ransomware.

Επιπλέον, μπορείτε να αποκτήσετε πρόσβαση στο Bitdefender Central δραστηριότητα πατώντας τον αντίστοιχο σύνδεσμο.

Η έκθεση ασφαλείας, η οποία παρέχει μια εβδομαδιαία κατάσταση για το προϊόν σας και διάφορες συμβουλές για τη βελτίωση της προστασίας του συστήματος, μπορεί να προσεγγιστεί πατώντας τον αντίστοιχο σύνδεσμο. Αυτές οι συμβουλές είναι σημαντικές για τη διαχείριση της συνολικής προστασίας και μπορείτε εύκολα να δείτε τις ενέργειες που μπορείτε να εφαρμόσετε στο σύστημα σας.

Η έκθεση δημιουργείται μία φορά την εβδομάδα και συνοψίζει τις σχετικές πληροφορίες σχετικά με τη δραστηριότητα του προϊόντος σας, ώστε να μπορείτε εύκολα να καταλάβετε τι συνέβη κατά τη διάρκεια αυτής της χρονικής περιόδου.

Οι πληροφορίες που παρέχονται από την Αναφορά Ασφαλείας χωρίζονται σε τρεις κατηγορίες:

- **Περιοχή Προστασία** - προβολή πληροφοριών σχετικά με την προστασία του συστήματος σας.

- **Αρχεία που σαρώθηκαν**

  Σας επιτρέπει να δείτε τα αρχεία που σαρώθηκαν από το Bitdefender αυτή την εβδομάδα. Μπορείτε να δείτε λεπτομέρειες, όπως τον αριθμό των σαρωμένων αρχείων και τον αριθμό των αρχείων που καθαρίστηκαν από Bitdefender.

  Για περισσότερες πληροφορίες σχετικά με την προστασία από αυτός, ανατρέξτε στο ???.

- **Ιστοσελίδες που σαρώθηκαν**

  Σας επιτρέπει να ελέγχετε σκληρά την προστασία των συνεδριάδων σας και μπλοκαρίστηκαν από το Bitdefender. Για να σας προστατεύσει από την αποκάλυψη προσωπικών πληροφοριών κατά την περίπτωση, το Bitdefender φροντίζει για την ασφαλή διαδικτυακή κυκλοφορία σας.

  Για περισσότερες πληροφορίες σχετικά με την προστασία Web, παρακαλούμε ανατρέξτε στο ???.

- **Τρωτά σημεία**

  Έναρξη
Σας δίνει τη δυνατότητα εύκολου εντοπισμού και διόρθωσης και των τρωτών σημείων του συστήματος, ώστε να κάνετε τον υπολογιστή σας πιο ασφαλή από κακόβουλο λογισμικό και hackers.

Για περισσότερες πληροφορίες σχετικά με την Σάρωση για Ευπάθειες, παρακαλούμε ανατρέξτε στο ???.

● Χρονολόγιο Συμβάντων

Σας επιτρέπει να έχετε μια συνολική εικόνα όλων των διαδικασιών σάρωσης και θεμάτων που διευθετούνται από το Bitdefender καθ’ όλη τη διάρκεια της εβδομάδας. Τα γεγονότα χωρίζονται κατά ημέρες.

Για περισσότερες πληροφορίες σχετικά με ένα λεπτομερές αρχείο καταγραφής των γεγονότων που αφορούν τις δραστηριότητες στον υπολογιστή σας, δείτε στο ???.

● Περιοχή ιδιωτικότητα (privacy)-προβολή πληροφοριών σχετικά με την μυστικότητα του συστήματός σας.

● Αρχεία στο θησαυροφυλάκιο (Vault)

Σας επιτρέπει να δείτε πόσα αρχεία είναι ασφαλισμένα έναντι ανεπιθύμητης πρόσβασης.

Για περισσότερες πληροφορίες σχετικά με το πώς να δημιουργήσετε κρυπτογραφημένες, προστατευόμενες με κωδικό λογικές μονάδες δίσκου (ή θησαυροφυλάκια) στον υπολογιστή σας, ανατρέξτε στο “Κρυπτογράφηση Αρχείου” (p. 158).

● Optimization περιοχή - προβολή πληροφοριών που σχετίζονται με το χώρο που εκκαθαρίστηκε, τη βελτιστοποίηση εφαρμογών και πόση μπαταρία του υπολογιστή σας σώσατε χρησιμοποιώντας τη λειτουργία μπαταρίας.

● Χώρος που καθαρίστηκε

Σας επιτρέπει να δείτε πόσος χώρος εκκαθαρίστηκε κατά τη διαδικασία βελτιστοποίησης του συστήματος. Το Bitdefender χρησιμοποιεί το Tune-Up για να συμβάλει στη βελτίωση της ταχύτητας του συστήματός σας.

Για περισσότερες πληροφορίες σχετικά με το Tune-Up, παρακαλούμε ανατρέξτε στο “Εργαλεία” (p. 197).

● Μπαταρία χρησιμοποιήθηκε
Σας επιτρέπει να δείτε πόση μπαταρία γλυτώσατε, ενώ το σύστημα έτρεχε σε λειτουργία μπαταρίας.

Για περισσότερες πληροφορίες σχετικά με τη λειτουργία Μπαταρίας, παρακαλούμε ανατρέξτε στο “Προφίλ Battery Mode” (p. 207).

**Βελτιστοποιημένες Εφαρμογές**

Σας επιτρέπει να δείτε τον αριθμό των εφαρμογών που έχουν χρησιμοποιηθεί στο πλαίσιο των προφίλ.

Για περισσότερες πληροφορίες σχετικά με τα Προφίλ, παρακαλούμε ανατρέξτε στο “Προφίλ” (p. 201).

**Ελέγχοντας την αναφορά ασφαλείας**

Η Αναφορά Ασφαλείας χρησιμοποιεί ένα σύστημα παρακολούθησης για να ανιχνεύει και να σας ενημερώνει σχετικά με τα ζητήματα που ενδέχεται να επηρεάσουν την ασφάλεια του υπολογιστή 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. Αξιοποιώντας την Αναφορά μπορείτε να ρυθμίσετε συγκεκριμένα στοιχεία του Bitdefender ή να λάβετε προληπτικά μέτρα για να προστατεύσετε τον υπολογιστή σας και τα προσωπικά σας δεδομένα.

**Ελέγχοντας την αναφορά ασφαλείας:**

1. Δείτε την αναφορά:

   ● Κάντε κλικ στο εικονίδιο επάνω στην αριστερή μπάρα του Bitdefender interface.

   Κάντε κλικ στο Security Report σύνδεσμο που βρίσκεται στην κάτω δεξιά γωνία του παραθύρου έκθεσης δραστηριοτήτων.

   ● Κάντε δεξιό κλικ στο εικονίδιο του Bitdefender στην περιοχή ειδοποιήσεων και επιλέξτε Εμφάνιση στατιστικών ασφαλείας.

   ● Μόλις η αναφορά είναι πλήρης, θα λάβετε μία αναδυόμενη ενημέρωση. Κάντε κλικ στο Show για να αποκτήσετε πρόσβαση στην αναφορά ασφαλείας.

   Θα δείτε την αναφορά που δημιουργήθηκε σε μία ιστοσελίδα που θα ανοίξει στο πρόγραμμα περιήγησης σας.
2. Ρίξτε μια ματιά στην κορυφή του παραθύρου για να δείτε την συνολική κατάσταση της ασφάλειας.

3. Ελέγξτε τις συστάσεις μας στο κάτω μέρος της σελίδας.

Το χρώμα στην περιοχή κατάστασης της ασφάλειας αλλάζει ανάλογα με τα ζητήματα που έχουν εντοπιστεί και εμφανίζονται διαφορετικά μηνύματα:

- **Η περιοχή είναι πράσινου χρώματος.** Δεν υπάρχουν θέματα για την επιδιόρθωση. Ο υπολογιστής και τα δεδομένα σας είναι προστατευμένα.

- **Η περιοχή έχει πορτοκαλί χρώμα.** Υπάρχουν Μη κρίσιμα ζητήματα που επηρεάζουν την ασφάλεια του συστήματός σας. Θα πρέπει να τα ελέγξετε και να τα διορθώσετε όταν έχετε το χρόνο.

- **Η περιοχή έχει κόκκινο χρώμα.** Υπάρχουν κρίσιμα ζητήματα που επηρεάζουν την ασφάλεια του συστήματός σας. Θα πρέπει να αντιμετωπίσετε άμεσα αυτά τα ζητήματα.

**Ενεργοποίηση ή απενεργοποίηση της ειδοποίησης Αναφοράς Ασφαλείας**

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

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

**2.3. 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 στο Bitdefender λογαριασμό από οποιονδήποτε υπολογιστή ή κινητή συσκευή που συνδέεται στο Internet μεταβαίνοντας στο https://central.bitdefender.com. 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 & Antivirus 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.
• Προστατεύστε τις συσκευές δικτύου και τα δεδομένα τους από κλοπή ή απώλεια με το Anti-Theft.
• Διαμορφώστε τις ρυθμίσεις του ΓΟΝΙΚΟΥ ΕΛΕΓΧΟΥ για τις συσκευές των παιδιών σας για να ελέγχετε τη δραστηριότητά τους από όπου κι αν βρίσκεστε.
• Επιλέξτε την Δραστηριότητα για να δείτε την κατάσταση της συνδρομής σας καθώς και τις ενεργοποιημένες στο δίκτυό σας συσκευές, και, όπου είναι εφικτό, μπορείτε να βελτιώσετε απομακρυσμένα την απόδοση των windows συσκευών σας.

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:
  1. Κάντε κλικ στο εικονίδιο ☑ στην αριστερή μπάρα του Bitdefender interface.
  2. Επιλέξτε τον σύνδεσμο Go to Bitdefender Central.
  3. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
• Από τον πληγό σας:
1. Ανοίξτε ένα πρόγραμμα περιήγησης σε οποιαδήποτε συσκευή με πρόσβαση στο Διαδίκτυο.


3. Συνδεθείτε στο Bitdefender λογαρισμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.

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 τις διαθέσιμες συσκευές 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.
3. Στο παράθυρο MY DEVICES κάντε κλικ στο INSTALL Bitdefender.
4. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:
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 RENEW 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. Επιλέξτε ΚΩΔΙΚΟΣ ΕΝΕΡΓΟΠΟΙΗΣΗΣ για να συνεχίσετε.

Η συνδρομή ενεργοποιήθηκε. Πηγαίνετε στο πάνελ Οι συσκευές μου και επιλέξτε ΕΓΚΑΤΑΣΤΑΣΗ Bitdefender για να εγκαταστήσετε το προϊόν σε μια από τις συσκευές σας.

Oι συσκευές μου

Η περιοχή My Devices 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 της συσκευής σας εμφανίζουν το όνομα της συσκευής, το καθεστώς προστασίας και το υπόλοιπο διαθέσιμότητας της συνδρομής 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. Κάντε κλικ στο εικονίδιο στην κάρτα της συσκευής που επιθυμείτε, στη συνέχεια, επιλέξτε Ρυθμίσεις.
4. Αλλάξτε το όνομα της συσκευής στο αντίστοιχο πεδίο, στη συνέχεια, επιλέξτε Αποθήκευση.

Σε περίπτωση που το Autopilot είναι απενεργοποιημένο, μπορείτε να το ενεργοποιήσετε πατώντας το διακόπτη. Κάντε κλικ στο Αποθήκευση για να εφαρμόσετε τις ρυθμίσεις.

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. Κάντε κλικ στο εικονίδιο στην κάρτα της συσκευής που επιθυμείτε, στη συνέχεια, επιλέξτε Προφίλ.
4. Κάντε κλικ στο κουμπί Προσθήκη κατόχου, συμπληρώστε τα αντίστοιχα πεδία, συμπλήρωσαν την ημερομηνία γέννησης και προσθέστε ακόμη και μια εικόνα προφίλ.

5. Κάντε κλικ στο ΠΡΟΣΘΗΚΗ για να αποθηκεύσετε ένα προφίλ.

6. Επιλέξτε τον επιθυμητό ιδιοκτήτη από τη λίστα Ιδιοκτήτης συσκευής και στη συνέχεια κάντε κλικ στο ΑΝΤΙΣΤΟΙΧΙΣΗ.

Για να ενημερώσετε εξ αποστάσεως το Bitdefender σε μια συσκευή:

1. Πρόσβαση στο Bitdefender Central.

2. Επιλέξτε το Οι συσκευές μου.

3. Κάντε κλικ στο εικονίδιο στην κάρτα της συσκευής που επιθυμείτε, στη συνέχεια, επιλέξτε Ενημέρωση.

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 ελέγξετε την κατάσταση της προστασίας των προϊόντων Bitdefender και τον αριθμό των ημερών που απομένουν για τη συνδρομή σας. Το καθεστώς προστασίας μπορεί να είναι πράσινο, όταν δεν υπάρχει κανένα πρόβλημα που να επηρεάζει το προϊόν σας, ή κόκκινο όταν η συσκευή βρίσκεται σε κίνδυνο. Όταν υπάρχουν προβλήματα που επηρεάζουν το προϊόν σας, κάντε κλικ στην επιλογή Προβολή προβλημάτων 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” (p. 106) και στο “Εκτέλεση γρήγορης σάρωσης” (p. 105).
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 ΠΕΡΙΣΣΟΤΕΡΑ για να λάβετε σε μια λεπτομερή έκθεση σχετικά με τα θέματα που βρέθηκαν και διορθώθηκαν.

Επιπλέον, μπορείτε να βελτιώσετε την εκκίνηση της συσκευής σας, εντοπίζοντας τις εφαρμογές που είναι υπεύθυνες για υψηλή κατανάλωση των πόρων του συστήματος. Κάντε κλικ στο κουμπί ΠΕΡΙΣΣΟΤΕΡΑ, και στη συνέχεια επιλέξτε τι θέλετε να κάνετε με τις ανιχνευμένες εφαρμογές. Α περισσότερες λεπτομέρειες σχετικά με αυτό το χαρακτηριστικό, ανατρέξτε στο “Έναρξη της εκκίνησης του συστήματός σας με ένα μόνο κλικ” (p. 197).

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 αυτό το χαρακτηριστικό, ανατρέξτε στο "Κατά της κλοπής συσκευής (Anti-Theft)" (p. 193).

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 αυτό το χαρακτηριστικό, ανατρέξτε στο “ΕΥΠΑΘΕΙΑ” (p. 143).

Δραστηριότητα

Η περιοχή δραστηριότητας στο Bitdefender Central είναι διαθέσιμη μόνο στους χρήστες που έχουν το Bitdefender Family Pack 2018 ή το Bitdefender Total Security 2018 για συνδρομή που σχετίζεται με τους λογαριασμούς τους. Ο ρόλος του είναι να αναφέρει πώς το Bitdefender προστάτεψε τις
συσκευές που είναι εγκατεστημένοι κατά τις τελευταίες επτά ημέρες, και να δείξει πληροφορίες σχετικά με τις περιλαμβάνει η συνδρομή.

Μόλις κάνετε πρόσβαση στο παράθυρο ΔΡΑΣΤΗΡΙΟΤΗΤΑ, οι ακόλουθες κάρτες είναι διαθέσιμες:

● ΠΡΟΣΤΑΣΙΑ. Εδώ μπορείτε να δείτε πληροφορίες σχετικά με τα αρχεία, εφαρμογές, και τις διευθύνσεις URL που έχουν αποκλειστεί λόγω ύποπτης συμπεριφοράς τους. Για να σας δείξει όταν έχουν συμβεί θέματα, διαγράμματα εμφανίζουν τα δεδομένα που συλλέγονται χωρίζονται σε ημέρες και ο αριθμός των ανιχνευμένων απειλών είναι διαθέσιμος. Επιπλέον, μπορείτε να μετακινήσετε το ποντίκι πάνω από τα δεδομένα που εμφανίζονται για να μάθετε τον αριθμό των εντοπισμένων απειλών.

Στο κάτω μέρος της κάρτας, μπορείτε να παρατηρήσετε το όνομα της συσκευής με το μεγαλύτερο αριθμό των απειλών.

● Tune Up. Από εδώ μπορείτε να βελτιστοποιήσετε την απόδοση των συσκευών Windows όπου έχετε εγκαταστήσει το Bitdefender Total Security προϊόν. Οι πληροφορίες που εμφανίζονται βασίζονται στην Bitdefender ενότητα Startup Optimizer που δείχνει ποιες εφαρμογές τρέχουν κατά την εκκίνηση του συστήματος και σας επιτρέπει να διαχειριστείτε τη συμπεριφορά τους σε αυτό το βήμα. Ανάλογα με τις αποφάσεις που ελήφθησαν από την κοινότητα με την εφαρμογή της εντολής Καθυστέρηση, μόνο οι τρεις πρώτες συσκευές εμφανίζονται. Κάντε κλικ στο Εφαρμογή για να γίνουν οι προτεινόμενες αλλαγές στην επιλεγμένη συσκευή.

Kάντε κλικ στο το σύνδεσμο που δείχνει τον αριθμό των ανιχνευμένων εφαρμογών και εξοικονόμηση χρόνου για να δείτε τις αποφάσεις άλλων Bitdefender χρηστών. Εμφανίζονται λεπτομέρειες σχετικά με τον χρόνο που χρειάζεται για την εκκίνηση του συστήματος σας, ο χρόνος που χρειάζονται οι εφαρμογές κατά την εκκίνηση και ο βελτιστοποιημένος χρόνος. Επιλέξτε ΚΑΘΥΣΤΕΡΗΣΕ ΟΛΕΣ αν θέλετε να τα σταματήσετε από το να εκτελούνται κατά την εκκίνηση. Για περισσότερες πληροφορίες σχετικά με την ενότητα Bitdefender Startup Optimizer παρακαλώ ανατρέξτε στο “Βελτιστοποίηση του χρόνου εκκίνησης του PC σας” (p. 198).

Σημείωση
Εάν δεν έχει εγκατασταθεί η προστασία Bitdefender στις συσκευές των Windows, η Tune Up κάρτα δεν θα περιέχει καμία πληροφορία.
Συνδρομή. Εδώ μπορείτε να δείτε πόσες συσκευές καλύπτει τη συνδρομή σας και σε πόσες συσκευές που έχετε εγκαταστήσει την Bitdefender προστασία. Για να εγκαταστήσετε το Bitdefender σε άλλες συσκευές, κάντε κλικ στο κουμπί ΕΓΚΑΤΑΣΤΑΣΗ κάτω από το λειτουργικό σύστημα που θέλετε και ακολουθήστε τα βήματα που απαιτούνται.

Το όνομα της συνδρομής σε χρήση εμφανίζεται μαζί με μια χρωματιστή κουκίδα:

- Μώβ - η συνδρομή σας είναι ενεργή.
- Κόκκινο - συνδρομή σας πρόκειται να λήξει. Σας συνιστούμε να ανανεώσετε το συντομότερο δυνατό για να συνεχίσει η προστασία της συσκευές σας.

Κάντε κλικ στο σύνδεσμο Περισσότερες λεπτομέρειες για να κατευθυνθείτε στην σελίδα Συνδρομές όπου μπορείτε να δείτε λεπτομερείς πληροφορίες σχετικά με την ενεργή συνδρομή σας.

Ο λογαριασμός μου

Στην οθόνη Ο λογαριασμός μου μπορείτε να προσωποποιήσετε το προφίλ σας, να αλλάξετε τον κωδικό του λογαριασμού σας και να χειριστείτε τις συνεδρίες σύνδεσης και τα μηνύματα βοήθεια του Bitdefender Central.

Μόλις επιλέξετε το Εικονίδιο στο επάνω δεξιό μέρος της οθόνης και επιλέξτε Ο λογαριασμός μου, έχετε τις ακόλουθες καρτέλες:

- Προφίλ - εδώ μπορείτε να προσθέσετε ή να αλλάξετε πληροφορίες σχετικά με τον λογαριασμό σας.
- Αλλαγή κωδικού - εδώ μπορείτε να αλλάξετε τον κωδικό του λογαριασμού σας.
- Συνεδρίες σύνδεσης - εδώ μπορείτε να δείτε και να χειριστείτε τις πιο πρόσφατες μη ενεργές ή ενεργές συνεδρίες σύνδεσης που σχετίζονται με τις ενεργοποιημένες συσκευές σας.
- Ρυθμίσεις - εδώ μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε τα μηνύματα βοήθεια του Bitdefender Central καθώς και να αποφασίσετε αν θα θέλατε ή όχι να ενημερώνεστε όταν λαμβάνονται snap φωτογραφίες από τις συσκευές σας.
Ειδοποιήσεις

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

2.4. Διατηρώντας το Bitdefender ενημερωμένο με τις πιο πρόσφατες ενημερώσεις

Νέο κακόβουλο λογισμικό ανιχνεύεται και προσδιορίζεται κάθε μέρα. Γι’αυτό είναι πολύ σημαντικό να διατηρήσουμε το Bitdefender ενημερωμένο με τις τελευταίες υπογραφές κακόβουλου λογισμικού (malware).

Αν είστε συνδεδεμένοι στο Internet μέσω ευρυζωνικής ή DSL σύνδεσης, το Bitdefender φροντίζει το ίδιο τον εαυτό του. Από προεπιλογή, το προϊόν ελέγχει για ενημερώσεις όταν ανοίγετε τον υπολογιστή σας και κάθε μία ώρα μετά από αυτό. Αν εντοπιστεί μια ενημερωμένη έκδοση, μεταφορτώνεται και εγκαθίσταται αυτόματα στον υπολογιστή 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 προστατεύσετε 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 ο υπολογιστής σας συνδέεται στο Internet μέσω ενός διακομιστή μεσολάβησης (Proxy server), πρέπει να διαμορφώσετε τις ρυθμίσεις proxy, όπως περιγράφεται στο “Πώς να ρυθμίσω το Bitdefender να χρησιμοποιήσει μια σύνδεση διακομιστή μεσολάβησης (proxy) του Internet;” (p. 90).

● Κατά τη λήψη ενημερώσεων σε μια αργή σύνδεση στο Internet ενδέχεται να συμβούν σφάλματα λήψης. Για την αντιμετώπιση τέτοιων σφαλμάτων, παρακαλούμε ανατρέξτε στο “Πώς να ενημερώσετε το Bitdefender σε μια αργή σύνδεση στο Internet” (p. 222)
Αν είστε συνδεδεμένοι στο Internet μέσω μιας dial up σύνδεσης, τότε συνιστάται να ενημερώνετε τακτικά το Bitdefender με αίτημα του χρήστη. Για περισσότερες πληροφορίες παρακολούθησε αναφερθείτε στο “Εκτελώντας ενημέρωση” (p. 49).

Έλεγχος αν το Bitdefender είναι επικαιροποιημένο με τις τελευταίες ενημερώσεις

Για να ελέγξετε την ώρα της τελευταίας ενημέρωσης του Bitdefender, ελέγξτε το Security Status, στην αριστερή πλευρά της περιοχής κατάστασης.

Για λεπτομερείς πληροφορίες σχετικά με τις τελευταίες ενημερώσεις, ελέγξτε τα συμβάντα ενημέρωσης:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα 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 δυνατό συντομότερα.

Εκτελώντας ενημέρωση

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

Για να ξεκινήσετε μια ενημέρωση, κάντε ένα από τα παρακάτω:

● Ανοίξτε το Bitdefender interface και κάντε κλικ στον σύνδεσμο UPDATE NOW που βρίσκεται κάτω από το status του προγράμματος σας.
● Κάντε δεξί κλικ στο Bitdefender εικονίδιο στην περιοχή ειδοποίησεων και επιλέξτε Αναβάθμιση τώρα.

Η λειτουργία "Ενημέρωση" θα συνδέθει 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
Μπορεί να χρειαστεί να κάνετε επανεκκίνηση του υπολογιστή, όταν έχετε ολοκληρώσει 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 εξ αποστάσεως το Bitdefender σε μια συσκευή:
1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το Οι συσκευές μου.
3. Κάντε κλικ στο εικονίδιο στην κάρτα της συσκευής που επιθυμείτε, στη συνέχεια, επιλέξτε Ενημέρωση.

Ενεργοποίηση ή απενεργοποίηση αυτόματης ενημέρωσης
Για να ενεργοποιήσετε ή απενεργοποιήσετε την αυτόματη ενημέρωση:
1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Ενημέρωση.
3. Κάντε κλικ στους αντίστοιχους διακόπτες ΌN/OFF.
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 μία ώρα, μόνιμα ή μέχρι μια 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.
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. Κάντε κλικ στο εικονίδιο Ενημέρωση στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Ενημέρωση 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.

Ενημέρωση τοποθεσίας

Το Bitdefender έχει ρυθμιστεί για την ενημέρωση από τους διακομιστές ενημέρωσης της Bitdefender στο Διαδίκτυο. Η τοποθεσία ενημέρωσης είναι μια γενική διεύθυνση στο Internet που ανακατευθύνεται αυτόματα στον πλησιέστερο στην περιοχή σας διακομιστή ενημέρωσης της Bitdefender.

Μην αλλάζετε τη θέση λήψης ενημερωμένων εκδόσεων, εκτός αν συνιστάται από εκπρόσωπο της Bitdefender ή του διαχειριστή του δικτύου σας (αν είστε συνδεδεμένοι σε ένα δίκτυο γραφείου).

Μπορείτε να επιστρέψετε στη γενικευμένη θέση λήψης ενημερωμένων εκδόσεων του Internet κάνοντας κλικ στο DEFAULT.
Κανόνες διαδικασίας ενημέρωσης

Μπορείτε να επιλέξετε ανάμεσα σε τρεις τρόπους για να κατεβάσετε και να εγκαταστήσετε τις ενημερωμένες εκδόσεις:

● **Ενημέρωση Silent** - Bitdefender αυτόματα λαμβάνει και υλοποιεί την ενημέρωση.
● **Ερώτηση πριν από τη λήψη** - κάθε φορά που είναι διαθέσιμη μια ενημέρωση, θα σας ζητηθεί επιβεβαίωση πριν από τη λήψη.
● **Ερώτηση πριν από την εγκατάσταση** - κάθε φορά που είναι διαθέσιμη μια ενημέρωση, θα σας ζητηθεί επιβεβαίωση πριν από την εγκατάστασή της.

Ορισμένες ενημερώσεις απαιτούν επανεκκίνηση για να ολοκληρωθεί η εγκατάσταση. Από προεπιλογή, εάν μια ενημερωμένη έκδοση απαιτεί επανεκκίνηση, το Bitdefender θα συνεχίσει να εργάζεται με τα παλιά αρχεία μέχρι ο χρήστης να κάνει επανεκκίνηση του υπολογιστή με δική του επιλογή. Η πρόνοια αυτή έχει ληφθεί για να αποφευχθεί η εμπλοκή της διαδικασίας ενημέρωσης του Bitdefender με την εργασία του χρήστη.

Αν θέλετε να ερωτηθείτε όταν μια ενημερωμένη έκδοση απαιτεί επανεκκίνηση, απενεργοποιήστε την επιλογή Αναβολή επανεκκίνησης πατώντας τον αντίστοιχο διακόπτη.

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 αυτή την ειδοποίηση, μπορείτε είτε να κάνετε κλικ στο ΕΠΑΝΕΚΚΙΝΗΣΗ ΤΩΡΑ στο παράθυρο Ειδοποιήσεις όπου αναφέρεται η πιο πρόσφατη ενημέρωση, ή να επανεκκινήσετε χειροκίνητα το σύστημα.
Σημείωση
3. ΠΩΣ ΜΠΟΡΕΙΤΕ ΝΑ

3.1. Εγκατάσταση

Πώς μπορώ να εγκαταστήσω το Bitdefender σε έναν δεύτερο υπολογιστή;

Εάν η συνδρομή που έχετε αγοράσει καλύπτει περισσότερους από έναν υπολογιστές, μπορείτε να χρησιμοποιήσετε τον Bitdefender λογαριασμό σας για να ενεργοποιήσετε έναν δεύτερο υπολογιστή.

Για να εγκαταστήσετε το Bitdefender σε έναν δεύτερο υπολογιστή:

1. Κάντε κλικ στο σύνδεσμο ΕΓΚΑΤΑΣΤΑΣΗ ΣΕ ΑΛΛΗ ΣΥΣΚΕΥΗ στην κάτω δεξιά γωνία του Bitdefender interface.
   Θα μεταφερθείτε στην ιστοσελίδα του Bitdefender λογαριασμού. Βεβαιωθείτε ότι έχετε συνδεθεί με τους κωδικούς σας.
2. Στο παράθυρο που εμφανίζεται επιλέξτε το επιθυμητό λειτουργικό σύστημα και στη κατόπιν επιλέξτε ΣΥΝΕΧΕΙΑ.
3. Πληκτρολογήστε τη διεύθυνση e-mail που θα θέλατε να λάβετε τον σύνδεσμο λήψης και εγκατάστασης της εφαρμογής για το επιλεγμένο λειτουργικό σύστημα.
4. Εκτελέστε το Bitdefender προϊόν που έχετε κατεβάσει. Περιμένετε μέχρι να ολοκληρωθεί η διαδικασία εγκατάστασης και κλείστε το παράθυρο.

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

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. Θα χρειαστεί να κάνετε επανεκκίνηση του υπολογιστή 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 εικονίδιο 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. Θα χρειαστεί να κάνετε επανεκκίνηση του υπολογιστή 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. Θα χρειαστεί να κάνετε επανεκκίνηση του υπολογιστή 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.

Από πού μπορώ να μεταφορτώσω το Bitdefender προϊόν μου;

Μπορείτε να εγκαταστήσετε το Bitdefender από το δίσκο εγκατάστασης ή χρησιμοποιώντας το πρόγραμμα εγκατάστασης που μπορείτε να κατεβάσετε στον υπολογιστή σας από το Bitdefender Central.

Σημείωση
Πριν από την εκτέλεση του κιτ εγκατάστασης, συνιστάται να αφαιρέσετε οποιαδήποτε λύση antivirus είναι εγκατεστημένη στο σύστημά σας. Όταν χρησιμοποιείτε περισσότερες από μία λύση ασφάλειας στον ίδιο υπολογιστή, το σύστημα γίνεται ασταθές.

Για να εγκαταστήσετε το Bitdefender απο το Bitdefender Central:
1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε το Οι συσκευές μου.
3. Στο παράθυρο MY DEVICES κάντε κλικ στο INSTALL Bitdefender.
4. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:
   - ΛΗΨΗ
     Κάντε κλικ στο κουμπί και αποθηκεύσετε το αρχείο εγκατάστασης.
   - Σε άλλη συσκευή
     Επιλέξτε Windows να κατεβάσετε Bitdefender προϊόν σας και, στη συνέχεια, κάντε κλικ στο κουμπί ΣΥΝΕΧΕΙΑ. Πληκτρολογήστε μια διεύθυνση e-mail στο αντίστοιχο πεδίο, και κάντε κλικ στο ΑΠΟΣΤΟΛΗ.
5. Εκτελέστε το Bitdefender προϊόν που έχετε κατεβάσει.
Πώς μπορώ να αλλάξω τη γλώσσα του Bitdefender;

Αν θέλετε να χρησιμοποιήσετε το Bitdefender σε άλλη γλώσσα, θα πρέπει να εγκαταστήσετε ξανά το προϊόν στην κατάλληλη γλώσσα.

Για να χρησιμοποιήσετε το Bitdefender σε άλλη γλώσσα:

1. Αφαιρέστε το Bitdefender ακολουθώντας τα παρακάτω βήματα:

   ● 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.

   ● Στα Windows 8 και στα Windows 8.1:
     a. Από την οθόνη Έναρξη 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 εικονίδιο 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.

   ● 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.

2. Αλλάξτε τη γλώσσα του Bitdefender Central:

   a. Πρόσβαση στο Bitdefender Central.
   b. Κάντε κλικ στο εικονίδιο στην επάνω δεξιά πλευρά της οθόνης.
   c. Κάντε κλικ στο o λογαριασμός μου στο μενού.
   d. Επιλέξτε την καρτέλα Profile.
   e. Επιλέξτε μια γλώσσα από το αναπτυσσόμενο πλαίσιο λίστας Language και, στη συνέχεια, κάντε κλικ στην επιλογή SAVE.

3. Κατεβάστε το αρχείο εγκατάστασης:

   a. Επιλέξτε το Οι συσκευές μου.
   b. Στο παράθυρο MY DEVICES κάντε κλικ στο INSTALL Bitdefender.
   c. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:

      ● ΛΗΨΗ
      Κάντε κλικ στο κουμπί και αποθηκεύσετε το αρχείο εγκατάστασης.

      ● Σε άλλη συσκευή
      Επιλέξτε Windows να κατεβάσετε Bitdefender προϊόν σας και, στη συνέχεια, κάντε κλικ στο Καταβάστε Bitdefender συσκευή σας και ΣΥΝΕΧΕΙΑ. Πληκτρολογήστε μια διεύθυνση e-mail στο αντίστοιχο πεδίο, και κάντε κλικ στο ΑΠΟΣΤΟΛΗ.

4. Εκτελέστε το Bitdefender προϊόν που έχετε κατεβάσει.

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

Πως μπορείτε να
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 προϊόν 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 εικονίδιο 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, 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 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.
   c. Στο παράθυρο MY DEVICES κάντε κλικ στο INSTALL Bitdefender.
   d. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:
      - ΛΗΨΗ
        Κάντε κλικ στο κουμπί και αποθηκεύσετε το αρχείο εγκατάστασης.
      - Σε άλλη συσκευή
        Επιλέξτε Windows να κατεβάσετε Bitdefender προϊόν σας και, στη συνέχεια, κάντε κλικ στο κουμπί ΣΥΝΕΧΕΙΑ. Πληκτρολογήστε μια διεύθυνση e-mail στο αντίστοιχο πεδίο, και κάντε κλικ στο ΑΠΟΣΤΟΛΗ.

2. Εκτελέστε το Bitdefender προϊόν που έχετε κατεβάσει.

Για περισσότερες πληροφορίες σχετικά με τη διαδικασία εγκατάστασης του Bitdefender, ανατρέξτε στο “Εγκατάσταση του Bitdefender προϊόντος σας” (p. 4).

Πώς μπορώ να αναβαθμίσω στην πιο πρόσφατη Bitdefender έκδοση:

Έκκινώντας με το Bitdefender 2018, 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 2017, 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 και, στη συνέχεια, κάντε κλικ στο κουμπί ΕΠΑΝΕΚΙΝΗΣΗ ΤΩΡΑ. Περιμένετε να γίνει επανεκκίνηση του υπολογιστή.

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.


3.2. Συνδρομές

Πώς μπορώ να ενεργοποιήσω τη Bitdefender συνδρομή μου χρησιμοποιώντας μια άδεια χρήσης;

Εάν έχετε μία έγκυρη άδεια και θέλετε να τη χρησιμοποιήσετε για να ενεργοποιήσετε μια συνδρομή για το Bitdefender Total Security, υπάρχουν δύο πιθανές περιπτώσεις:

● Έχετε κάνει αναβάθμιση από προηγούμενη έκδοση Bitdefender σε νέα:

1. Μόλις η αναβάθμιση σε Bitdefender Total Security ολοκληρωθεί, θα σας ζητηθεί να συνδεθείτε στο Bitdefender λογαριασμό σας.
2. Κάντε κλικ στο **Sign In**, και στη συνέχεια πληκτρολογήστε το e-mail και το password του Bitdefender λογαρισμού.

3. Κάντε κλικ στο **SIGN IN** για να συνεχίσετε.

4. Μια ειδοποίηση που σας ενημερώνει ότι δημιουργήθηκε μια συνδρομή εμφανίζεται στην οθόνη του λογαριασμού σας. Η συνδρομή που δημιουργήθηκε θα ισχύει για τις υπόλοιπες ημέρες της άδειας σας και για τον ίδιο αριθμό των χρηστών.

Οι συσκευές που χρησιμοποιούν προηγούμενες Bitdefender εκδόσεις και έχουν καταχωρηθεί με την άδεια που μετατρέψατε σε συνδρομή πρέπει να καταχωρήσουν στο ίδιο Bitdefender λογαρισμό.

- Το Bitdefender δεν είχε εγκατασταθεί παλαιότερα στο σύστημα:
  1. Μόλις ολοκληρωθεί η διαδικασία εγκατάστασης, θα σας ζητηθεί να συνδεθείτε στο Bitdefender λογαριασμό σας.
  2. Κάντε κλικ στο **Sign In**, και στη συνέχεια πληκτρολογήστε το e-mail και το password του Bitdefender λογαρισμού.
  3. Κάντε κλικ στο **SIGN IN** για να συνεχίσετε και κάντε κλικ στο κουμπί **FINISH** για να αποκτήσετε πρόσβαση στο Bitdefender Total Security interface.

4. Κάντε κλικ στο εικονίδιο ☀ στην αριστερή μπάρα του Bitdefender interface.
5. Επιλέξτε τον σύνδεσμο Κωδικός Ενεργοποίησης.

- Εμφανίζεται ένα νέο παράθυρο.
6. Κάντε κλικ στον σύνδεσμο **Get your FREE upgrade now!**.
7. Πληκτρολογήστε τον κωδικό άδειας χρήσης σας στο αντίστοιχο πεδίο και κάντε κλικ στο κουμπί **UPGRADE MY PRODUCT**. Μια συνδρομή με την ίδια διάθεση και αριθμό των χρηστών του κωδικού άδειας χρήσης σας συσχετίζεται με το λογαριασμό σας.

### 3.3. Bitdefender Central

Πώς μπορώ να συνδεθώ στο Bitdefender Central χρησιμοποιώντας έναν άλλο online λογαριασμό;

Έχετε δημιουργήσει ένα νέο Bitdefender λογαριασμό και θέλετε να το χρησιμοποιείτε από τώρα και στο εξής.
Για να χρησιμοποιήσετε με επιτυχία έναν άλλο λογαριασμό:

1. Κάντε κλικ στο εικονίδιο  στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο κουμπί SWITCH ACCOUNT για να αλλάξετε το λογαριασμό που συνδέεται με τον υπολογιστή.
3. Πληκτρολογήστε τη διεύθυνση e-mail και τον κωδικό πρόσβασης του λογαριασμού σας στα αντίστοιχα πεδία 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. 327).

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. Επιλέξτε την καρτέλα Settings.
5. Απενεργοποιήστε την επιλογή Turn on/off help messages.

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 στο εικονίδιο στην επάνω δεξιά πλευρά 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**.

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

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

- **Από τη διεπαφή Bitdefender:**
  1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
  2. Κάντε κλικ στο κουμπί **SWITCH ACCOUNT**. Εμφανίζεται ένα νέο παράθυρο.
  3. Κάντε κλικ στο σύνδεσμο **Ξέχασα τον κωδικό πρόσβασης μου**.
  4. Πληκτρολογήστε τη διεύθυνση e-mail που χρησιμοποιήσατε για να δημιουργήσετε τον Bitdefender και στη συνέχεια κάντε κλικ στο **FORGOT PASSWORD** κουμπί.
  5. Ελέγξτε το email σας και κάντε κλικ στο κουμπί που παρέχεται. Ανοίγει το παράθυρο Bitdefender ΕΠΑΝΑΦΟΡΑ ΚΩΔΙΚΟΥ ΠΡΟΣΒΑΣΗΣ.
  6. Πληκτρολογήστε τη διεύθυνση ηλεκτρονικού ταχυδρομείου και τον νέο κωδικό πρόσβασης στο αντίστοιχο πεδίο. Ο κωδικός πρόσβασης πρέπει να αποτελείται από τουλάχιστον 8 χαρακτήρες και να περιλαμβάνει νούμερα.
  7. Κάντε κλικ στο κουμπί **RESET PASSWORD**.

- **Από τον πλοηγό σας:**
  2. Κάντε κλικ στο σύνδεσμο **Ξέχασα τον κωδικό πρόσβασής μου**.
  3. Πληκτρολογήστε την διεύθυνση e-mail, στη συνέχεια, κάντε κλικ στο κουμπί **ΔΕΝ ΘΥΜΑΜΑΙ ΤΟΝ ΚΩΔΙΚΟ**.
4. 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.

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

Στον Bitdefender λογαριασμό 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 λογαριασμό στο μενού.
4. Επιλέξτε την καρτέλα Χειρισμός συνεδριών.
5. Στην περιοχή Ενεργές συνδέσεις, επιλέξτε ΑΠΟΣΥΝΔΕΣΗ στην επιλογή δίπλα στη συσκευή που θέλετε να τερματίσετε την σύνδεση.

3.4. Έλεγχος με το Bitdefender

Πώς μπορώ να ελέγξω ένα αρχείο ή ένα φάκελο;

Ο ευκολότερος τρόπος για να ελέγξετε ένα αρχείο ή φάκελο είναι να κάνετε δεξί κλικ στο αντικείμενο που θέλετε να ελέγξετε , να δείξετε 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.

Έλεγχος ενός κοινόχρηστου στοιχείου δικτύου πριν από την αντιγραφή αρχείων στον υπολογιστή σας.

Πώς μπορώ να ελέγξω το σύστημά μου;

Για να εκτελέσετε μια πλήρη σάρωση του συστήματος:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα Antivirus επιλέξτε Σάρωση Συστήματος.
4. Ακολουθείτε 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 παρακολούθηστε τον Οδηγό σαρωτή Antivirus "(p. 110).

Πώς μπορώ να προγραμματίσω μια σάρωση;

Μπορείτε να ρυθμίσετε το Bitdefender προϊόν σας να ξεκινήσει τη σάρωση από σημαντικές τοποθεσίες του συστήματος, όταν δεν είστε μπροστά στον υπολογιστή.

Για να προγραμματίσετε μια σάρωση:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα Antivirus επιλέξτε Διαχείριση σαρώσεων.
4. Επιλέξτε τον τύπο σάρωσης που θέλετε να προγραμματίσετε. Σάρωση συστήματος ή Γρήγορη Σάρωση, και στη συνέχεια επιλέξτε Επιλογές Σάρωσης.
Εναλλακτικά, μπορείτε να δημιουργήσετε έναν τύπο σάρωσης που θα ταιριάζει στις ανάγκες σας, κάνοντας κλικ στο Νέα προσαρμοσμένη εργασία.

5. Ενεργοποιήστε το διακόπτη Προγραμματισμός.

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

- Κατά την εκκίνηση του συστήματος
- Μία φορά
- Περιοδικά

Στο παράθυρο Στόχοι Σάρωσης μπορείτε να επιλέξετε τις θέσεις που θέλετε να σαρωθούν.

Πώς μπορώ να δημιουργήσω μία εργασία προσαρμοσμένης σάρωσης;

Αν θέλετε να σαρώσετε συγκεκριμένες θέσεις στον υπολογιστή σας ή να ρυθμίσετε τις επιλογές σάρωσης, να ρυθμίσετε και να εκτελέσετε μια προσαρμοσμένη εργασία σάρωσης.

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

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα Antivirus επιλέξτε Διαχείριση σαρώσεων.
4. Κάντε κλικ στο Νέα προσαρμοσμένη εργασία. Στην καρτέλα Βασικό εισάγετε ένα όνομα για τη σάρωση και επιλέξτε τις θέσεις που πρόκειται να σαρωθούν.
5. Αν θέλετε να ρυθμίσετε τις επιλογές σάρωσης στη λεπτομέρεια, επιλέξτε την καρτέλα για προχωρημένους.

Μπορείτε εύκολα να ρυθμίσετε τις επιλογές σάρωσης με την προσαρμογή του επιπέδου σάρωσης. Σύρετε το ρυθμιστικό κατά μήκος της κλίμακας για να ρυθμίσετε το επιθυμητό επίπεδο σάρωσης.
Μπορείτε επίσης να επιλέξετε να κλείσει τον υπολογιστή, όταν η σάρωση είναι ολοκληρωθεί και δεν βρέθηκαν απειλές. Να θυμάστε ότι αυτή θα είναι η προεπιλεγμένη συμπεριφορά κάθε φορά που θα εκτελέσετε αυτή την εργασία.

6. Κάντε κλικ στο OK για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

7. Χρησιμοποιείστε τον αντίστοιχο διακόπτη αν θέλετε να θέσετε ένα χρονοδιάγραμμα για την εργασία σάρωσης.

8. Κάντε κλικ στο Έναρξη Σάρωσης και ακολουθήστε τον Οδηγό Σάρωσης για να ολοκληρώσετε τη σάρωση. Στο τέλος της σάρωσης, θα σας ζητήσει να επιλέξετε τις ενέργειες που πρέπει να ληφθούν για τα εντοπισμένα αρχεία, εάν εντοπίσθηκαν κάποια μολυσμένα.

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

Πώς μπορώ να εξαιρέσω ένα φάκελο από τη σάρωση:

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

Οι εξαιρέσεις θα πρέπει να χρησιμοποιούνται από χρήστες που έχουν προσωπικές 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 το φάκελο στη λίστα Εξαιρέσεις:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο ΕΞΑΙΡΕΣΕΙΣ στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS

4. Επιλέξτε την καρτέλα ΕΞΑΙΡΕΣΕΙΣ.

5. Κάντε κλικ στο μενού Λίστα αρχείων και φακέλων που εξαιρούνται από τη σάρωση και στη συνέχεια στο κουμπί ΠΡΟΣΘΗΚΗ.

6. Κάντε κλικ στο κουμπί Αναζήτηση, επιλέξτε το φάκελο που θέλετε να αποκλείσετε από τη σάρωση και, στη συνέχεια, επιλέξτε τον τύπο σάρωσης που θα πρέπει να αποκλείεται.

7. Κάντε κλικ στο Add για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

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 Εξαίρεσεων του Bitdefender:

1. Απενεργοποιήστε την σε πραγματικό χρόνο προστασία από τους ιούς του Bitdefender:
   a. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
   b. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
   c. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS.
   d. Στο παράθυρο ΑΣΠΙΔΑ, κάντε κλικ στον διακόπτη ON/OFF.

2. 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. 92).

3. Επαναφορά αρχείου από την περιοχή Καραντίνας:
   a. Κάντε κλικ στο εικονίδιο ☐ στην αριστερή μπάρα του Bitdefender interface.
   b. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
   c. Κάντε κλικ στο εικονίδιο ☐ στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS
   d. Επιλέξτε την καρτέλα Καραντίνα.
   e. Επιλέξτε το αρχείο και κάντε κλικ στο RESTORE.

4. Προσθέστε το αρχείο στη λίστα Εξαιρέσεως. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο “Πώς μπορώ να εξαιρέσω ένα φάκελο από τη σάρωση;” (p. 69).

5. Ενεργοποιήστε την σε πραγματικό χρόνο προστασία από ιούς του Bitdefender.

6. Επικοινωνήστε με εκπροσώπους μας υποστήριξης ώστε μπορούμε να αφαιρέσουμε την υπογραφή ανίχνευσης. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο “Ζητήστε βοήθεια” (p. 327).

Πώς ελέγχω τι ιούς 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 αποτελείας 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. Κάντε κλικ στο εικονίδιο Ω στην αριστερή μπάρα του Bitdefender interface.
2. Στην καρτέλα All επιλέξτε την ειδοποίηση που αφορά την τελευταία σάρωση.

Εδώ μπορείτε να βρείτε όλα τα κακόβουλα προγράμματα εκδηλώσεων σάρωσης, συμπεριλαμβανομένων των απειλών που έντοπιστήκαν από την κατά την πρόσβαση σάρωση, σαρώσεις που ενεργοποιήθηκαν από το χρήστη και τροποποιήσεις κατάστασης για τις 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 στο VIEW LOG.

3.5. ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ

Πώς μπορώ να προστατέψω τα παιδιά μου από διαδικτυακές απειλές;

Ο Γονικός Σύμβουλος του Bitdefender σας επιτρέπει να περιορίσετε την πρόσβαση στο Διαδίκτυο και σε ειδικές εφαρμογές, αποτρέποντας τα παιδιά σας από το να βλέπουν ακατάλληλο περιεχόμενο όταν δεν είστε κοντά.

Για να ρυθμίσετε το Parental Advisor:

1. Κάντε κλικ στο εικονίδιο Ω στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο Parental Advisor κουμπί.

Θα μεταφερθείτε στην ιστοσελίδα του Bitdefender λογαριασμού. Βεβαιωθείτε ότι έχετε συνδεθεί με τους κωδικούς σας.
3. Ανοίγει το Parental Advisory ταμπλό. Από εδώ μπορείτε να ελέγξετε και να διαμορφώσετε τις ρυθμίσεις του Γονικού Συμβουλίου.
4. Κάντε κλικ στο ADD PROFILE στη δεξιά πλευρά του παραθύρου MY CHILDREN.
5. Ορίστε συγκεκριμένες πληροφορίες στα αντίστοιχα πεδία, όπως: όνομα, φύλο, και ημερομηνία γέννησης. Για να προσθέσετε φωτογραφία στο προφίλ, επιλέξτε τον σύνδεσμο ΠΡΟΣΘΗΚΗ ΑΡΧΕΙΟΥ. Κάντε κλικ στο ΕΠΟΜΕΝΟ 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. Εάν η συσκευή του παιδιού σας έχει ήδη εγκατεστημένο το Bitdefender Total Security, επιλέξτε τη συσκευή του από τη διαθέσιμη λίστα, και στη συνέχεια επιλέξτε το λογαριασμό που θέλετε να ελέγχετε. Κάντε κλικ στο SAVE.

Εάν το παιδί σας χρησιμοποιεί υπολογιστή ή κινητή συσκευή και ο Bitdefender Γονικός Έλεγχος δεν είναι εγκατεστημένος, επιλέξτε ΠΡΟΣΘΗΚΗ ΣΥΣΚΕΥΗΣ. Εάν το παιδί σας χρησιμοποιεί μια συσκευή Mac και η εφαρμογή Bitdefender Antivirus για Mac δεν είναι εγκατεστημένη, κάντε κλικ στο ίδιο κουμπί. Επιλέξτε το λειτουργικό σύστημα που θέλετε να εγκαταστήσετε την εφαρμογή και, στη συνέχεια, κάντε κλικ στο κουμπί ΕΠΟΜΕΝΟ ΒΗΜΑ για να συνεχίσετε.

7. Πληκτρολογήστε την email διεύθυνση που θα θέλατε να λάβετε τον σύνδεσμο λήψης και εγκατάστασης της εφαρμογής Bitdefender Γονικού Έλεγχου, και στη συνέχεια επιλέξτε ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΕΓΚΑΤΑΣΤΑΣΗΣ.

Ελέγξτε τις δραστηριότητες των παιδιών σας και αλλάξτε τις ρυθμίσεις Γονικού Συμβούλου με τη χρήση του Bitdefender λογαριασμού από οποιονδήποτε υπολογιστή ή κινητή συσκευή που συνδέεται στο Διαδίκτυο.

Σημαντικό

Στις συσκευές που βασίζονται στα Windows, πρέπει να λάβετε και να εγκαταστήσετε το Bitdefender Total Security που έχετε συμπεριλάβει στη συνδρομή σας. Στις macOS συσκευές, το προϊόν Bitdefender Antivirus για Mac πρέπει να κατέβει και να εγκατασταθεί. Σε συσκευές Android και iOS, θα πρέπει να κατεβάσετε και να εγκαταστήσετε τον Bitdefender Γονικό Σύμβουλο.
Πώς μπορώ να εμποδίσω την πρόσβαση του παιδιού μου σε μια ιστοσελίδα;

Ο Bitdefender Γονικός Σύμβουλος σας επιτρέπει να ελέγχετε το περιεχόμενο που είναι προσβάσιμο από το παιδί σας, ενώ χρησιμοποιεί τη συσκευή του και σας δίνει τη δυνατότητα να μπλοκάρετε την πρόσβασή σε ένα δικτυακό τόπο.

Για να αποκλείσετε την πρόσβαση σε μια ιστοσελίδα, θα πρέπει να την προσθέσετε στη λίστα Εξαιρέσεις, ως εξής:

2. Συνδεθείτε στο Bitdefender λογαρισμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Κάντε κλικ στο Γονικός Σύμβουλος για να αποκτήσετε πρόσβαση στο ταμπλό.
4. Επιλέξτε το προφίλ του παιδιού σας από το παράθυρο MY CHILDREN.
5. Επιλέξτε την καρτέλα WEBSITES.
6. Κάντε κλικ στο κουμπί ΔΙΑΧΕΙΡΙΣΗ.
7. Πληκτρολογήστε την ιστοσελίδα που θέλετε να αποκλείσετε στο αντίστοιχο πεδίο.
8. Επιλέξτε Αποδοχή ή Άρνηση.
9. Κάντε κλικ στο ΟΛΟΚΛΗΡΩΣΗ για να αποθηκεύσετε τις αλλαγές.

Σημείωση
Οι περιορισμοί μπορούν να οριστούν μόνο για συσκευές Android και Windows.

Πώς μπορώ να αποτρέψω το παιδί μου από το να παίζει ένα παιχνίδι;

Ο Γονικός Σύμβουλος του Bitdefender σας επιτρέπει να ελέγχετε το περιεχόμενο που έχει πρόσβαση το παιδί σας ενώ χρησιμοποιεί τον υπολογιστή.

Για να εμποδίσει την πρόσβαση σε ένα παιχνίδι:

2. Συνδεθείτε στο Bitdefender λογαρισμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Κάντε κλικ στο Γονικός Σύμβουλος για να αποκτήσετε πρόσβαση στο ταμπλό.
4. Επιλέξτε το προφίλ του παιδιού σας από το παράθυρο MY CHILDREN.
5. Επιλέξτε την καρτέλα ΕΦΑΡΜΟΓΕΣ.
   Μια λίστα με κάρτες εμφανίζεται. Οι κάρτες αντιπροσωπεύουν τις εφαρμογές χρησιμοποιεί το παιδί σας.
6. Επιλέξτε την κάρτα με την εφαρμογή που θέλετε το παιδί σας να σταματήσει να χρησιμοποιεί.
   Το σύμβολο που εμφανίζεται υποδεικνύει ότι το παιδί σας δεν θα είναι σε θέση να χρησιμοποιήσει την εφαρμογή.

Πώς μπορώ να αποτρέψω το παιδί μου από το να έρχεται σε επαφή με μη έμπιστα πρόσωπα:

Ο Bitdefender Γονικός Σύμβουλος σας δίνει τη δυνατότητα να εμποδίσετε τηλεφωνικές κλήσεις από άγνωστους αριθμούς τηλεφώνου ή από φίλους από τη λίστα τηλεφώνου του παιδιού σας.

Για να μπλοκάρετε μία επαφή σε μία Android συσκευή με εγκατεστημένη την εφαρμογή Bitdefender Parental Advisor:

2. Συνδεθείτε στο Bitdefender λογαρισμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Κάντε κλικ στο Γονικός Σύμβουλος για να αποκτήσετε πρόσβαση στο ταμπλό.
4. Επιλέξτε το προφίλ του παιδιού που θέλετε να ορίσετε περιορισμούς.
5. Επιλέξτε την καρτέλα Επαφές τηλεφώνου.
   Μια λίστα με κάρτες εμφανίζεται. Οι κάρτες αντιπροσωπεύουν τις επαφές από το τηλέφωνο του παιδιού σας.
6. Επιλέξτε την κάρτα με τον αριθμό τηλεφώνου που θέλετε αποκλείστε.
   Το σύμβολο που εμφανίζεται υποδεικνύει ότι το παιδί σας δεν θα είναι να λάβει τηλεφωνήματα από το συγκεκριμένο τηλεφωνικό αριθμό.
Για να αποκλείσετε μία επαφή σε μία Android συσκευή που δεν έχει εγκατεστημένη την εφαρμογή Bitdefender Parental Advisor:

2. Συνδεθείτε στο Bitdefender λογαριασμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασης σας.
3. Κάντε κλικ στο Γονικός Σύμβουλος για να αποκτήσετε πρόσβαση στο ταμπλό.
4. Επιλέξτε το προφίλ του παιδιού που θέλετε να ορίσετε περιορισμούς.
5. Επιλέξτε τον σύνδεσμο Εγκατάσταση Parental Advisor σε device στην επιθυμητή κάρτα.
6. Κάντε κλικ στο ΠΡΟΣΘΗΚΗ ΣΥΣΚΕΥΗΣ στο παράθυρο που εμφανίζεται.
7. Η επιλογή Bitdefender Parental Advisor για Android είναι προεπιλεγμένη. Επιλέξτε ΕΠΟΜΕΝΟ για να συνεχίσετε, και στη συνέχεια εγκαθιστάτε την εφαρμογή στην επιθυμητή συσκευή.
8. Επιλέξτε την καρτέλα Επαφές τηλεφώνου.
   Μια λίστα με κάρτες εμφανίζεται. Οι κάρτες αντιπροσωπεύουν τις επαφές από το Android smartphone του παιδιού σας.
9. Επιλέξτε την κάρτα με τον αριθμό τηλεφώνου που θέλετε αποκλείσετε.
   Το σύμβολο που εμφανίζεται υποδεικνύει ότι το παιδί σας δεν θα είναι να λάβει τηλεφωνήματα από το συγκεκριμένο τηλεφωνικό αριθμό.

Για να αποκλείσετε άγνωστους αριθμούς τηλεφώνου, ενεργοποιήστε το διακόπτη Αποκλεισμός αλληλεπιδράσεων με άγνωστους (χωρίς αναγνώριση κλήσης).

Σημείωση
Οι περιορισμοί τηλεφωνικών κλήσεων μπορούν να οριστούν μόνο για συσκευές Android που έχουν προστεθεί στο προφίλ του παιδιού σας.

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

Ο Bitdefender Γονικός Σύμβουλος σας επιτρέπει να ορίσετε μια τοποθεσία ως ασφαλή ή μη προσβάσιμη για το παιδί σας.

Για να ορίσετε μια τοποθεσία:
2. Συνδεθείτε στο Bitdefender λογαρισμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Κάντε κλικ στο Γονικός Σύμβουλος για να αποκτήσετε πρόσβαση στο ταμπλό.
4. Επιλέξτε το προφίλ του παιδιού σας από το παράθυρο MY CHILDREN.
5. Επιλέξτε την καρτέλα Τοποθεσία παιδιού.
6. Κάντε κλικ στο Συσκευές στο πλαίσιο που έχετε στο παράθυρο Τοποθεσία παιδιού.
7. Κάντε κλικ στο ΕΠΙΛΟΓΗ ΣΥΣΚΕΥΗΣ και στη συνέχεια, επιλέξτε τη 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 ασφαλής, 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.

Πώς μπορώ να μποκάρω την πρόσβαση του παιδιού μου στις συνδεδεμένες σε αυτό συσκεύες του κατά την διάρκεια των σχολικών ημερών;

Ο Bitdefender Σύμβουλος Γονικού Ελέγχου σας επιτρέπει να οριοθετήσετε την πρόσβαση του παιδιού σας στις συσκευές του κατά την διάρκεια του σχολείου και μέχρι να ολοκληρωθεί η δουλειά του σχολείου για το σπίτι. Για να θέσετε τους περιορισμούς:

1. Συνδεθείτε στο Parental Advisor μέσω του Bitdefender Central.
2. Από το παράθυρο ΤΑ ΠΑΙΔΙΑ ΜΟΥ, επιλέξτε το προφίλ του παιδιού του οποίου θέλετε να δώσετε περιορισμούς.
3. Επιλέξτε την καρτέλα Χρονοδιάγραμμα.
4. Στην περιοχή Όρια της ημέρας, επιλέξτε ΣΥΓΚΕΚΡΙΜΕΝΟ.
5. Επιλέξτε το Όρια Σχολικής Ημέρας check box.
6. Επιλέξτε από το πλέγμα τα χρονικά διαστήματα κατά τα οποία η πρόσβαση στο Διαδίκτυο θα θέλατε να είναι αποκλεισμένη.

Σημείωση
Οι περιορισμοί μπορούν να οριστούν μόνο για συσκευές Android και Windows.

Πώς μπορώ να αποκλείσω την πρόσβαση του παιδιού μου στις συνδεδεμένες σε αυτό συσκευές του κατά την διάρκεια της νύχτας της σχολικής περιόδου;

Ο Bitdefender Γονικός Έλεγχος σας επιτρέπει να οριοθετήσετε την πρόσβαση του παιδιού σας στις συσκευές του τις νύχτες κατά την διάρκεια της σχολικής περιόδου.

Για να θέσετε τους περιορισμούς:
1. Συνδεθείτε στο Parental Advisor μέσω του Bitdefender Central.
2. Από το παράθυρο ΤΑ ΠΑΙΔΙΑ ΜΟΥ, επιλέξτε το προφίλ του παιδιού του οποίου θέλετε να δώσετε περιορισμούς.
3. Επιλέξτε την καρτέλα Χρονοδιάγραμμα.
4. Στην περιοχή Όρα Ύπνου, επιλέξτε το Νύχτες Σχολείου check box.
5. Χρησιμοποιήστε τα πάνω και κάτω βέλη του πληκτρολογίου στα αντίστοιχα πεδία για να θέσετε τον χρόνο που θα θέλατε η πρόσβαση να είναι αποκλεισμένη.

Σημείωση
Οι περιορισμοί μπορούν να οριστούν μόνο για συσκευές Android και Windows.
Πώς μπορώ να αποκλείσω την πρόσβαση του παιδιού μου στις συσκευές του κατά την διάρκεια του Σαββατοκύριακου;

Ο Bitdefender Γονικός Έλεγχος σας επιτρέπει να οριοθετήσετε την πρόσβαση του παιδιού σας στις συσκευές του κατά την διάρκεια του Σαββατοκύριακου.

Για να θέσετε τους περιορισμούς:

1. Συνδεθείτε στο Parental Advisor μέσω του Bitdefender Central.
2. Από το παράθυρο ΤΑ ΠΑΙΔΙΑ ΜΟΥ, επιλέξτε το προφίλ του παιδιού του οποίου θέλετε να δώσετε περιορισμούς.
3. Επιλέξτε την καρτέλα Χρονοδιάγραμμα.
4. Στην περιοχή Ωρα Ύπνου, επιλέξτε το Βραδιές Σαββατοκύριακου check box.
5. Χρησιμοποιήστε τα πάνω και κάτω βέλη του πληκτρολογίου στα αντίστοιχα πεδία για να θέσετε τον χρόνο που θα θέλατε να είναι αποκλεισμένη.
6. Στην περιοχή Ωρα της ημέρας έχετε τις ακόλουθες επιλογές:
   ● ΣΩΡΕΥΤΙΚΑ
     a. Επιλέξτε το Όρια Χρόνου Σαββατοκύριακου check box.
     b. Τραβήξτε την κλίμακα προς τα δεξιά ή αριστερά για να ορίσετε τον επιτρεπόμενο χρόνο πρόσβασης στις συσκευές.
   ● ΣΥΓΚΕΚΡΙΜΕΝΑ
     a. Επιλέξτε το Όρια Χρόνου Σαββατοκύριακου check box.
     b. Επιλέξτε από το πλέγμα τα χρονικά διαστήματα κατά τα οποία η πρόσβαση στο Διαδίκτυο θα θέλατε να είναι αποκλεισμένη.

Σημειώστε ότι το ΣΟΡΕΥΤΙΚΑ και ΣΥΓΚΕΚΡΙΜΕΝΑ δεν είναι σχεδιασμένα για να είναι ενεργοποιημένα ταυτόχρονα,

Σημείωση
Οι περιορισμοί μπορούν να οριστούν μόνο για συσκευές Android και Windows.

Πώς να αφαιρέσετε το προφίλ ενός παιδιού

Αν θέλετε να αφαιρέσετε ένα υπάρχον προφίλ παιδιού:
2. Συνδεθείτε στο Bitdefender λογαρισμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
3. Κάντε κλικ στο Πατρικό Σώματος για να αποκτήσετε πρόσβαση στο ταμπλό.
4. Κάντε κλικ στο εικονίδιο από το προφίλ του παιδιού που θέλετε να διαγράψετε, στη συνέχεια, επιλέξτε Διαγραφή.

3.6 Έλεγχος Απορρήτου

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

Για να βεβαιωθείτε ότι οι διαδικτυακές δραστηριότητές σας παραμένουν ιδιωτικές, μπορείτε να χρησιμοποιήσετε το πρόγραμμα περιήγησης που παρέχεται από το Bitdefender για να προστατεύσει 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 δραστηριότητές σας ασφαλείς και ιδιωτικές:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο κουμπί Safepay.
3. Κάντε κλικ στο κουμπί για να αποκτήσετε πρόσβαση στο Εικονικό Πληκτρολόγιο.

Χρησιμοποιήστε το Εικονικό Πληκτρολόγιο όταν πληκτρολογείτε απόρρητες πληροφορίες όπως τους κωδικούς πρόσβασης σας.
Τι μπορώ να κάνω αν η συσκευή μου έχει κλεφθεί;

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. Στο παράθυρο MY DEVICES, επιλέξτε τη συσκευή.
4. Κάντε κλικ στο Anti-Theft (Κατά της κλοπής συσκευής).
5. Επιλέξτε την λειτουργία που θέλετε να χρησιμοποιήσετε

- **ΕΝΤΟΠΙΣΜΟΣ** - εμφανίζει την τοποθεσία της συσκευής σας στο Google Maps.

- **Ειδοποίηση** - στέλνει μια ειδοποίηση στη συσκευή.

- **Κλείδωμα** - κλειδώνετε τον υπολογιστή σας και ορίζετε ένα αριθμητικό PIN κώδικα για το ξεκλείδωμα του. Εναλλακτικά, ενεργοποιήστε την αντίστοιχη επιλογή για να επιτρέψετε το Bitdefender να λαμβάνει στιγμιότυπα του ατόμου που προσπαθεί να αποκτήσει πρόσβαση συσκευή σας.

- **Wipe** (απαλοιφή) - διαγράφετε όλα τα δεδομένα από τον υπολογιστή 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.
Πώς μπορώ να χρησιμοποιήσω τα θησαυροφυλάκια (vaults) αρχείων ;

To Bitdefender File Vault σας επιτρέπει να δημιουργήσετε κρυπτογραφημένα, προστατευόμενα από κωδικό πρόσβασης λογικούς δίσκους (ή θησαυροφυλάκια) στον υπολογιστή σας, όπου μπορείτε να αποθηκεύετε με ασφάλεια εμπιστευτικούς και ευαίσθητους εγγράφους σας. Σε φυσικό επίπεδο το θησαυροφυλάκιο (vault) είναι ένα αρχείο αποθηκευμένο στον τοπικό σκληρό δίσκο και φέρει την επέκταση .bvd

Όταν δημιουργείτε ένα θησαυροφυλάκιο αρχείων, δύο στοιχεία είναι σημαντικά: το μέγεθος και ο κωδικός πρόσβασης. Το προεπιλεγμένο μέγεθος 100 MB θα πρέπει να είναι αρκετό για τα προσωπικά σας έγγραφα, αρχεία Excel και άλλα παρόμοια δεδομένα. Ωστόσο, για τα βίντεο ή άλλα μεγάλα αρχεία μπορεί να χρειαστείτε περισσότερο χώρο.

Για να αποθηκεύσετε με ασφάλεια τα εμπιστευτικά ή ευαίσθητα αρχεία ή τους φακέλους σας στο Bitdefender file vaults:

● Δημιουργήστε ένα θησαυροφυλάκιο αρχείων και να ορίσετε έναν ισχυρό κωδικό πρόσβασης για αυτό.

Για να δημιουργήσετε ένα θησαυροφυλάκιο, κάντε δεξί κλικ σε μια κενή περιοχή της επιφάνειας εργασίας ή σε ένα φάκελο στον υπολογιστή σας, δείξτε στο Bitdefender > Bitdefender Vault Άρχειων και επιλέξτε Δημιουργία Vault αρχείων.

Εμφανίζεται ένα νέο παράθυρο. Ακολουθήστε την εξής διαδικασία:

1. Κάντε κλικ στο Περιήγηση , επιλέξτε τη θέση του vault και αποθηκεύστε το με το επιθυμητό όνομα.
2. Επιλέξτε έναν γράμμα μονάδας δίσκου από το μενού. Όταν ανοίξεις το vault, ένας εικονικός δίσκος αντιστοιχισμένος στο επιλεγμένο γράμμα εμφανίζεται στο Ο υπολογιστής μου.
3. Πληκτρολογήστε τον κωδικό πρόσβασης Vault στα πεδία κωδικός και Επιβεβαίωση.
4. Αν θέλετε να αλλάξετε το προεπιλεγμένο μέγεθος (100 MB) του Vault, χρησιμοποιήστε το πάνω και κάτω βέλος από το Vault size (MB) spin box.
5. Κάντε κλικ στο Δημιουργία.
Σημείωση
Όταν ανοίξει το χρηματοκιβώτιο, μια εικονική μονάδα δίσκου εμφανίζεται στο Ο Υπολογιστής Μου. Η μονάδα δίσκου φρει το γράμμα μονάδας δίσκου που εκχωρήθηκε στο θησαυροφυλάκιο.

● Προσθέστε τα αρχεία ή τους φακέλους που θέλετε να φυλάξετε στο θησαυροφυλάκιο.

Για να προσθέσετε ένα αρχείο σε ένα θησαυροφυλάκιο, πρέπει πρώτα να ανοίξετε το θησαυροφυλάκιο.

1. Πλοηγηθείτε στο .bvd θησαυροφυλάκιο.
2. Κάντε δεξί κλικ στο αρχείο Vault, δείξτε στο Bitdefender File Vault και επιλέξτε Άνοιγμα.
3. Στο παράθυρο που εμφανίζεται εισάγετε τον κωδικό πρόσβασης, επιλέξτε ένα γράμμα μονάδας δίσκου για να εκχωρήσετε στο vault και κάντε κλικ OK.

Τώρα μπορείτε να εκτελέσετε εργασίες στη μονάδα δίσκου που αντιστοιχεί στο επιθυμητό θησαυροφυλάκιο (vault) χρησιμοποιώντας την Εξερεύνηση των Windows, όπως ακριβώς θα κάνατε με ένα κανονικό δίσκο. Για να προσθέσετε ένα αρχείο σε ένα ανοικτό vault, μπορείτε να κάνετε δεξί κλικ στο αρχείο, δείξτε στο Bitdefender File Vault και επιλέξτε Προσθήκη στο Vault.

● Κρατήστε το Vault πάντα κλειδωμένο.

Να ανοίγετε τα θησαυροφυλάκια, μόνο όταν θα πρέπει να τα προσελέστε ή να διαχειριστείτε το περιεχόμενό τους. Για να κλειδώσετε ένα θησαυροφυλάκιο, κάντε δεξί κλικ στον αντίστοιχο εικονικό δίσκο από το Ο υπολογιστής μου, δείξτε στο Bitdefender File Vault και επιλέξτε Κλείδωμα.

● Βεβαιωθείτε ότι δεν διαγράψετε το .bvd vault αρχείο.

Διαγραφή του αρχείου διαγράφει επίσης το περιεχόμενο του θησαυροφυλάκιου.

Για περισσότερες πληροφορίες σχετικά με τη λειτουργία με θησαυροφυλάκια, παρακαλούμε ανατρέξτε στο "Κρυπτογράφηση Αρχείου" (p. 158).
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.

Ο Bitdefender καταστροφέας αρχείου (File Shredder) θα σας βοηθήσει να καταστρέψετε γρήγορα αρχεία ή φακέλους από τον υπολογιστή σας χρησιμοποιώντας το αναδυόμενο μενού 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. Εμφανίζεται ένα παράθυρο επιβεβαίωσης. Επιλέξτε ΝΑΙ, ΔΙΑΓΡΑΦΗ για να ξεκινήσει ο οδηγός καταστροφής αρχείων.
   Περιμένετε να τελειώσει το Bitdefender την καταστροφή των αρχείων.
3. Τα αποτελέσματα εμφανίζονται. Επιλέξτε ΤΕΛΟΣ για να βγείτε από τον οδηγό.

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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο ΠΡΟΣΤΑΣΙΑ WEB, επιλέξτε Πρόσβαση στη Webcam.
   Εμφανίζεται η λίστα με τις εφαρμογές που έχουν ζητήσει πρόσβαση στην κάμερα σας.
4. Επιλέξτε την εφαρμογή που θέλετε να επιτρέψετε ή να απαγορεύσετε την πρόσβαση και, στη συνέχεια, κάντε κλικ στον αντίστοιχο διακόπτη.
   Για να δείτε τι έχουν επιλέξει οι άλλοι Bitdefender χρήστες για την επιλεγμένη εφαρμογή, κάντε κλικ στο εικονίδιο. Θα ειδοποιείστε κάθε φορά που μία από τις εφαρμογές που αναφέρονται αποκλείονται...
από τους Bitdefender χρήστες, ανεξάρτητα του status του αυτόματου πιλότου.
Για να προσθέσετε χειροκίνητα εφαρμογές σε αυτή τη λίστα, κάντε κλικ στο σύνδεσμο Προσθήκη νέας εφαρμογής στη λίστα.

Σημείωση
Καθώς οι εφαρμογές των Windows Store εκτελούνται με μία και μοναδική διαδικασία, κάθε φορά που η πρόσβαση σε μία από τις εφαρμογές της ορίζεται ως "Επιτρέπεται" ή "Αποκλεισμός", ο κανόνας θα εφαρμοστεί σε ολόκληρο το σύστημα. O Internet Explorer και ο Microsoft Edge είναι δύο παραδείγματα τέτοιων εφαρμογών.

3.7. Εργαλεία βελτιστοποίησης
Πώς μπορώ να βελτιώσω την απόδοση του συστήματός μου;

Η απόδοση του συστήματός 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 ενισχύουν την απόδοση του συστήματός σας και την απόδοσή του έχουν ως εξής:

● “Βελτιστοποίηση της απόδοσης του συστήματός σας με ένα μόνο κλικ” (p. 85)
● “Σάρωση του συστήματός σας σε τακτά χρονικά διαστήματα” (p. 86)

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 συστήματός σας με την ανίχνευση και την καθαρισμό άχρηστων αρχείων.

Για να ξεκινήσετε τη διαδικασία OneClick Optimizer:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο OneClick Optimizer κουμπί.

3. Επιτρέψτε στο Bitdefender να αναζητήσει τα αρχεία που μπορούν να διαγραφούν, στη συνέχεια, κάντε κλικ στο κουμπί OPTIMIZE για να ολοκληρώσετε τη διαδικασία.

Για περισσότερες πληροφορίες σχετικά με το πώς μπορείτε να βελτιώσετε την ταχύτητα του υπολογιστή σας με ένα μόνο κλικ, μπορείτε να ανατρέξετε στο “Βελτιστοποίηση της ταχύτητας του συστήματός σας με ένα μόνο κλικ” (p. 197).

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 κακόβουλου λογισμικού (malware) που απειλούν την ασφάλεια του συστήματός σας και σαρώνει επίσης μέσα συμπιεσμένα αρχεία.

Για να ξεκινήσετε τη σάρωση του συστήματος:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα Antivirus επιλέξτε Σάρωση Συστήματος.
4. Ακολουθήστε τα βήματα του οδηγού.

Πώς μπορώ να βελτιώσω το χρόνο εκκίνησης του συστήματος;

Περιττές εφαρμογές που ενοχλητικά επιβραδύνουν το χρόνο εκκίνησης όταν ανοίγετε το PC σας μπορούν να απενεργοποιηθούν ή να αναβληθεί η εκκίνησή τους με τη βελτιστοποίηση εκκίνησης (startup Optimizer ) εξοικονομώντας σας πολύτιμο χρόνο.

Για να χρησιμοποιήσετε το Startup Optimizer:
1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο Startup Optimizer κουμπί.
3. Επιλέξτε τις εφαρμογές που θέλετε να καθυστερούν κατά την εκκίνηση του συστήματος.

Για περισσότερες πληροφορίες σχετικά με τη βελτιστοποίηση του χρόνου εκκίνησης του HY σας, παρακαλούμε ανατρέξτε στο “Βελτιστοποίηση του χρόνου εκκίνησης του PC σας” (p. 198).

3.8. Χρήσιμες πληροφορίες

Πώς μπορώ να δοκιμάσω τη λύση antivirus 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 από ιούς σας χρησιμοποιώντας ένα ασφαλές αρχείο που αναπτύχθηκε για το σκοπό αυτό.

Για να ελέγξετε την λύση antivirus σας:

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 ιός).

Εάν κάνετε κλικ καταλαβαίνω, προχωράμε όπως έχετε βρεις ή άλλως , η λήψη του τεστ θα ξεκινήσει και ένα Bitdefender αναδυόμενο θα σας ενημερώνει ότι ένας ιός 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. 327).

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 στη 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 στη 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.

Σημείωση

Αυτή η διαδικασία επανεγκατάστασης θα διαγράψει οριστικά τις προσαρμοσμένες ρυθμίσεις.

Πως γίνεται να κλείνει αυτόματα ο υπολογιστής μετά την ολοκλήρωση της σάρωσης:

To Bitdefender προσφέρει πολλαπλές εργασίες σάρωσης που μπορείτε να χρησιμοποιήσετε για να βεβαιωθείτε ότι το σύστημά σας δεν έχει μολυνθεί με κακόβουλο λογισμικό. Η πλήρης σάρωση για το σύνολο του υπολογιστή μπορεί να διαρκέσει περισσότερο χρόνο για να ολοκληρωθεί, ανάλογα με το υλικό του συστήματός σας και τη διαμόρφωση λογισμικού.

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

Σκεφτείτε το εξής παράδειγμα: έχετε τελειώσει την εργασία σας στον υπολογιστή και θέλετε να πάτε για ύπνο. Θα θέλατε το Bitdefender να ελέγξει ολόκληρο το σύστημά σας για κακόβουλο λογισμικό.

Ρύθμιση του Bitdefender για να κλείσει το σύστημά σας στο τέλος της σάρωσης:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο **ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ**.

3. Στην ενότητα **Antivirus** επιλέξτε **Διαχείριση σαρώσεων**.

4. Στο παράθυρο **ΔΙΑΧΕΙΡΙΣΗ ΕΡΓΑΣΙΩΝ ΣΑΡΩΣΗΣ**, επιλέξτε **Νέα προσαρμοσμένη εργασία** για να εισάγετε ένα όνομα για τη σάρωση και να επιλέξτε τους χώρους στη συσκευή που πρόκειται να σαρώθουν.
5. Αν θέλετε να ρυθμίσετε τις επιλογές σάρωσης στη λεπτομέρεια, επιλέξτε την καρτέλα για προχωρημένους.

6. Επιλέξτε κλείσιμο τον υπολογιστή, όταν η σάρωση είναι ολοκληρωθεί και δεν βρεθούν απειλές.

7. Κάντε κλικ στο OK για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

8. Κάντε κλικ στην επιλογή Έναρξη Σάρωσης να σαρώσετε το σύστημά σας.

Εάν δεν βρεθούν απειλές, ο υπολογιστής θα κλείσει.

Εάν υπάρχουν παραμένοντες μη εξουδετερωμένες απειλές, θα σας ζητηθεί να επιλέξετε τις ενέργειες που πρέπει να εφαρμοστούν σε αυτές. Για περισσότερες πληροφορίες παρακαλείται να συνεχίσετε στο "Οδηγός σαρωτή Antivirus" (p. 110).

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

Εάν ο υπολογιστής σας συνδέεται στο Internet μέσω ενός διακομιστή μεσολάβησης (Proxy server), πρέπει να προσαρμόσετε τις ρυθμίσεις proxy στο Bitdefender. Εάν ο υπολογιστής σας συνδέεται στο Internet μέσω ενός διακομιστή μεσολάβησης (Proxy server), πρέπει να προσαρμόσετε τις ρυθμίσεις proxy στο Bitdefender. Εάν ο υπολογιστής σας συνδέεται στο Internet μέσω ενός διακομιστή μεσολάβησης (Proxy server), πρέπει να προσαρμόσετε τις ρυθμίσεις proxy στο Bitdefender.

Σημαντικό
Οικιακές Συνδέσεις στο Διαδίκτυο συνήθως δεν χρησιμοποιούν διακομιστή μεσολάβησης. Ως γενικός κανόνας, ελέγχετε και διαμορφώστε τις ρυθμίσεις του διακομιστή μεσολάβησης σύνδεση στο Bitdefender πρόγραμμα 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. Κάντε κλικ στον παράδειγμα του στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Advanced.
3. Ενεργοποιήστε την επιλογή Χρήση proxy κάνοντας κλικ στον αντίστοιχο διακόπτη.
4. Κάντε κλικ στο Διαχειριστείτε proxies.
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
To 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 μεσολάβησης.

○ 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..

Χρησιμοποιώ μια 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 o υπολογιστής μου από το μενού Έναρξη.
3. Κάντε δεξί κλικ στο O 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.

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 εικονίδιό του.

2. Ψάξτε στην περιοχή του συστήματος για να βρείτε πληροφορίες σχετικά με τον τύπο του συστήματός σας.

Εμφάνιση κρυφών αντικειμένων στα Windows.

Τα βήματα αυτά είναι χρήσιμα σε περιπτώσεις όπου έχουμε να κάνουμε με μία περίπτωση malware 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 εικονίδιό 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 дίσκου.
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.

Πώς μπορώ να καταργήσω τις άλλες λύσεις ασφαλείας;
Ο κύριος λόγος για τη χρήση μιας λύσης ασφαλείας 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 λύση ασφαλείας στον ίδιο υπολογιστή, το σύστημα γίνεται ασταθές. Ο Bitdefender Total Security εγκαταστάσεις αυτόματα 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, στη συνέχεια, επιλέξτε Εγκατεστημένες 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 απελευθέρωσης από την ιστοσελίδα του προμηθευτή ή επικοινωνήστε απευθείας μαζί του για να σας δώσει τις κατευθυντήριες γραμμές για απελευθέρωση.

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 αντικρουόμενους οδηγούς συσκευών μέχρι ιούς που εμποδίζουν την κανονική εκκίνηση των Windows. Σε Ασφαλή λειτουργία εργάζονται λίγες μόνο εφαρμογές και τα Windows φορτώνουν μόνο τα βασικά προγράμματα οδήγησης και ένα ελάχιστο σετ υποσυστημάτων του λειτουργικού συστήματος. Ως εκ τούτου οι περισσότεροι ιοί είναι ανενεργά 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. Κάντε επανεκκίνηση του Υπολογιστή
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 επανεκκίνησε 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. ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΑΣΦΑΛΕΙΑΣ ΣΑΣ

4.1. Αntivirus Προστασία

Το Bitdefender προστατεύει τον υπολογιστή σας από κάθε είδους κακόβουλο λογισμικό (ιούς, 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 κακόβουλου λογισμικού 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 στο κακόβουλο λογισμικό, και καθιστά τον υπολογιστή ασφαλή. Αυτή η λειτουργία είναι ουσιώδες συστατικό κάθε προγράμματος ασφάλειας των υπολογιστών.

Οι προχωρημένοι χρήστες μπορούν να ρυθμίσουν εξαιρέσεις σάρωσης, εάν δεν θέλουν να σαρωθούν συγκεκριμένα αρχεία ή τύποι αρχείων. Για περισσότερες πληροφορίες αναφερθείτε στο "Διαμόρφωση εξαιρέσεων σάρωσης." (p. 117).

Όταν το Bitdefender εντοπίσει έναν ιό ή άλλο κακόβουλο λογισμικό, 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 σαρωθούν με την εν λόγω λειτουργία αναφέρονται ως εξαιρέσιμα αρχεία. Για περισσότερες πληροφορίες αναφερθείτε στο "Διαμόρφωση εξαιρέσεων σάρωσης." (p. 114).

Σημαντικό

Για να εμποδίσετε την μόλυνση του υπολογιστή σας από ιούς αφήστε ενεργή την σάρωση κατά την πρόσβαση.

Φόρτωση του υπολογιστή με ιό

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 συνδέονται με τον υπολογιστή σας για να εξασφαλίσει ότι μπορείτε να έχετε πρόσβαση με ασφάλεια. Για περισσότερες πληροφορίες αναφερθείτε στο "Αυτόματη σάρωση των αφαιρούμενων μέσων" (p. 114).

Διαχείριση της ασφάλειας σας
απολυμανθούν μετακινούνται στην καραντίνα προκειμένου να απομονωθεί η μόλυνση. Για περισσότερες πληροφορίες παρακολούμε αναφερθείτε στο "Διαχείριση αρχείων σε καραντίνα" (p. 120).

Εάν ο υπολογιστής σας έχει μολυνθεί με κακόβουλο λογισμικό, ανατρέξτε στο "Αφαίρεση κακόβουλου λογισμικού από το σύστημα σας" (p. 236). Για να σας βοηθήσει να καθαρίσετε τον υπολογιστή σας από κακόβουλο λογισμικό που δεν μπορεί να αφαιρεθεί ενώ το λειτουργικό σύστημα των Windows είναι ενεργό, το Bitdefender σας παρέχει "Bitdefender Λειτουργία διάσωσης (Περιβάλλον διάσωσης στα Windows 10)" (p. 237). Αυτό είναι ένα αξιόπιστο περιβάλλον, ειδικά σχεδιασμένο για την απομάκρυνση του κακόβουλου λογισμικού, το οποίο σας επιτρέπει να εκκινήσετε τον υπολογιστή σας ανεξάρτητα από τα Windows. Όταν ο υπολογιστής εκτελείται στη λειτουργία διάσωσης (περιβάλλον διάσωσης στα Windows 10), το κακόβουλο λογισμικό των Windows είναι ανενεργό, καθιστώντας εύκολη την κατάργηση του.

Σάρωση κατά την πρόσβαση (σε πραγματικό χρόνο προστασία)

Το Bitdefender παρέχει συνεχή, σε πραγματικό χρόνο προστασία ενάντια σε ένα ευρύ φάσμα απειλών malware 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 ενάντια σε κακόβουλο λογισμικό:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS.
4. Στο παράθυρο ΑΣΠΙΔΑ, κάντε κλικ στον διακόπτη ΟΝ/ΟFF.
5. Αν θέλετε να απενεργοποιήσετε την προστασία σε πραγματικό χρόνο, εμφανίζεται ένα παράθυρο προειδοποίησης. Θα πρέπει να
επιβεβαιώστε 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 προστασία σε πραγματικό χρόνο είναι απενεργοποιημένη, δεν θα προστατεύετε από απειλές κακόβουλου λογισμικού.

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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS.
4. Στο παράθυρο ΑΣΠΙΔΑ, κάντε κλικ στο μενού ΕΜΦΑΝΙΣΗ ΠΡΟΗΓΜΕΝΩΝ ΡΥΘΜΙΣΕΩΝ.
5. Θα εμφανιστεί ένα παράθυρο.
6. Κυλίστε προς τα κάτω στο παράθυρο για να διαμορφώσετε τις ρυθμίσεις σάρωσης, όπως απαιτείται.

Διαχείριση της ασφάλειας σας
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 επιλογές για αρχεία που έχουν προσπελασθεί. Μπορείτε να ρυθμίσετε το Bitdefender για να σαρώσετε όλα τα προσβάσιμα αρχεία ή εφαρμογές (αρχεία προγράμματος) μόνο. Σάρωση όλων των προσβάσιμων αρχείων παρέχει καλύτερη προστασία, ενώ σαρώνει τις εφαρμογές μόνο, μπορεί να χρησιμοποιηθεί για την καλύτερη απόδοση του συστήματος.

Από προεπιλογή, τόσο τοπικοί φάκελοι όσοι και φάκελοι δικτύου (κοινόχρηστοι ή μη) υπόκεινται σε σάρωση κατά την πρόσβαση. Για την καλύτερη απόδοση του συστήματος, μπορείτε να εξαιρέσετε θέσεις δικτύου από την σάρωση κατά την πρόσβαση.

Εφαρμογές (ή αρχεία του προγράμματος) είναι πολύ πιο ευάλωτα σε επιθέσεις malware από άλλους τύπους αρχείων. Αυτή η κατηγορία περιλαμβάνει τις ακόλουθες επεκτάσεις αρχείων:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; eeh; exe; exes; fky; frs; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; js; jse; jse; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdm; mdt; mdw; mem; mhtml; mmp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; pтом; potx; ppa; ppm; pps; ppsm; ppssx; ppt; pptm; pptx; psc; prf; prg; pst; pub; puz; pvd; pwc; py; py; pyo; qpx; rbx; rgs; rox; rpx; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxz; wbk; wcm; wdm; wiz; wiz; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsx; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsd; xtp

- Σάρωση στο εσωτερικό των 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. Το
κακόβουλο λογισμικό 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.

Αν αποφασίσετε να χρησιμοποιήσετε αυτήν την επιλογή, ενεργοποιήστε την και στη συνέχεια σύρετε το ρυθμιστικό κατά μήκος της κλίμακας για να ορίσετε ένα μέγιστο αποδεκτό όριο μεγέθους (σε MB) αρχείων που θα σαρωθούν για πρόσβαση.

● Σάρωση των e-mail. Για την αποφυγή μεταφόρτωσης κακόβουλων προγραμμάτων στον υπολογιστή σας, το Bitdefender σαρώνει αυτόματα τα εισερχόμενα και τα εξερχόμενα ηλεκτρονικά μηνύματα.

Αν και δεν συνιστάται, μπορείτε να απενεργοποιήσετε την σάρωση e-mail για ιούς για να αυξήσετε την απόδοση του συστήματος. Αν απενεργοποιήσετε τις αντίστοιχες επιλογές σάρωσης, τα μηνύματα e-mail και τα αρχεία που λαμβάνονται ή κατεβαίνουν από το Internet δεν θα σαρωθούν, επιτρέποντας έτσι μολυσμένα αρχεία να αποθηκεύονται στον υπολογιστή σας. Αυτό δεν είναι μια μεγάλη απειλή, διότι η σε πραγματικό χρόνο προστασία θα εμποδίσει το κακόβουλο λογισμικό, όταν γίνεται προσπέλαση στα μολυσμένα αρχεία (άνοιγμα, μετακίνηση, αντιγραφή ή εκτέλεση).

● 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 ένας ιός 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 νέων και τροποποιημένων αρχείων, μπορείτε να βελτιώσετε σημαντικά τη συνολική απόκριση του συστήματος με μία ελάχιστη έκπτωση τον 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 πληκτρολόγιο 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 κατά την εκκίνηση του συστήματος. Επιλέξτε το Early boot scan για να σαρώσετε το σύστημα σας κατά την εκκίνηση, την στιγμή που όλες οι κρίσιμες υπηρεσίες είναι φορτωμένες. Ο σκοπός αυτού του χαρακτηριστικού είναι να βελτιώσει την ανίχνευση του ιού κατά την εκκίνηση του συστήματος και τον χρόνο εκκίνησης του συστήματος σας.

Οι δράσεις που αναλαμβάνονται σχετικά με το ανιχνευθέν κακόβουλο λογισμικό

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

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS.
4. Στο παράθυρο ΑΣΠΙΔΑ, κάντε κλικ στο μενού ΕΜΦΑΝΙΣΗ ΠΡΟΗΓΜΕΝΩΝ ΡΥΘΜΙΣΕΩΝ.

Θα εμφανιστεί ένα παράθυρο.
5. Κάντε κύλιση προς τα κάτω στο παράθυρο μέχρι να δείτε τις επιλογές Ενέργειες μετά την ολοκλήρωση της σάρωσης.
6. 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. Αρχεία που ανιχνεύονται ως μολυσμένα ταιριάζουν σε μια υπογραφή κακόβουλου λογισμικού στο Bitdefender Malware Signature Database. 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 παρακολούμε αναφερθείτε στο “Διαχείριση αρχείων σε καραντίνα” (p. 120).

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

● Υποπτα αρχεία. Τα αρχεία ανιχνεύονται ως ύποπτα από την ευρετική ανάλυση. Τα ύποπτα αρχεία δεν μπορούν να επιδιορθωθούν, επειδή δεν είναι διαθέσιμα καμία λογισμική που επιδιορθώνει. 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 malware της Bitdefender. Αν επιβεβαιωθεί παρουσία κακοβουλου λογισμικού, μια υπογραφή απελευθερώνεται για να επιτρέψει την αφαίρεσή του κακοβουλου λογισμικού.

● 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 αρχείων στην 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 παρακολούμε αναφερθείτε στο “Διαχείριση αρχείων σε καραντίνα” (p. 120).
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 κακόβουλο λογισμικό, με ελάχιστες επιπτώσεις στην απόδοση του συστήματος.

Για να επαναφέρετε τις ρυθμίσεις προστασίας στην προεπιλογή:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS
4. Στο παράθυρο ΑΣΠΙΔΑ, κάντε κλικ στο μενού ΕΜΦΑΝΙΣΗ ΠΡΟΗΓΜΕΝΩΝ ΡΥΘΜΙΣΕΩΝ.
   Θα εμφανιστεί ένα παράθυρο.
5. Κάντε κύλιση προς τα κάτω στο παράθυρο μέχρι να δείτε την επιλογή Επαναφορά ρυθμίσεων. Επιλέξτε αυτήν την επιλογή για να επαναφέρετε τις προεπιλεγμένες ρυθμίσεις της προστασίας από ιούς.

On-demand σάρωση
Ο κύριος στόχος για το Bitdefender είναι να κρατήσει τον υπολογιστή σας καθαρό από ιούς. Αυτό γίνεται εμποδίζοντας τους νέους ιούς από τον υπολογιστή σας και σαρώνοντας τα e-mail σας και τυχόν νέα αρχεία που κατεβαίνουν ή αντιγράφονται στο σύστημά σας.

Υπάρχει ο κίνδυνος ότι ένας ιός έχει ήδη εισχωρήσει στο σύστημά σας, πριν και να εγκαταστήσετε το Bitdefender. Για αυτό η σάρωση του υπολογιστή σας για παραμένοντες στη μνήμη ιούς είναι μια πολύ καλή ιδέα αφού έχετε εγκαταστήσει το Bitdefender. Και είναι σίγουρα μια καλή ιδέα να σαρώνετε τον υπολογιστή σας συχνά για ιούς.

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 τον υπολογιστή σας όποτε
θέλετε, εκτελώντας τις προεπιλεγμένες εργασίες ή τις δικές σας εργασίες σάρωσης (οριζόμενες από το χρήστη). Αν θέλετε να σαρώσετε συγκεκριμένες θέσεις στον υπολογιστή σας ή να ρυθμίσετε τις επιλογές σάρωσης, να ρυθμίσετε και να εκτελέσετε μια προσαρμοσμένη εργασία σάρωσης.

Σάρωση αρχείου ή φάκελου για κακόβουλο λογισμικό

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 ζητήσει 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 cloud για την ανίχνευση κακόβουλου λογισμικού που εκτελείται στο σύστημά σας. Η εκτέλεση της Γρήγορη σάρωση 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. Κάντε κλικ στο εικονίδιο Μ στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα Antivirus επιλέξτε 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 ζητήσει να επιλέξετε τις ενέργειες που πρέπει να εφαρμοστούν σε αυτές.

Η για πιο γρήγορα, κάντε κλικ στο εικονίδιο Μ στην αριστερή μπάρα του Bitdefender interface και στη συνέχεια κάντε κλικ στο κουμπί Quick Scan.
Εκτέλεση Σάρωσης Συστήματος

Η εργασία Σάρωση Συστήματος σαρώνει όλο τον υπολογιστή για όλους τους τύπους κακόβουλου λογισμικού που απειλούν την ασφάλειά του, όπως ιός, spyware, adware, rootkits και άλλα.

Σημείωση
Επειδή η Σάρωση Συστήματος εκτελεί μια πλήρη σάρωση του όλου συστήματος, η σάρωση μπορεί να πάρει λίγο χρόνο. Ως εκ τούτου, συνιστάται να εκτελέσετε αυτή την εργασία όταν δεν χρησιμοποιείτε τον υπολογιστή σας.

Πριν την εκτέλεση Σάρωσης Συστήματος, συνιστώνται τα εξής:

● Βεβαιωθείτε ότι το Bitdefender είναι ενημερωμένο με τις τελευταίες υπογραφές malware. Σάρωση στον υπολογιστή σας, χρησιμοποιώντας μια βάση δεδομένων με παλαιό αρχείο υπογραφών μπορεί να αποτρέψει το Bitdefender από την ανίχνευση νέου malware που εμφανίστηκαν μετά την τελευταία ενημέρωση. Για περισσότερες πληροφορίες παρακολούθετε το "Διατηρώντας το Bitdefender ενημερωμένο με τις πιο πρόσφατες ενημερώσεις" (p. 48).

● Τερματίστε όλα τα ανοιχτά προγράμματα.

Αν θέλετε να σαρώσετε συγκεκριμένες θέσεις στον υπολογιστή σας ή να ρυθμίσετε τις επιλογές σάρωσης, να ρυθμίσετε και να εκτελέσετε μια προσαρμοσμένη εργασία έργωσης. Για περισσότερες πληροφορίες παρακολούθετε αναφερθείτε στο "Ρύθμιση προσαρμοσμένης σάρωσης" (p. 107).

Για να εκτελέσετε μια σάρωση του συστήματος:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα Antivirus επιλέξτε Σάρωση Συστήματος.
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 παραμένοντες μη εξουδετερωμένες απειλές, θα σας ζητηθεί να επιλέξετε τις ενέργειες που πρέπει να εφαρμοστούν σε αυτές.
Ρύθμιση προσαρμοσμένης σάρωσης

Για να διαμορφώσετε μια προσαρμοσμένη σάρωση σε λεπτομέρεια και στη συνέχεια να την εκτελέσετε:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Στην ενότητα Antivirus επιλέξτε Διαχείριση σαρώσεων.

4. Κάντε κλικ στο κουμπί New custom task. Στην καρτέλα Βασικό εισάγετε ένα όνομα για τη σάρωση και επιλέξτε τις θέσεις που πρόκειται να σαρωθούν.

5. Αν θέλετε να ρυθμίσετε τις επιλογές σάρωσης στη λεπτομέρεια, επιλέξτε την καρτέλα για προχωρημένους. Εμφανίζεται ένα νέο παράθυρο. Ακολουθείστε αυτά τα βήματα:

a. Μπορείτε εύκολα να ρυθμίσετε τις επιλογές σάρωσης με την προσαρμογή του επιπέδου σάρωσης. Σύρετε το ρυθμιστικό κατά μήκος της κλίμακας για να ρυθμίσετε το επιθυμητό επίπεδο σάρωσης. Χρησιμοποιήστε την περιγραφή στη δεξιά πλευρά της κλίμακας για να εντοπίσετε το επίπεδο σάρωσης που ταιριάζει καλύτερα στις ανάγκες σας.

b. Μπορείτε επίσης να ρυθμίσετε αυτές τις γενικές επιλογές:

- **Εκτέλεση της εργασίας με χαμηλή προταιρεότητα.** Μειώνει την προτεραιότητα της διαδικασίας σάρωσης. Θα επιτρέψει σε άλλα προγράμματα να τρέξουν γρηγορότερα και θα αυξήσει το χρόνο που απαιτείται για την ολοκλήρωση της διαδικασίας σάρωσης.

- **Ελαχιστοποιήστε τον Οδηγό σάρωσης στην περιοχή ειδοποιήσεων.** Ελαχιστοποιήστε το παράθυρο σάρωσης στην περιοχή ειδοποιήσεων. Κάντε διπλό κλικ στο Bitdefender εικονίδιο για να το ανοίξετε.
Καθορίστε τη δράση που θα αναληφθεί σε περίπτωση που δεν βρεθούν απειλές.

c. Κάντε κλικ στο OK για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

6. Αν θέλετε να ορίσετε ένα χρονοδιάγραμμα για την εργασία σάρωσης, χρησιμοποιήστε το διακόπτη Schedule στο παράθυρο Basic. Επιλέξτε μία από τις αντίστοιχες επιλογές για να θέσετε ένα χρονοδιάγραμμα:

- Κατά την εκκίνηση του συστήματος
- Μία φορά
- Περιοδικά

7. Κάντε κλικ στο έναρξη σάρωσης και ακολουθήστε τον οδηγό Antivirus Scan για να ολοκληρώσετε τη σάρωση. Ανάλογα με τις θέσεις που πρέπει να σαρωθούν, η σάρωση μπορεί να πάρει λίγο χρόνο. Στο τέλος της σάρωσης, θα σας ζητήσει να επιλέξετε τις ενεργείες που πρέπει να ληφθούν για τα εντοπισμένα αρχεία, εάν εντοπισθούν κάποια μολυσμένα.

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

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 αρχείων. Μπορείτε να ρυθμίσετε το Bitdefender για να σαρώσετε όλους τους τύπους αρχείων ή εφαρμογών (αρχεία προγράμματος) μόνο. Σάρωση όλων των αρχείων παρέχει την καλύτερη προστασία, ενώ η σάρωση των εφαρμογών μόνο, μπορεί να χρησιμοποιηθεί για την καλύτερη απόδοση του συστήματος.

Εφαρμογές (ή αρχεία του προγράμματος) είναι πολύ πιο ευάλωτα σε επιθέσεις malware από άλλους τύπους αρχείων. Αυτή η κατηγορία περιλαμβάνει τις ακόλουθες επεκτάσεις αρχείων: 386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com;
Επιλογές Σάρωσης για τα αρχεία. Συμπιεσμένα αρχεία που περιέχουν μολυσμένα αρχεία δεν αποτελούν άμεση απειλή για την ασφάλειά του συστήματός σας. Το κακόβουλο λογισμικό 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.

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

Τομείς εκκίνησης σάρωσης. Μπορείτε να ρυθμίσετε το Bitdefender για να σαρώσετε τους τομείς εκκίνησης του σκληρού δίσκου. Ο τομέας του σκληρού δίσκου περιέχει τον απαραίτητο κώδικα υπολογιστή για την ενεργοποίηση της διαδικασίας εκκίνησης. Όταν ένας ιός 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.
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 σάρωσης 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 προώθησης 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 ζητήσει να δώσετε τον κωδικό. Προστατευμένα 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 παρακάψετε 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 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 ΟΚ για να συνεχίσετε τη σάρωση.

Βήμα 2 - Επιλέξτε ενέργειες

Στο τέλος της σάρωσης, θα σας ζητήσει να επιλέξετε τις ενέργειες που πρέπει να ληφθούν για τα εντοπισμένα αρχεία, εάν εντοπίσθηκαν κάπως προστατευμένα.

Σημείωση

Όταν εκτελέστε 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 ζητήσει να επιλέξετε τις ενέργειες που πρέπει να εφαρμοστούν σε αυτές.
Τα μολυσμένα αντικείμενα εμφανίζονται σε ομάδες, με βάση το malware με το οποίο 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 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.** Αρχεία που ανιχνεύονται ως μολυσμένα ταιριάζουν σε μια υπογραφή κακόβουλου λογισμικού στο Bitdefender Malware Signature Database. 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 μολυνθεί εξαφανίζεται. Για περισσότερες πληροφορίες παρακαλούμε να αναφέρετε στο “Διαχείριση αρχείων σε καραντίνα” (p. 120).

**Σημαντικό**

Για συγκεκριμένους τύπους malware, 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 απομονωθεί μια πιθανή μόλυνση.

Από προεπιλογή θα εκτελεστεί μια αυτόματα εργαστήρια, το κακόβουλο λογισμικό αναζητά στον κακόβουλο λογισμικό της Bitdefender. Αν επιβεβαιωθεί ο χρήση του κακόβουλου λογισμικού, θα απελευθερώνεται για να απολύσει τον κακόβουλο λογισμικό.
● 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. Το αρχείο καταγραφής παρέχεται σε μορφή .xml και μπορεί να αποθηκευτεί τοπικά κάνοντας κλικ στο κουμπί Αποθήκευση αρχείου καταγραφής και, στη συνέχεια, επιλέγοντας μια θέση αποθήκευσης.

Σημαντικό
Στις περισσότερες περιπτώσεις 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 κακόβουλου λογισμικού από το
σύστημά σας” (p. 236).

Έλεγχος ανίχνευσης αρχείων καταγραφής

Κάθε φορά που γίνεται μια σάρωση, δημιουργείται ένα αρχείο καταγραφής
tης 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
tον 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. Κάντε κλικ στο εικονίδιο Ω στην αριστερή μπάρα του Bitdefender
interface.

2. Στην καρτέλα All επιλέξτε την ειδοποίηση που αφορά την τελευταία
σάρωση.

Εδώ μπορείτε να βρείτε όλα τα κακόβουλα προγράμματα εκδηλώσεων
σάρωσης, συμπεριλαμβανομένων των απειλών που εντοπίστηκαν από
την κατά την πρόσβαση σάρωση, σαρώσεις που ενεργοποιήθηκαν από
το χρήστη και τροποποιήσεις κατάστασης για τις αυτόματες σαρώσεις.

3. Στη λίστα ειδοποιήσεων, μπορείτε να ελέγξετε τις σαρώσεις που έχουν
dιεξαχθεί πρόσφατα. Κάντε κλικ σε μια ειδοποίηση για να δείτε
λεπτομέρειες σχετικά με αυτή.

4. Για να ανοίξετε ένα αρχείο καταγραφής της σάρωσης, κάντε κλικ στο
VIEW LOG.

Αυτόματη σάρωση των αφαιρούμενων μέσων

Το Bitdefender ανιχνεύει αυτόματα πότε συνδέετε μια αφαιρούμενη
συσκευή αποθήκευσης στον υπολογιστή σας και τη σαρώνει στο παρασκήνιο
όταν είναι ενεργοποιημένη η επιλογή Autoscan. Αυτό συνιστάται
προκειμένου να εμποδιστούν ιοί και άλλα κακόβουλα προγράμματα από
to να μολύνουν τον υπολογιστή 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 κακόβουλο λογισμικό στο παρασκήνιο (με την
προυπόθεση ότι η αυτόματη σάρωση είναι ενεργοποιημένη για αυτό το
είδος της συσκευής). Το Bitdefender εικονίδιο σάρωσης θα εμφανιστεί
στην περιοχή ειδοποιήσεων. Μπορείτε να κάνετε κλικ σε αυτό το εικονίδιο
gια να ανοίξετε το παράθυρο σάρωσης και να δείτε την πρόοδο της
σάρωσης.

Αν o Αυτόματος πιλότος είναι ενεργοποιημένος, δεν θα ενοχληθείτε
σχετικά με τη σάρωση. Η σάρωση απλά θα καταγραφεί και οι πληροφορίες
σχετικά με αυτήν θα είναι διαθέσιμες στο παράθυρο Notifications.
Αν o Αυτόματος πιλότος είναι απενεργοποιημένος:
1. θα ενημερωθείτε από ένα αναδυόμενο παράθυρο για την σύνδεση νέας
συσκευής και την σάρωσή της.
2. Στις περισσότερες περιπτώσεις, το Bitdefender καταργεί αυτόματα το
εντοπισμένο κακόβουλο λογισμικό 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.

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

Αυτή η πληροφορία μπορεί να σας είναι χρήσιμη:

- Παρακαλώ να είστε προσεκτικοί όταν χρησιμοποιείτε μολυσμένα από κακόβουλο λογισμικό CD / DVD, καθώς το κακόβουλο λογισμικό δεν μπορεί να αφαιρεθεί από το δίσκο (το μέσο αποθήκευσης είναι μόνο για ανάγνωση). Βεβαιωθείτε η σε πραγματικό χρόνο προστασία είναι ενεργοποιημένη για να αποτρέψετε τη διάδοση κακόβουλου λογισμικού 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 αντιμετώπισετε το κακόβουλο λογισμικό, ανατρέξτε στο "Αφαίρεση κακόβουλου λογισμικού από το σύστημά σας" (p. 236).

Διαχείριση σάρωσης αφαιρούμενων μέσων

Για να διαχειριστείτε την αυτόματη σάρωση των αφαιρούμενων μέσων:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS.
4. Επιλέξτε την καρτέλα ΜΟΝΑΔΕΣ ΚΑΙ ΣΥΣΚΕΥΕΣ.

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 πάει στην καραντίνα. Εάν αποτύχουν και ο 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.

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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Advanced.
3. Κάντε κλικ στους αντίστοιχους διακόπτες ON/OFF.

Διαμόρφωση εξαιρέσεων σάρωσης.

Το Bitdefender επιτρέπει την εξαίρεση συγκεκριμένων αρχείων, φακέλων ή επεκτάσεων αρχείων από τη σάρωση. Αυτή η λειτουργία έχει σκοπό να αποφεύγουν 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 ισχύουν για την κατά την πρόσβαση σάρωση, για την κατόπιν αιτήματος σάρωση μόνο, ή και για τις δύο. Τα
αντικείμενα που εξαιροúνται από την κατά την πρόσβαση σάρωση δεν θα πρόκειται να σαρωθούν, είτε τα προσπελάζετε εσείς είτε μία εφαρμογή,

Σημείωση
Οι εξαιρέσεις ΔΕΝ θα σηκώνουν για σάρωση συστήματος και των συναφών σαρώσεων. Η σάρωση του συστήματος κατά παραγγελία σας δίνει τη δυνατότητα να αναλύσετε ολόκληρο το σύστημα για κακόβουλες απειλές που θέτουν σε κίνδυνο την ασφάλεια των δεδομένων σας. 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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS
4. Επιλέξτε την καρτέλα Εξαιρέσεις.
5. Κάντε κλικ στο List of files and folders excluded from scanning. Στο παράθυρο εμφανίζεται, μπορείτε να διαχειριστείτε τα αρχεία και τους φακέλους που εξαιρούνται από τη σάρωση.
6. Προσθήκη εξαιρέσεων, ακολουθώντας αυτά τα βήματα:
   a. Κάντε κλικ στο κουμπί ADD.
   b. Κάντε κλικ στο Browse, επιλέξτε το αρχείο ή το φάκελο που θέλετε να εξαιρεθεί από τη σάρωση και, στη συνέχεια, κάντε κλικ στο κουμπί OK. Εναλλακτικά, μπορείτε να πληκτρολογήσετε (ή να κάνετε αντιγραφή και επικόλληση) τη διαδρομή του αρχείου ή του φακέλου στο πεδίο επεξεργασίας.
   c. Από προεπιλογή, το επιλεγμένο αρχείο ή ο φάκελος εξαιρείται και από την on-access και από την on-demand σάρωση. Για να κάνετε αλλαγές όταν εφαρμόζετε τον αποκλεισμό, επιλέξτε μία από τις άλλες επιλογές.
   d. Κάντε κλικ στο Προσθήκη.
Εξαιρώντας επεκτάσεις από τη σάρωση

Όταν εξαιρείτε μια επέκταση αρχείου από τη σάρωση, το Bitdefender δεν θα σαρώνει πλέον τα αρχεία με αυτή την επέκταση, ανεξάρτητα από τη θέση τους στον υπολογιστή 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 επεκτάσεις από τη σάρωση, επειδή οι αποκλεισμοί αναζήτησης μπορούν να κάνουν τον υπολογιστή σας ευάλωτο σε κακόβουλο λογισμικό.

Για να εξαιρέσετε επεκτάσεις αρχείων από τη σάρωση:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS.
4. Επιλέξτε την καρτέλα Εξαιρέσεις.
5. Κάντε κλικ στο List of extensions excluded from scanning. Στο παράθυρο που εμφανίζεται, μπορείτε να διαχειριστείτε τις επεκτάσεις αρχείων που εξαιρούνται από τη σάρωση.
6. Προσθήκη εξαιρέσεων, ακολουθώντας αυτά τα βήματα:
   a. Κάντε κλικ στο κουμπί ADD.
   b. Εισάγετε τα extensions που θέλετε να εξαιρεθούν από τη σάρωση, χωρίζοντας τα με ένα ερωτηματικό (;). Εδώ είναι ένα παράδειγμα:
      txt;avi;jpg
   c. Από προεπιλογή, όλα τα αρχεία με τις καθορισμένες επεκτάσεις αποκλείονται και από την on-access και από την on-demand σάρωση. Για να κάνετε αλλαγές όταν εφαρμόζετε τον αποκλεισμό, επιλέξτε μία από τις άλλες επιλογές.
   d. Κάντε κλικ στο Προσθήκη.
Διαχείριση εξαιρέσεων σάρωσης.

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

Για να διαχειριστείτε τις εξαιρέσεις σάρωσης:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS.
4. Επιλέξτε την καρτέλα Εξαιρέσεις.
5. Χρησιμοποιήστε τις επιλογές στο List of files and folders excluded from scanning για τη διαχείριση των αποκλεισμών σάρωσης.
6. Για να καταργήσετε ή να επεξεργαστείτε τις εξαιρέσεις σάρωσης, κάντε κλικ σε μία από τις διαθέσιμες συνδέσεις. Ακολουθήστε την εξής διαδικασία:
   ● Για να αφαιρέσετε μια καταχώρηση από τον πίνακα, επιλέξτε τη και κάντε κλικ στο κουμπί ΑΦΑΙΡΕΣΗ.
   ● Για να επεξεργαστείτε μια καταχώρηση από τον πίνακα, κάντε διπλό κλικ επάνω της (ή επιλέξτε την και κάντε κλικ στο κουμπί EDIT). Ένα νέο παράθυρο εμφανίζεται, όπου μπορείτε να αλλάξετε την επέκταση ή τη διαδρομή που θα αποκλειστεί και το είδος της σάρωσης από την οποία θέλετε να αποκλειστεί, όπως απαιτείται. Κάντε τις απαραίτητες αλλαγές και στη συνέχεια κάντε κλικ στο Τροποποίηση.

Διαχείριση αρχείων σε καραντίνα

Το Bitdefender απομονώνει τα αρχεία που έχουν μολυνθεί από κακόβουλα προγράμματα και που δεν μπορεί να τα καθαρίσει καθώς και τα ύποπτα αρχεία και τα τοποθετεί σε μια ασφαλή περιοχή με την ονομασία καραντίνα. Όταν ένας ιός 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.
malware της Bitdefender. Αν επιβεβαιωθεί παρουσία κακόβουλου λογισμικού, μια υπογραφή απελευθερώνεται για να επιτρέψει την αφαίρεση του κακόβουλου λογισμικού.

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

Για να ελέγξετε και να διαχειριστείτε αρχεία σε καραντίνα:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠРОВОΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS.
4. Επιλέξτε την καρτέλα Καραντίνα.
5. Τα αρχεία σε καραντίνα διαχειρίζονται αυτόματα από το Bitdefender σύμφωνα με τις προεπιλεγμένες ρυθμίσεις καραντίνας. Αν και δεν συνιστάται, μπορείτε να προσαρμόσετε τις ρυθμίσεις απομόνωσης σύμφωνα με τις προτιμήσεις σας.

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

Υποβολή ύποπτων αρχείων σε καραντίνα για περαιτέρω ανάλυση.
Κρατήστε αυτή την επιλογή ενεργοποιημένη για να στείλετε αυτόματα τα αρχεία σε καραντίνα, στα εργαστήρια της Bitdefender. Τα αρχεία-δείγματα θα πρέπει να αναλυθούν από τους ερευνητές κακόβουλου λογισμικού της Bitdefender. Αν επιβεβαιωθεί παρουσία κακόβουλου λογισμικού, μια υπογραφή απελευθερώνεται για να επιτρέψει την αφαίρεση του κακόβουλου λογισμικού.

Διαγραφή περιεχομένου παλαιότερου από 30 ημέρες.
Από προεπιλογή, αρχεία σε καραντίνα μεγαλύτερα από 30 ημέρες διαγράφονται αυτόματα. Αν θέλετε να αλλάξετε αυτό το χρονικό διάστημα, πληκτρολογήστε μια νέα τιμή στο αντίστοιχο πεδίο. Για να απενεργοποιήσετε την αυτόματη διαγραφή των παλαιών αρχείων σε καραντίνα, πληκτρολογήστε 0.
6. Για να διαγράψετε ένα αρχείο σε καραντίνα, επιλέξτε το και κάντε κλικ στο κουμπί DELETE. Αν θέλετε να επαναφέρετε ένα αρχείο σε καραντίνα στην αρχική του θέση, επιλέξτε το και κάντε κλικ στο κουμπί RESTORE.

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 στον υπολογιστή, ψάχνοντας για δράσεις κακόβουλου λογισμικού. Κάθε μία από αυτές τις δράσεις βαθμολογείται και υπολογίζεται μια συνολική βαθμολογία για κάθε διαδικασία.

Ός μέτρο ασφάλειας, θα ενημερώνεστε κάθε φορά που ανιχνεύεται και αποκλείεται μια επίθεση ransomware, ακόμα και αν έχει ενεργοποιηθεί η λειτουργία αυτόματου πιλότου.

Ενεργοποιώντας ή απενεργοποιώντας το Advanced Threat Defense

Για να ενεργοποιήσετε ή να απενεργοποιήσετε το Advanced Threat Defense:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο μενού ADVANCED THREAT DEFENSE, κάντε κλικ στον διακόπτη ON/OFF.

Σημείωση

Για να διατηρήσετε το σύστημά σας προστατευμένο από ransomware και άλλες επιθέσεις κακόβουλου λογισμικού, σας συνιστούμε να διατηρείτε το Advanced Threat Defense όσο το δυνατόν περισσότερο.

Ελέγχοντας ανιχνευμένες επιθέσεις ransomware

Για να ελέγξετε τις επιθέσεις ransomware που εντοπίστηκαν από την Advanced Threat Defense:
1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο μενού ADVANCED THREAT DEFENSE, κάντε κλικ στο Προστασία από Ransomware.
4. Στο παράθυρο με την περιγραφή Advanced Threat Defense, κάντε κλικ στην επιλογή Το κατάλαβα.

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.

Ελέγχοντας υπόπτες απειλές που ανιχνεύθηκαν

Για να ελέγξετε τις επιθέσεις ransomware που εντοπίστηκαν από το Advanced Threat Defense:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο μενού ADVANCED THREAT DEFENSE, κάντε κλικ στο Threat Defense.
4. Στο παράθυρο με την περιγραφή Advanced Threat Defense, κάντε κλικ στην επιλογή Το κατάλαβα.

Εμφανίζονται οι εφαρμογές που εντοπίστηκαν ως απειλές και αποκλείστηκαν τις τελευταίες 90 ημέρες. Για να βρείτε λεπτομέρειες σχετικά με την εφαρμογή, 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 αποκλείονται αν εκτελούν ενέργειες που μοιάζουν με αυτές ενός κακόβουλου λογισμικού. Το Advanced Threat Defense θα συνεχίσει να παρακολουθεί τις εφαρμογές που έχουν εξαιρεθεί.

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

Διαχείριση της ασφάλειας σας
1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ADVANCED THREAT DEFENSE.

4. Στο παράθυρο WHITELIST, κάντε κλικ στην επιλογή Προσθήκη εφαρμογών στη λίστα επιτρεπτών εφαρμογών.

5. Βρείτε και επιλέξτε την εφαρμογή που θέλετε να εξαιρέσετε και, στη συνέχεια, κάντε κλικ στο κουμπί OK.

Για να αφαιρέσετε μια καταχώρηση από τη λίστα, κάντε κλικ στο κουμπί Κατάργηση.

4.3. ΠΡΟΣΤΑΣΙΑ Web

Το Bitdefender Web Protection 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 διαμορφώσετε τις ρυθμίσεις Προστασία Web:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου WEB PROTECTION.

Κάντε κλικ στους διακόπτες για να ενεργοποιήσετε ή να απενεργοποιήσετε:
Η σάρωση του HTTP αποκλείει την κακόβουλη λειτουργία του κακόβουλου λογισμικού που προέρχεται από το Διαδίκτυο, συμπεριλαμβανομένων των λήψεων μετάδοσης.

Ο Σύμβουλος Αναζήτησης, ένα στοιχείο που βαθμολογεί τα αποτελέσματα των ερωτημάτων στη μηχανή αναζήτησής σας και τις συνδέσεις που δημιουργήθηκαν 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 δημιουργήθηκαν στις ακόλουθες διαδικτυακές υπηρεσίες κοινωνικής δικτύωσης:
- Facebook
- Twitter

- Σάρωση SSL.

Πιο εξελιγμένες επιθέσεις θα μπορούσαν να χρησιμοποιήσουν την ασφαλή κυκλοφορία στο Web για να παραπλανήσουν τα θύματά τους. Επομένως, συνιστάται να ενεργοποιήσετε την σάρωση SSL.

- Προστασία κατά της απάτης.
- Προστασία από phishing.

Μπορείτε να δημιουργήσετε μια λίστα ιστοσελίδων οι οποίες δεν θα σαρωθούν από τα προγράμματα Bitdefender antimalware, antiphishing και antifraud. Ο κατάλογος θα πρέπει να περιλαμβάνει μόνο τις ιστοσελίδες που εμπιστεύεστε πλήρως. Για παράδειγμα, προσθέστε τις ιστοσελίδες όπου χρησιμοποιείτε για τα online ψώνια σας.

Για να διαμορφώσετε και να διαχειριστείτε ιστότοπους χρησιμοποιώντας την web protection που παρέχεται από το Bitdefender:
1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Στο παράθυρο WEB PROTECTION, επιλέξτε Επιτρεπτή λίστα (Whitelist).

4. Στο πλαίσιο κειμένου Προσθήκη URL, πληκτρολογήστε το όνομα του ιστότοπου που θέλετε να προσθέσετε στη λίστα επιτρεπτών URL και στη συνέχεια κάντε κλικ στο κουμπί Προσθήκη.

Για να καταργήσετε μια ιστοσελίδα από τη λίστα, επιλέξτε τη από τη λίστα και κάντε κλικ στο σύνδεσμο Αφαίρεση.

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 την ιστοσελίδα κάνοντας κλικ Επιστροφή στην ασφάλεια.
- Προχωρήστε στην ιστοσελίδα, παρά την προειδοποίηση, κάνοντας κλικ Κατανοώ τους κινδύνους, πήγαινε με εκεί ούτως ή άλλως.

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 παρακολούθηση αναφερθείτε στο “Τα εσωτερικά των Antispam” (p. 128).

Η Προστασία Antispam του Bitdefender είναι διαθέσιμη μόνο για τους πελάτες e-mail που είναι ρυθμισμένοι για 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 σβήστονται, τότε θα σβηστέει επίσης και ο φάκελος Spam. Παράλλα αυτά, ο φάκελος Spam θα ξαναδημιουργηθεί μόλις ένα e-mail χαρακτηριστεί ως ανεπιθύμητο.
Τα εσωτερικά των Antispam

Φίλτρα προστασίας από spam

Το Bitdefender Antispam μηχανή ενσωματώνει την cloud προστασία και άλλα πολλά διαφορετικά φίλτρα που εξεσφαλίζουν 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. Χρησιμοποιώντας τον κατάλογο 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 Σύνολο χαρακτήρων

Πολλά ανεπιθύμητα μηνύματα γραμμένα σε κυριλλικά και / ή ασιατικά σύνολα χαρακτήρων. Το Φίλτρο Σύνολο χαρακτήρων ανιχνεύει τέτοιο είδος 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.

Υποστηρίζομενοι 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:

- Mozilla Thunderbird 14 ή μεταγενέστερο

Ενεργοποίηση ή απενεργοποίηση της antispam προστασίας

Η προστασία Antispam είναι ενεργοποιημένη από προεπιλογή.
Για να ενεργοποιήσετε ή να απενεργοποιήσετε τη δυνατότητα Anti Spam:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο ANTISPAM, κάντε κλικ στον διακόπτη ON/OFF.

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 να ανατρέξετε στο “Υποστηριζόμενοι πελάτες e-mail και πρωτόκολλα” (p. 129).

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 μεταφερθεί 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

To ✉️ 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 τη 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 παρακαλούμε αναφερθείτε στο “Διαμόρφωση του καταλόγου Spammers” (p. 134).
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 περιεχόμενο τους. Για περισσότερες πληροφορίες παρακαλούμε αναφερθείτε στο “Διαμόρφωση του καταλόγου φίλων” (p. 132).

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 antispam.
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 αποδεχθείτε. 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. Πηγάνετε στο φάκελο Εισερχόμενα.
3. Επιλέξτε τα μη ανιχνευθέντα spam μηνύματα

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.

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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα ANTISPAM, επιλέξτε Διαχείριση φίλων.

Για να προσθέσετε μια διεύθυνση ηλεκτρονικού ταχυδρομείου, επιλέξτε την επιλογή E-mail address εισάγετε τη διεύθυνση και πατήστε έπειτα Add. Σύνταξη: name@domain.com.

Για να προσθέσετε όλες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου από ενα συγκεκριμένο domain, επιλέξτε την επιλογή Domain name εισάγετε το όνομα του domain και πατήστε έπειτα Add. Σύνταξη: @domain.com, *domain.com και domain.com - όλα τα λαμβανόμενα 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 επιθήματα domain) θα φθάσουν στο Inbox σας ανεξάρτητα από το περιεχόμενό τους

*com - όλα τα λαμβανόμενα μηνύματα ηλεκτρονικού ταχυδρομείου που έχουν το επίθεμα com περιοχών θα φθάσουν στο Inbox σας ανεξάρτητα από το περιεχόμενό τους

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 τον κατάλογο, χτυπήστε την αντίστοιχη σύνδεση Remove. Για να διαγράψετε όλα τις καταχωρήσεις από τον κατάλογο, χτυπήστε την Clear List κουμπί.

Μπορείτε να σώσετε τον κατάλογο φίλων σε ένα αρχείο έτσι ώστε να προσθέσετε τον κρητημοποιήσετε σε έναν άλλο υπολογιστή ή μετά από 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 έναν προηγουμένως σωμενό κατάλογο φίλων, πατήστε το κουμπί Load και ανοίξτε το αντίστοιχο .bwl αρχείο. Για να επαναφέρεστε το περιεχόμενο του υπάρχοντος καταλόγου κατά τη
φόρτωση ενός προηγουμένως σωσμένου καταλόγου, επιλέξτε Overwrite current list.

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

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 στο Spammers στην Bitdefender antispatoolbar που είναι ενσωματωμένο στον client του ηλεκτρονικού σας ταχυδρομείου.

- Εναλλακτικά:
  1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
  2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
  3. Στην ενότητα ANTISPAM, επιλέξτε Διαχείριση Spammers.

Για να προσθέσετε μια διεύθυνση ηλεκτρονικού ταχυδρομείου, επιλέξτε την επιλογή E-mail address εισάγετε τη διεύθυνση και πατήστε έπειτα Add. Σύνταξη: name@domain.com.

Για να προσθέσετε όλες τις διευθύνσεις ηλεκτρονικού ταχυδρομείου από ένα συγκεκριμένο domain, επιλέξτε την επιλογή Domain name εισάγετε το όνομα του domain και πατήστε έπειτα Add. Σύνταξη:

- @domain.com, *domain.com και domain.com - όλα τα λαμβανόμενα μηνύματα ηλεκτρονικού ταχυδρομείου από το domain.com θα χαρακτηριστούν ως SPAM
- *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 προσθέτετε 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 τον κατάλογο, χτυπήστε την αντίστοιχη σύνδεση Remove. Για να διαγράψετε όλα τις καταχωρήσεις από τον κατάλογο, χτυπήστε το Clear List κουμπί.

Μπορείτε να σώσετε τον κατάλογο Spammers σε ένα αρχείο έτσι ώστε μπορείτε να τον χρησιμοποιήσετε σε έναν άλλο υπολογιστή ή μετά από επανεγκατάσταση του προϊόντος. Για να σώσετε το κατάλογο Spammers, πατήστε το κουμπί Save και σώστε τη λίστα στην επιθυμητή θέση. Το αρχείο θα έχει μία .bwl επέκταση.

Για να φορτώσετε έναν προηγουμένο κατάλογο Spammers, πατήστε το κουμπί Load και ανοίξτε το αντίστοιχο .bwl αρχείο. Για να επαναρυθμίσετε το περιεχόμενο του υπάρχοντος καταλόγου κατά τη φόρτωση ενός προηγουμένου καταλόγου, επιλέξτε Overwrite current list.

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

Διαμόρφωση των τοπικών φίλτρων antispam
Όπως περιγράφεται στο “Τα εσωτερικά των Antispam” (p. 128), το Bitdefender χρησιμοποιεί έναν συνδυασμό διαφορετικών φίλτρων antispam για να προσδιορίσει το spam. Τα φίλτρα antispam είναι προ-ρυθμισμένα για πιο 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. Κάντε κλικ στο εικονίδιο ☐ στην αριστερή μπάρα του Bitdefender 
   interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο ☐ εικονίδιο στην κάτω δεξιά γωνία του παραθύρου 
   ANTIISPAM
4. Κάντε κλικ στους αντίστοιχους διακόπτες ON/OFF.

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.

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. Κάντε κλικ στο εικονίδιο ☐ στην αριστερή μπάρα του Bitdefender 
   interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTISPAM

4. Στο παράθυρο ΡΥΘΜΙΣΕΙΣ, επιλέξτε τις επιθυμητές επιλογές.
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 antispm toolbar (συνήθως βρίσκεται στο πάνω μέρος του παραθύρου της εφαρμογής ηλεκτρονικού ταχυδρομείου) και κατόπιν στο Cloud Settings tab.

4.5. ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ (Firewall)

To Firewall (τείχος προστασίας) προστατεύει τον υπολογιστή σας από τις εισερχόμενες και εξερχόμενες προσπάθειες μη εξουσιοδοτημένης σύνδεσης, τόσο σε τοπικά δίκτυα όσο και στο Internet. 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 μη αυτόματο τρόπο τους κανόνες για εφαρμογές.

Ως μέτρο ασφάλειας, θα ενημερώνεστε κάθε φορά που αποκλείεται η πρόσβαση σε κάποιο κακόβουλο πρόγραμμα, ακόμη και αν έχει ενεργοποιηθεί η λειτουργία αυτόματου πιλότου.

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. 141).

Ενεργοποίηση ή απενεργοποίηση της firewall προστασίας

Για να ενεργοποιήσετε ή απενεργοποιήσετε το firewall:
1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο FIREWALL, κάντε κλικ στον διακόπτη ON/OFF.

Προειδοποίηση
Επειδή εκθέτει τον υπολογιστή σας σε μη εξουσιοδοτημένες συνδέσεις, η παενεργοποίηση του firewall θα πρέπει να είναι μόνο ένα προσωρινό μέτρο. Επαναφέρετε το firewall σε ενέργεια το συντομότερο δυνατόν.

Διαχείριση κανόνων εφαρμογών
Για να δείτε και να διαχειριστείτε τους κανόνες του firewall που ελέγχουν την πρόσβαση των εφαρμογών σε πόρους δικτύου και του Internet:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο FIREWALL, επιλέξτε Πρόσβαση εφαρμογών.
4. Στο παράθυρο με την περιγραφή Firewall, κάντε κλικ στην επιλογή Το κατάλαβα.

Μπορείτε να δείτε τα τελευταία 15 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 προσαρμογών που διακρίνονται (Home, Office, Public ή All) στους οποίους ισχύει ο κανόνας. Οι κανόνες δημιουργούνται αυτόματα για να φιλτράρετε δικτυακή πρόσβαση μέσω του προσαρμογέα. Από προεπιλογή, οι κανόνες δημιουργούνται για κάθε δίκτυο. Μπορείτε να δημιουργήσετε με μη αυτόματο τρόπο κανόνες ή να επεξεργαστείτε υπάρχοντες κανόνες για το φιλτράρισμα δικτυακής πρόσβασης 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 διευθύνσεις 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 Κανόνα Εφαρμογής

Για να προσθέσετε έναν κανόνα εφαρμογής:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου FIREWALL.
4. Κάντε κλικ στο σύνδεσμο Προσθήκη κανόνα στο επάνω μέρος του παραθύρου ΚΑΝΟΝΕΣ.

Στην καρτέλα ΡΥΘΜΙΣΕΙΣ μπορείτε να εφαρμόσετε τις ακόλουθες αλλαγές:

- Εφαρμόστε αυτόν τον κανόνα σε όλες τις εφαρμογές. Ενεργοποιήστε αυτή την επιλογή για να εφαρμοστεί ο κανόνας σε όλες τις εφαρμογές.
- Διαδρομή προγράμματος. Κάντε κλικ στο Περιήγηση (Browse) και επιλέξτε την εφαρμογή για την οποία ισχύει ο κανόνας.
**Δικαιώματα.** Επιλέξτε μια από τις διαθέσιμες εξουσιοδοτήσεις:

<table>
<thead>
<tr>
<th>Δικαιώματα</th>
<th>Περιγραφή</th>
</tr>
</thead>
<tbody>
<tr>
<td>Να θα επιτραπεί δικτυακή/Διαδικτυακή πρόσβαση στη συγκεκριμένη εφαρμογή υπό τις συγκεκριμένες συνθήκες.</td>
<td></td>
</tr>
<tr>
<td>Απορρίπτεται θα απαγορευτεί η δικτυακή/Διαδικτυακή πρόσβαση στη συγκεκριμένη εφαρμογή υπό τις συγκεκριμένες συνθήκες.</td>
<td></td>
</tr>
</tbody>
</table>

**Τύπος Δικτύου.** Επιλέξτε τον τύπο δικτύου για τον οποίο ισχύει ο κανόνας. Μπορείτε να αλλάξετε τον τύπο με το άνοιγμα αναδιπλούμενου μενού τύπου Δικτύου και την επιλογή ενός από τους διαθέσιμους τύπους από τον κατάλογο.

<table>
<thead>
<tr>
<th>Τύπος Δικτύου</th>
<th>Περιγραφή</th>
</tr>
</thead>
<tbody>
<tr>
<td>Όλα τα Δίκτυα</td>
<td>Επιτρέψτε όλη την κυκλοφορία μεταξύ του υπολογιστή και των άλλων υπολογιστών ανεξαρτήτως του τύπου του δικτύου.</td>
</tr>
<tr>
<td>Home/Office</td>
<td>Επιτρέψτε όλη την κυκλοφορία μεταξύ του υπολογιστή και των άλλων υπολογιστών στο τοπικό δίκτυο.</td>
</tr>
<tr>
<td>Δημόσια</td>
<td>Η κίνηση φιλτράρεται.</td>
</tr>
</tbody>
</table>

**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 εφαρμοστεί σε ένα συγκεκριμένο πρωτόκολλο, πληκτρολογήστε τον αριθμό που αντιστοιχεί στο πρωτόκολλο που θέλετε να ψηφίσετε στο κενό πεδίο που μπορείτε να γράψετε.
Σημείωση

● Οδηγεία. Επιλέξτε από το το μενού τη διεύθυνση κυκλοφορίας (εξερχόμενη/εισερχόμενη) για την οποία ισχύει ο κανόνας.

<table>
<thead>
<tr>
<th>Οδηγεία</th>
<th>Περιγραφή</th>
</tr>
</thead>
<tbody>
<tr>
<td>Εξερχόμενος</td>
<td>Ο κανόνας αυτός ισχύει μόνο για την εξερχόμενη κίνηση.</td>
</tr>
<tr>
<td>Εισερχόμενος</td>
<td>Ο κανόνας αυτός ισχύει μόνο για την εισερχόμενη κίνηση.</td>
</tr>
<tr>
<td>Και τα δύο</td>
<td>Ο κανόνας ισχύει και στις δύο κατευθύνσεις.</td>
</tr>
</tbody>
</table>

Στην καρτέλα ΓΙΑ ΠΡΟΧΩΡΗΜΕΝΟΥΣ μπορείτε να προσαρμόσετε τις παρακάτω 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 σύνδεσμο Επαναφορά κανόνων στο επάνω μέρος του παραθύρου ΚΑΝΟΝΕΣ.

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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου FIREWALL.
4. Επιλέξτε την καρτέλα ΤΥΠΟΣ ΔΙΚΤΥΟΥ.
5. Επιλέξτε τις ρυθμίσεις που θέλετε να εφαρμόσετε κατά τη σύνδεση με τους ακόλουθους προσαρμογείς:
   - Wi-Fi
   - Ethernet

Διαμόρφωση ρυθμίσεων για προχωρημένους

Για να διαμορφώσετε τις ρυθμίσεις για προχωρημένους του firewall:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου FIREWALL.
4. Επιλέξτε την καρτέλα Ρυθμίσεις.
Μπορούν να ρυθμιστούν οι ακόλουθες λειτουργίες:

- **Ανίχνευση σάρωσης θυρών** - ανιχνεύει και μπλοκάρει τις προσπάθειες για να ανίχνευση των ανοιχτών θυρών.

  Οι ανιχνεύσεις θυρών χρησιμοποιούνται συχνά από τους χάκερ για να ανακαλύψουν ποιες θύρες είναι ανοικτές στον υπολογιστή σας. Στη συνέχεια θα μπορούσαν να εισβάλουν στον υπολογιστή σας βρίσκοντας μια λιγότερο ασφαλή ή τρωτή θύρα.

- **Paranoid mode** - οι ειδοποιήσεις εμφανίζονται κάθε φορά που μια εφαρμογή προσπαθεί να συνδεθεί στο διαδίκτυο. Επιλέξτε Αποδοχή ή Άρνηση. Όταν η λειτουργία Paranoid Mode, οι λειτουργίες Αυτόματος πιλότος και Προφίλ απενεργοποιούνται αυτόματα. Το Paranoid Mode μπορεί να χρησιμοποιηθεί ταυτόχρονα με την Κατάσταση μπαταρίας.

- **λειτουργία Stealth** - αν μπορείτε να εντοπιστείτε από άλλους υπολογιστές. Κάντε κλικ στο Επεξεργασία stealth συνδέσεων για να επιλέξετε πότε η συσκευή σας θα μπορεί ή δεν θα μπορεί να είναι ορατή σε άλλους υπολογιστές.

- **Προεπιλεγμένη συμπεριφορά εφαρμογής** - επιτρέψτε στο Bitdefender να εφαρμόσει αυτόματες ρυθμίσεις σε εφαρμογές χωρίς καθορισμένους κανόνες. Κάντε κλικ στο Διαμόρφωση εφαρμογών για να επιλέξετε αν θα πρέπει να εφαρμόζονται 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 του υπολογιστή σας από κακόβουλα άτομα και εφαρμογές είναι να κρατήσετε ενημερωμένο το λειτουργικό σύστημα και τις εφαρμογές που χρησιμοποιείτε τακτικά. Επιπλέον, για να αποτρέψετε την μη εξουσιοδοτημένη φυσική πρόσβαση στον υπολογιστή σας, πρέπει να επιλέξετε ισχυρούς κωδικούς πρόσβασης (κωδικούς που δεν μπορεί εύκολα κάποιος να μαντέψει) για κάθε λογαριασμό χρήστη των Windows και για τα δίκτυα Wi-Fi με τα οποία συνδέεστε.
Το Bitdefender ελέγχει αυτόματα το σύστημά σας για τρωτά σημεία και σας προειδοποιεί για αυτά. Σαρώνει για τα εξής:

● παλιές εφαρμογές στον υπολογιστή σας.
● ενημερώσεις των Windows που λείπουν.
● αδύναμοι κωδικοί πρόσβασης για λογαριασμούς χρηστών των Windows.
● Μη ασφαλή ασύρματα Δίκτυα και routers.

To 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.

Σάρωση του συστήματός σας για ευπάθειες

Για να διορθώσετε τα τρωτά σημεία του συστήματος, χρησιμοποιώντας την επιλογή Σάρωση ευπάθειας:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε το κουμπί ΕΛΕΓΧΟΣ ΕΥΠΑΘΕΙΑΣ.
3. Περιμένετε για το Bitdefender να ελέγξει το σύστημα σας για ευπάθειες. Για να διακόψετε τη διαδικασία της σάρωσης, κάντε κλικ στο κουμπί Παράβλεψη στο επάνω μέρος του παραθύρου.

Κρίσιμα Microsoft Updates

Κάντε κλικ στο κουμπί Προβολή Λεπτομερειών για να δείτε τη λίστα των κρίσιμων ενημερώσεων των Windows που δεν είναι εγκατεστημένες στον υπολογιστή σας.

Για να ξεκινήσετε την εγκατάσταση των επιλεγμένων ενημερώσεων, κάντε κλικ στο Εγκατάσταση ενημερώσεων. Παρακαλώ σημειώστε ότι μπορεί να χρειαστεί λίγο χρόνο για να εγκαταστήσετε τις
ενημερώσεις και κάποιες από αυτές μπορεί να χρειαστούν επανεκκίνηση του συστήματος για να ολοκληρωθεί η εγκατάσταση. Εάν είναι απαραίτητο, κάντε επανεκκίνηση του συστήματος σας όσο το δυνατόν συντομότερα.

● Ανανεώσεις Εφαρμογών

Εάν μια εφαρμογή δεν είναι ενημερωμένη, κάντε κλικ στο σύνδεσμο Λήψη νέας έκδοσης για να κατεβάσετε την τελευταία έκδοση.

Κάντε κλικ στο κουμπί Προβολή Λεπτομερειών για να δείτε πληροφορίες σχετικά με την εφαρμογή που πρέπει να ενημερωθεί.

● Αδύναμοι κωδικοί πρόσβασης του λογαριασμού των Windows

Μπορείτε να δείτε τη λίστα με τους λογαριασμούς χρηστών των Windows που έχουν ρυθμιστεί στον υπολογιστή σας και το επίπεδο της προστασίας που παρέχουν οι κωδικοί πρόσβασής τους.

Κάντε κλικ στην επιλογή Αλλαγή κωδικού πρόσβασης κατά τη σύνδεση για να ορίσετε έναν νέο κωδικό πρόσβασης για το σύστημά σας.

Κάντε κλικ στο κουμπί Προβολή Λεπτομερειών για να τροποποιήσετε τους αδύναμους κωδικούς 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 έναν ισχυρό κωδικό πρόσβασης, χρησιμοποιήστε ένα συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμούς και ειδικούς χαρακτήρες (όπως #, $ ή @).

● Ασθενή δίκτυα Wi-Fi

Κάντε κλικ στο View details για να μάθετε περισσότερα σχετικά με το ασύρματο δίκτυο στο οποίο είστε συνδεδεμένοι. Συνιστάται να ορίσετε έναν ισχυρότερο κωδικό πρόσβασης για το δίκτυο του σπιτιού σας, κάντε κλικ στον ανάλογο σύνδεσμο.

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.

Στη δεξιά-πάνω γωνία του παραθύρου μπορείτε να φιλτράρετε τα αποτελέσματα σύμφωνα με τις προτιμήσεις σας.
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 Notifications.

Για να ελέγξετε και να διορθώσετε θέματα που ανιχνεύτηκαν:

1. Κάντε κλικ στο εικονίδιο ☐ στην αριστερή μπάρα 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 στην επιλογή INSTALL.
   - Εάν η αυτόματη ενημέρωση των Windows είναι απενεργοποιημένη, κάντε κλικ στην επιλογή ENABLE.
   - 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 αδύναμο κωδικό πρόσβασης, κάντε κλικ στο CHANGE PASSWORD για να αναγκάσετε τον χρήστη να αλλάξει τον κωδικό πρόσβασης στην επόμενη σύνδεσή ή για να αλλάξετε εσείς τον κωδικό πρόσβασης. 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 FIX για να την απενεργοποιήσετε.
   - Εάν ο router σας έχει διαμορφωθεί 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 WIFI SETTINGS.

Για να διαμορφώσετε τις ρυθμίσεις παρακολούθησης ευπάθειας:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο ΕΥΠΑΘΕΙΑ, κάντε κλικ στον διακόπτη ON / OFF.

Σημαντικό
Για να ενημερώνετε αυτόματα σχετικά με τις ευπάθειες του συστήματος ή της εφαρμογής, κρατήστε την επιλογή Vulnerability ενεργοποιημένη.

4. Επιλέξτε τις ευπάθειες του συστήματος που θέλετε να ελέγχονται τακτικά, χρησιμοποιώντας τους αντίστοιχους διακόπτες.

Κρίσιμα Microsoft 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. Λημμένες εφαρμογές μπορούν να αξιοποιηθούν από κάκοβουλο λογισμικό, κάνοντας τον υπολογιστή σας ευάλωτο σε εξωτερικές επιθέσεις.

Αδύναμοι 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 @).

Αυτόματη έναρξη Media
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 ενημερώσεις**

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 περισσότερα αποτελέσματα ασύρματα δίκτυα δεν είναι ασφαλή, επιτρέποντας το στα αδιάκριτα βλέμματα των χάκερ να έχουν πρόσβαση στις δεδομένα σας.

**Σημείωση**

Εάν απενεργοποιήσετε την παρακολούθηση μιας συγκεκριμένης δυναμικής ευπάθειας, θέματα που σχετίζονται με αυτή, δεν θα καταγράφονται στο παράθυρο Συμβάντα.

**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 διαρρέεται η πληροφορία μέσω του δικτύου.

Τα δεδομένα προσωπικού χαρακτήρα νούνται 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, κοινωνικών δικτύων 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 κρυπτογραφημένων 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 Safepay™ με την δυνατότητα Wi-Fi Hotspot ενεργοποιημένη.

Το Bitdefender Wi-Fi Security Advisor δίνει πληροφορίες σχετικά με:

- Οικιακά 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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ΕΥΠΑΘΕΙΑ.
4. Στο παράθυρο ΡΥΘΜΙΣΕΙΣ, επιλέξτε τον αντίστοιχο ON/OFF διακόπτη.

Διαμόρφωση οικιακού Wi-Fi δικτύου

Για να ξεκινήσετε τη ρύθμιση του οικιακού σας δικτύου:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα ΕΥΠΑΘΕΙΑ, επιλέξτε Wi-Fi Security Advisor.
4. Στην καρτέλα Ηομε Φι-Φι, κάντε κλικ στο κουμπί ΕΠΙΛΕΞΤΕ ΗΟΜΕ 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.

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 το Web Protection έχουν ενεργοποιηθεί:
  - Σάρωση SSL
  - 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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα ΕΥΠΑΘΕΙΑ, επιλέξτε Wi-Fi Security Advisor.
4. Ανάλογα με τις πληροφορίες που χρειάζεστε, επιλέξτε μία από τις δύο καρτέλες, Home Wi-Fi ή Public 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 σπουδαίοτήτά 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 εγκληματικούς 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.

Κρατήστε την επιλογή Notify ενεργοποιημένη για να λαμβάνετε ειδοποιήσεις κάθε φορά που το σύστημά σας συνδέεται σε αυτό το δίκτυο.

4.7. Προστασία για webcam

Το ότι οι χάκερ μπορούν να πάρουν τον έλεγχο την κάμερας σας για να σας κατασκοπεύουν 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, ακόμα κι αν έχει ενεργοποιηθεί η λειτουργία αυτόματου πιλότου.

Ενεργοποίηση ή απενεργοποίηση της προστασίας της Webcam

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο ΠΡΟΣΤΑΣΙΑ WEBCAM, κάντε κλικ στον διακόπτη ON/ OFF.

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. Κάντε κλικ στο εικονίδιο ☑ στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Κάντε κλικ στο εικονίδιο ☑ στην κάτω δεξιά γωνία του παραθύρου ΠΡΟΣΤΑΣΙΑ WEBCAM.

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 εξαρτούνται από αυτήν τη ρύθμιση.

- Ορίστε την πρόσβαση στην κάμερα με βάση τις επιλογές των Bitdefender χρηστών - εάν η πλειοψηφία των Bitdefender χρηστών θεωρούν μια δημοφιλή εφαρμογή ως αβλαβή, τότε η πρόσβασή της στην κάμερα web θα είναι αυτόματα ρυθμισμένη στο Επιτρέπεται. 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 αποκλείεται από την πλειοψηφία των Bitdefender χρηστών, ακόμη και αν έχει ενεργοποιηθεί η λειτουργία αυτόματου πιλότου.

Ειδοποίησης

- Ειδοποίηση όταν οι επιτρεπόμενες εφαρμογές συνδέονται με την κάμερα web - θα ειδοποιηθείτε κάθε φορά που μια επιτρεπόμενη εφαρμογή αποκτά πρόσβαση στην κάμερα web, ακόμα και αν έχει ενεργοποιηθεί η λειτουργία αυτόματου πιλότου.

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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο ΠΡΟΣΤΑΣΙΑ WEB, επιλέξτε Πρόσβαση στη Webcam.
4. Στο παράθυρο με την περιγραφή της λειτουργίας Προστασία Webcam, κάντε κλικ στο σύνδεσμο Έναρξη προσθήκης εφαρμογών στη λίστα πρόσβασης διαδικτυακής κάμερας.
5. Μεταβείτε στο αρχείο .exe που θέλετε να προσθέσετε στη λίστα και, στη συνέχεια, κάντε κλικ στο κουμπί OK.
6. Κάντε κλικ στο διακόπτη πρόσβασης Επιτρέπεται/Αποκλεισμένη πρόσβαση.

Για να δείτε τι έχουν επιλέξει οι άλλοι Bitdefender χρήστες για την επιλεγμένη εφαρμογή, κάντε κλικ στο εικονίδιο.

Για να προσθέσετε επιπλέον εφαρμογές, κάντε κλικ στη σύνδεση Προσθήκη νέας εφαρμογής στη λίστα.

Οι εφαρμογές που θα ζητήσουν πρόσβαση στην κάμερά σας μαζί με την ώρα της τελευταίας δραστηριότητας θα εμφανιστούν σε αυτό το παράθυρο.

Θα ειδοποιείστε κάθε φορά που μία από τις επιτρεπόμενες εφαρμογές αποκλείεται από τους Bitdefender χρήστες, ανεξάρτητα από το status του αυτόματου πιλότου.

Σημείωση
Καθώς οι εφαρμογές των Windows Store εκτελούνται με μία και μοναδική διαδικασία, κάθε φορά που η πρόσβαση σε μία από τις εφαρμογές της ορίζεται ως "Επιτρέπεται" ή "Αποκλεισμός", ο κανόνας θα εφαρμοστεί σε ολόκληρο το σύστημα. O Internet Explorer και ο Microsoft Edge είναι δύο παραδείγματα τέτοιων εφαρμογών.

4.8. Ασφαλή Αρχεία
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.

Η μόλυνση μπορεί να εξαπλωθεί μέσω μηνυμάτων spam, από τη λήψη συνημμένων, ή επισκεπτόμενοι μολυσμένες ιστοσελίδες και εγκαθιστώντας κακόβουλες εφαρμογές χωρίς να ενημερώνεται ο χρήστης για το τι συμβαίνει στο σύστημά του.

Το Ransomware μπορεί να έχει μία από τις ακόλουθες συμπεριφορές εμποδίζοντας την πρόσβαση του χρήστη το σύστημά του:

● Να κρυπτογραφεί τα ευαίσθητα και προσωπικά αρχεία, χωρίς να δίνει τη δυνατότητα αποκρυπτογράφησης μέχρι να καταβληθούν οι πληρωμές από το θύμα.

● Να κλειδώνει την οθόνη του υπολογιστή και να εμφανίζει ένα μήνυμα ζητώντας χρήματα. Σε αυτή την περίπτωση, δεν υπάρχει κρυπτογραφημένο αρχείο, μόνο ο χρήστης αναγκάζεται να προχωρήσει με την πληρωμή.

● Να εμποδίζει εφαρμογές να εκτελεστούν.

Με τα Bitdefender ασφαλή αρχεία μπορείτε να προστατεύετε προσωπικά αρχεία από επιθέσεις ransomware, όπως έγγραφα, φωτογραφίες ή ταινίες.

Σημείωση
Το Advanced Threat Defense και τα Ασφαλή Αρχεία είναι δύο επίπεδα άμυνας εναντίον των ransomware. Το Advanced Threat Defense είναι το χαρακτηριστικό που σταματά τις επιθέσεις ransomware στις κρίσιμες περιοχές του συστήματός σας, ενώ τα Safe Files διασφαλίζουν ότι κανένα σημαντικό αρχείο στον υπολογιστή σας δεν θα κρυπτογραφηθεί.

Ενεργοποίηση ή απενεργοποίηση των Ασφαλών Αρχείων

Για να ενεργοποιήσετε ή να απενεργοποιήσετε τη δυνατότητα Ασφαλή Αρχεία:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Στο παράθυρο ΑΣΦΑΛΗ ΑΡΧΕΙΑ, κάντε κλικ στον διακόπτη ON/OFF.
Κάθε φορά που μια εφαρμογή θα προσπαθήσει να αποκτήσει πρόσβαση σε ένα προστατευμένο αρχείο, ένα αναδυόμενο παράθυρο Bitdefender εμφανίζεται. Μπορείτε να επιτρέψετε ή να αρνηθείτε την πρόσβαση.

**Σημείωση**
Η λειτουργία ασφαλών αρχείων είναι ενεργοποιημένη από προεπιλογή.

### Προστατέψτε τα προσωπικά αρχεία σας από επιθέσεις ransomware

Αν θέλετε να εγκατασταθούν τα προσωπικά αρχεία σας σε ένα καταφύγιο:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο ΑΣΦΑΛΗ ΑΡΧΕΙΑ, επιλέξτε Προστατευμένοι Φάκελοι.
4. Στο παράθυρο με την περιγραφή Ασφαλή Αρχεία, επιλέξτε το κουμπί ΠΡΟΣΤΑΣΙΑ ΠΕΡΙΣΣΟΤΕΡΩΝ ΦΑΚΕΛΩΝ.
5. Επιλέξτε το φάκελο που θέλετε να προστατεύσετε και στη συνέχεια κάντε κλικ στο κουμπί OK.

Για να προσθέσετε επιπλέον φακέλους, κάντε κλικ στο σύνδεσμο Προστασία περισσότερων φακέλων. Εναλλακτικά, μεταφέρετε φακέλους σε αυτό το παράθυρο.

Από προεπιλογή, οι φάκελοι Εικόνες, Βίντεο, Μουσική, Επιφάνεια εργασίας και Λήψεις προστατεύονται από επιθέσεις απειλής. Τα προσωπικά δεδομένα που αποθηκεύονται σε ηλεκτρονικές υπηρεσίες φιλοξενίας αρχείων, όπως το Box, Dropbox, το Google Drive, και OneDrive περιλαμβάνονται επίσης στην προστασία, υπό την προϋπόθεση ότι οι εφαρμογές τους είναι εγκατεστημένες στο σύστημα.

Για να αποφύγετε την επιβράδυνση του συστήματος, σας συνιστούμε να προσθέσετε το πολύ 30 φακέλους ή να αποθηκεύσετε πολλά αρχεία σε έναν μόνο φάκελο.

**Σημείωση**
Οι προσαρμοσμένοι φάκελοι προστατεύονται μόνο για τους τρέχοντες χρήστες. Τα αρχεία συστήματος και εφαρμογών δεν μπορούν να προστεθούν στις εξαιρέσεις.
Ρύθμιση πρόσβασης 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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο ΑΣΦΑΛΗ ΑΡΧΕΙΑ, επιλέξτε Πρόσβαση εφαρμογών.
4. Εφαρμογές που έχουν ζητήσει να αλλάξουν αρχεία στους προστατευμένους φακέλους σας θα εμφανιστούν εδώ. Κάντε κλικ στο διακόπτη Επέτρεψε που βρίσκεται δίπλα στην εφαρμογή για την οποία είστε σίγουρος ότι είναι ασφαλής.

Στο ίδιο παράθυρο μπορείτε να απενεργοποιήσετε την προστασία ransomware για συγκεκριμένες εφαρμογές κάνοντας κλικ στον διακόπτη Αποκλεισμός.

Αν θέλετε να προσθέσετε νέες εφαρμογές στη λίστα, κάντε κλικ στη σύνδεση Προσθήκη νέας εφαρμογής στη λίστα.

Προστασία κατά την εκκίνηση

Είναι γνωστό ότι πολλές εφαρμογές malware είναι ρυθμισμένες να τρέχουν κατά την εκκίνηση του συστήματος, γεγονός που μπορεί να βλάψει σοβαρά ένα μηχάνημα. H Bitdefender Προστασία Χρόνου εκκίνησης σαρώνει όλες τις κρίσιμες περιοχές του συστήματος πριν από την ολοκλήρωση της φόρτωσης όλων των αρχείων, με μηδενική επίπτωση στο σύστημα.

Για να απενεργοποιήσετε την Προστασία κατά την εκκίνηση:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ΠΡΟΣΤΑΤΕΥΜΕΝΑ ΑΡΧΕΙΑ.
4. Κάντε κλικ στον διακόπτη ON/OFF.

Σημείωση
Οι εφαρμογές που έχουν προστεθεί στις εξαιρέσεις θα σαρωθούν επίσης και θα αντιμετωπιστούν ανάλογα.

4.9. Κρυπτογράφηση Αρχείου

Το Bitdefender File Encryption (κρυπτογράφηση αρχείων) σας επιτρέπει να δημιουργήσετε κρυπτογραφημένα, προστατευόμενα από κωδικό πρόσβασης λογικούς δίσκους (ή θησαυροφυλάκια- Vaults) στον υπολογιστή σας, όπου μπορείτε να αποθηκεύετε με ασφάλεια τα εμπιστευτικά και ευαίσθητα εγγράφων σας. Τα δεδομένα που αποθηκεύονται στα θησαυροφυλάκια μπορούν να προσπελαστούν μόνο από χρήστες που γνωρίζουν τον κωδικό πρόσβασης.

Ο κωδικός πρόσβασης σας επιτρέπει να ανοίξετε, αποθηκεύσετε δεδομένα και να κλείσετε ένα θησαυροφυλάκιο, διατηρώντας παράλληλα την ασφάλειά τους. Όσο είναι ανοιχτό το vault, μπορείτε να προσθέσετε νέα αρχεία, να έχετε πρόσβαση σε φακέλους ή να τα αλλάξετε.

Σε φυσικό επίπεδο το θησαυροφυλάκιο (vault) είναι ένα αρχείο αποθηκευμένο στον τοπικό σκληρό δίσκο και φέρει την επέκταση .bvd Αν και μπορεί να προσεγγιστεί το φυσικό αρχείο που αντιπροσωπεύει τους δίσκους του Vault από ένα διαφορετικό λειτουργικό σύστημα (όπως το Linux), οι πληροφορίες που είναι αποθηκευμένες σε αυτούς τους δίσκους δεν μπορούν να διαβαστούν, επειδή είναι κρυπτογραφημένες.

Τα αρχεία θησαυροφυλάκιου μπορείτε να τα διαχειριστείτε από το Bitdefender παράθυρο ή χρησιμοποιώντας το αναδυόμενο μενού των Windows και τη λογική μονάδα δίσκου που συνδέεται με το vault.

Διαχείριση Αρχείων vault

Για να διαχειριστείτε το vaults των αρχείων σας από Bitdefender, κάντε κλικ στο eικονίδιο στην αριστερή μπάρα του Bitdefender interface. Τα υφιστάμενα vaults αρχείων εμφανίζονται στην ενότητα των File Vaults.

Δημιουργία Αρχείου vault (κρύπτης ή θησαυροφυλάκια)

Για τη δημιουργία νέου vault:
1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Στην ενότητα ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΩΝ επιλέξτε το Δημιουργία File Vault.

4. Διευκρινίστε την τοποθεσία και το όνομα του αρχείου Vault.
   ● Πληκτρολογήστε το όνομα του αρχείου vault στο αντίστοιχο πεδίο.
   ● Κάντε κλικ στο Περιήγηση, επιλέξτε τη θέση του vault και αποθηκεύστε το με το επιθυμητό όνομα.

5. Επιλέξτε ένα γράμμα μονάδας δίσκου από το αντίστοιχο μενού. Όταν ανοίξετε το vault, ένας εικονικός δίσκος αντιστοιχισμένος στο επιλεγμένο γράμμα εμφανίζεται στο Ο υπολογιστή μου.

6. Αν θέλετε να αλλάξετε το προεπιλεγμένο μέγεθος (100 MB) του Vault, χρησιμοποιήστε το πάνω και κάτω βέλος από το Vault size (MB) spin box.

7. Πληκτρολογήστε τον επιθυμητό κωδικό πρόσβασης Vault στα πεδία Κωδικός και Επιβεβαίωση κωδικού. Οι κωδικοί πρόσβασης πρέπει να αποτελείται από τουλάχιστον 8 χαρακτήρες. Όποιος προσπαθεί να ανοίξει το θησαυροφυλάκιο και να αποκτήσει πρόσβαση στα αρχεία του πρέπει να πληκτρολογήσει τον κωδικό πρόσβασης.

8. Επιλέξτε Create. (Δημιουργία)
   Το Bitdefender θα σας ενημερώσει αμέσως για το αποτέλεσμα της ενέργειας. Εάν έχει παρουσιαστεί κάποιο σφάλμα, χρησιμοποιήστε το μήνυμα σφάλματος για να αντιμετωπίσετε το σφάλμα.
   Για να δημιουργήσετε γρηγορότερα ένα νέο vault, κάντε δεξί κλικ στην επιφάνεια εργασίας ή σε ένα φάκελο στον υπολογιστή σας, δείξτε στο Bitdefender > Bitdefender File Vault και επιλέξτε Δημιουργία Vault αρχείων.

**Σημείωση**
Μπορεί να είναι βολικό για να αποθηκεύσετε όλα τα αρχεία θησαυροφυλάκιου (vault files) στην ίδια θέση. Με αυτόν τον τρόπο, μπορείτε να τα βρείτε γρηγορότερα.
Εισαγωγή file vault

Για να εισάγετε ένα file vault που έχετε αποδηκεύσει οποιοδήποτε:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΩΝ επιλέξτε το Εισαγωγή Vault.
4. Αναζητήστε την τοποθεσία του vault και επιλέξτε το (το αρχείο .bvd).
5. Κάντε κλικ στο Open (άνοιγμα)

Ανοιγμα Αρχείου vault (κρύπτης ή θησαυροφυλάκια)

Για να αποκτήσετε πρόσβαση και να εργαστείτε με τα αρχεία που φυλάσσονται σε ένα θησαυροφυλάκιο, πρέπει πρώτα να ανοίξετε το θησαυροφυλάκιο. Όταν ανοίξει το χρηματοκιβώτιο, μια εικονική μονάδα δίσκου εμφανίζεται στον Υπολογιστή Μου. Η μονάδα δίσκου ψρει το γράμμα μονάδας δίσκου που εκχωρήθηκε στο θησαυροφυλάκιο. Για να ανοίξετε το vault:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
   Τα υφιστάμενα vaults αρχείων εμφανίζονται στην ενότητα των File Vaults.
2. Κάντε κλικ στο View Vaults σύνδεσμο, και στη συνέχεια επιλέξτε το vault που θέλετε να ανοίξετε.
3. Κάντε κλικ στο κουμπί Unlock και πληκτρολογήστε τον κωδικό πρόσβασης που απαιτείται.
4. Κάντε κλικ στο OK, και μετά στο Open κουμπίγια να ανοίξετε το vault σας.

Το Bitdefender θα σας ενημερώσει αμέσως για το αποτέλεσμα της ενέργειας. Εάν έχει παρουσιαστεί κάποιο σφάλμα, χρησιμοποιήστε το μήνυμα σφάλματος για να αντιμετωπίσετε και επιλύσετε το σφάλμα.

Για να ανοίξετε γρηγορότερα ένα vault, εντοπίστε στον υπολογιστή σας το .bvd αρχείο που αντιπροσωπεύει το vault που θέλετε να ανοίξετε. Κάντε δεξί κλικ στο αρχείο, δείξτε στο Bitdefender File Vault και επιλέξτε
Άνοιγμα. Πληκτρολογήστε τον κωδικό πρόσβασης που απαιτείται και στη συνέχεια κάντε κλικ στο OK.

Προσθήκη αρχείων σε Vault (θησαυροφυλάκιο)

Για να μπορέσετε να προσθέσετε αρχεία ή φακέλους σε ένα χρηματοκιβώτιο, θα πρέπει να ανοίξετε το χρηματοκιβώτιο.

Για να προσθέσετε νέα αρχεία στο vault σας:

1. Κάντε κλικ στο εικονίδιο ☐ στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο ☐ στην κάτω δεξιά γωνία του παραθύρου ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΩΝ.
4. Στο παράθυρο Ta Vault μου, επιλέξτε το vault που θέλετε να ανοίξετε.
5. Κάντε κλικ στο κουμπί Unlock και πληκτρολογήστε τον κωδικό πρόσβασης που απαιτείται.
6. Κάντε κλικ στο κουμπί Άνοιγμα για να ανοίξετε το vault σας.
7. Προσθέστε τα αρχεία ή τους φακέλους, όπως κάνετε συνήθως στα Windows (για παράδειγμα, μπορείτε να χρησιμοποιήσετε τη μέθοδο αντιγραφή -και- επικόλληση).

Για να προσθέσετε γρηγορότερα αρχεία στο vault, κάντε δεξί κλικ στο αρχείο ή στο φάκελο που θέλετε να αντιγράψετε σε ένα vault, δείξτε το Bitdefender Φάκελος Vault και κάντε κλικ στο Προσθήκη στο Αρχείο Vault.

- Εάν μόνο ένα vault είναι ανοιχτό, το αρχείο ή ο φάκελος αντιγράφεται απευθείας σε εκείνο το vault.
- Εάν αρκετά θησαυροφυλάκια είναι ανοιχτά, θα σας ζητηθεί να επιλέξετε το θησαυροφυλάκιο που θα αντιγράψετε το στοιχείο. Επιλέξτε από το μενού το γράμμα μονάδας δίσκου που αντιστοιχεί στο επιθυμητό Vault και κάντε κλικ στο OK για να αντιγράψετε το στοιχείο.

Κλείδωμα vault

Όταν τελειώσετε με την εργασία σας σε ένα θησαυροφυλάκιο αρχείων, θα πρέπει να το κλειδώσετε προκειμένου να προστατεύσετε τα δεδομένα σας. Κλειδώνοντας το vault, η αντίστοιχη μονάδα εικονικού δίσκου
εξαφανίζεται από το "Ο Υπολογιστής μου". Κατά συνέπεια, η πρόσβαση στα δεδομένα που είναι αποθηκευμένα στο θησαυροφυλάκιο είναι εντελώς αποκλεισμένη.

Για να κλειδώσετε ένα vault:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Στην ενότητα File Vaults, επιλέξτε Προβολή vaults.
3. Στο παράθυρο Τα Vault μου, επιλέξτε το vault που θέλετε να κλειδώσετε.
4. Κάντε κλικ στο κουμπί Κλείδωμα.

Το Bitdefender θα σας ενημερώσει αμέσως για το αποτέλεσμα της ενέργειας. Εάν έχει παρουσιαστεί κάποιο σφάλμα, χρησιμοποιήστε το μήνυμα σφάλματος για να αντιμετωπίσετε το σφάλμα.

Για να κλειδώσετε γρηγορότερα ένα vault, κάντε δεξιό κλικ στο .bvd που αντιπροσωπεύει το vault, επιλέξτε Bitdefender αρχείο Vault κάντε κλικ στο Κλείδωμα.

Αφαίρεση Αρχείων απο το Vault (κρύπτη ή Θησαυροφυλάκιο)

Για να καταργήσετε αρχεία ή φακέλους από ένα vault, το vault θα πρέπει να είναι ανοικτό. Για να καταργήσετε αρχεία ή φακέλους από ένα vault:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΩΝ.
4. Στο παράθυρο Τα Vault μου, επιλέξτε το vault από το οποίο θέλετε να διαγράψετε αρχεία.
5. Κάντε κλικ στο κουμπί ΞΕΚΛΕΙΔΩΣΤΕ, σε περίπτωση που είναι κλειδωμένο.
6. Κάντε κλικ στο κουμπί Άνοιγμα.
Αφαιρέστε τα αρχεία ή τους φακέλους, όπως κάνετε συνήθως στα Windows (για παράδειγμα, κάντε δεξί κλικ σε ένα αρχείο που θέλετε να διαγράψετε και επιλέξτε Διαγραφή).

Αλλαγή Κωδικού Πρόσβασης Vault (Κρύπτης ή θησαυροφυλάκιο)

Ο κωδικός πρόσβασης προστατεύει το περιεχόμενο ενός vault έναντι μη εξουσιοδοτημένης πρόσβασης. Μόνο χρήστες που γνωρίζουν τον κωδικό πρόσβασης μπορούν να ανοίξουν το θησαυροφυλάκιο και να έχουν πρόσβαση στα έγγραφα και δεδομένα που είναι αποθηκευμένα μέσα σε αυτό.

Το Vault πρέπει να είναι κλειδωμένο για να μπορέσετε να αλλάξετε τον κωδικό πρόσβασης. Για να αλλάξετε τον κωδικό πρόσβασης ενός vault:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΑΡΧΕΙΩΝ.
4. Στο παράθυρο Τα Vault μου, επιλέξτε το vault του οποίου θέλετε να αλλάξετε τον κωδικό.
5. Κάντε κλικ στο κουμπί Ρυθμίσεις.
6. Πληκτρολογήστε τον τρέχοντα κωδικό πρόσβασης του vault στο πεδίο Old Password.(Παλιός Κωδικός πρόσβασης)
7. Πληκτρολογήστε τον νέο κωδικό πρόσβασης του Vault στα πεδία Νέος κωδικός και Επιβεβαίωση Νέου Κωδικού.

Σημείωση
Οι κωδικοί πρόσβασης πρέπει να αποτελείται από τουλάχιστον 8 χαρακτήρες. Για έναν ισχυρό κωδικό πρόσβασης, χρησιμοποιήστε ένα συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμούς και ειδικούς χαρακτήρες (όπως #, $ ή @).

Το Bitdefender θα σας ενημερώσει αμέσως για το αποτέλεσμα της ενέργειας. Εάν έχει παρουσιαστεί κάποιο σφάλμα, χρησιμοποιήστε το μήνυμα σφάλματος για να αντιμετωπίσετε το σφάλμα.
Για να αλλάξετε τον κωδικό πρόσβασης ενός vault πιο γρήγορα, εντοπίστε στον υπολογιστή σας το .bvd αρχείο που εκπροσωπεί το vault. Κάντε δεξί κλικ στο αρχείο, δείξτε στο Bitdefender File Vault και επιλέξτε Change Vault Password. (Αλλαγή κωδικού πρόσβασης Vault)

4.10. Προστασία των κωδικών σας με το Διαχειριστή Κωδικών Ασφαλείας

Χρησιμοποιούμε τους υπολογιστές μας για να ψωνίσουμε on-line ή για να πληρώσουμε τους λογαριασμούς μας, για να συνδεθούμε με πλατφόρμες κοινωνικής δικτύωσης ή να συνδεθούμε με εφαρμογές άμεσων μηνυμάτων. Αλλά, όπως όλοι γνωρίζουμε, 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 χρησιμοποιήσουν 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 πρόσβασης 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
● Κωδικούς πρόσβασης 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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο WALLET, κάντε κλικ στην επιλογή Δημιουργία νέου Wallet.
4. Επιλέξτε Δημιουργία νέου.
5. Πληκτρολογήστε τις απαιτούμενες πληροφορίες στα αντίστοιχα πεδία.

● Ετικέτα Wallet - πληκτρολογήστε ένα μοναδικό όνομα για τη βάση δεδομένων Wallet.
● Βασικός Κωδικός Πρόσβασης - πληκτρολογήστε έναν κωδικό πρόσβασης για το Wallet σας.
● Πληκτρολογήστε ξανά τον κωδικό πρόσβασης - Πληκτρολογήστε ξανά τον κωδικό πρόσβασης που έχετε ορίσει.
● 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. Αν επιλέξετε Ναι, οι τραπεζικές πληροφορίες θα παραμένουν αποθηκευμένες τοπικά στη συσκευή σας. 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 αποθηκεύσει τοπικά:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο WALLET, κάντε κλικ στην επιλογή Δημιουργία νέου Wallet.
4. Επιλέξτε Από άλλη τοποθεσία.
5. Βρείτε την τοποθεσία που βρίσκεται η βάση δεδομένων του wallet και επιλέξτε το .db αρχείο,
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 από το Wallet σας:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο WALLET, κάντε κλικ στο My Wallets.

4. Επιλέξτε το εικονίδιο στο επιθυμητό wallet, και στη συνέχεια επιλέξτε ΕΞΑΓΩΓΗ.

5. Βρείτε την τοποθεσία που βρίσκεται η βάση δεδομένων του wallet και επιλέξτε το .db αρχείο.

6. Κάντε κλικ στο Αποθήκευση.

Σημείωση
Το Wallet πρέπει να ανοίξει προκειμένου η επιλογή ΕΞΑΓΩΓΗ να είναι διαθέσιμη.
Εάν το wallet που θέλετε να εξάγετε είναι κλειδωμένο, επιλέξτε το κουμπί ΕΝΕΡΓΟΠΟΙΗΣΗ WALLET, και στη συνέχεια εισάγετε τον κωδικό που είχατε δώσει όταν το είχατε δημιουργήσει.

Συγχρονίστε τα wallets σας στο cloud
Για να ενεργοποιήσετε ή να απενεργοποιήσετε το συγχρονισμό των wallets:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Στο παράθυρο WALLET, κάντε κλικ στο My Wallets.

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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Στο παράθυρο WALLLET, κάντε κλικ στο My Wallets.

4. Επιλέξτε το επιθυμητή βάση δεδομένων του Wallet από το παράθυρο ΤΑ WALLETS ΜΟΥ, και στη συνέχεια επιλέξτε ΕΝΕΡΓΟΠΟΙΗΣΗ WALLET.

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
- Websites
- 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 καταχώρηση από τον πίνακα, επιλέξτε το και κάντε κλικ στο κουμπί Επεξεργασία.

- 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:
Διαχείριση ρυθμίσεων Διαχειριστή Κωδικών Ασφαλείας

Για να ρυθμίσετε τον κύριο κωδικό πρόσβασης αναλυτικά:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο WALLET, κάντε κλικ στον διακόπτη ON/OFF.

Διαθέσιμες επιλογές:

- **ΝΑ ερωτηθώ για το βασικό μου τον κωδικό όταν συνδέομαι στον υπολογιστή μου** - Θα σας ζητηθεί να εισάγετε τον βασικό σας κωδικό όταν συνδέσετε 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.
- **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 πρόσβασης 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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου WALLET.

4. Επιλέξτε την καρτέλα Plugins.

   Επιλέξτε μια εφαρμογή για να χρησιμοποιηθεί από το Διαχειριστή Κωδικών Ασφαλείας και βελτιώστε την εμπειρία σας:
   - Microsoft Edge
   - 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 πλοήγησης σας, αυτόματα σώζονται στο Wallet.

Για να διαμορφώσετε τις ρυθμίσεις Autofill:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου WALLET.

4. Επιλέξτε την καρτέλα ΡΥΘΜΙΣΕΙΣ ΑΥΤΟΜΑΤΗΣ ΣΥΜΠΛΗΡΩΣΗΣ.

5. Ρυθμίστε τις εξής επιλογές:
   - Ρυθμίστε το πώς το Wallet ασφαλίζει τα διαπιστευτήρια σας:
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. To 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:

- Ανοίγμα Πορτοφολιού - ανοίγει το πορτοφόλι.
- Κλείδωμα Πορτοφολιού - κλειδώνει το πορτοφόλι.
4.11. 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, δεδομένων 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
αποκτήστε πρόσβαση σε έναν ιδιωτικό διαδικτυακό χώρο. Για περισσότερες πληροφορίες παρακαλούμε αναφερθείτε στο “Προστασία των κωδικών σας με το Διαχειριστή Κωδικών Ασφαλείας” (p. 164).

To Bitdefender Safepay™ προσφέρει τις ακόλουθες δυνατότητες:

● Εμποδίζει την πρόσβαση στην επιφάνεια εργασίας σας και οποιαδήποτε απόψειμα 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.
● Συνοδεύεται με ενσωματωμένη προστασία hotspot για να χρησιμοποιηθεί όταν ο υπολογιστής σας είναι συνδεδεμένος 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 ανιχνεύει όταν μεταβαίνετε σε ιστοσελίδα ηλεκτρονικών συναλλαγών ή σε ηλεκτρονικό κατάστημα με οποιοδήποτε πρόγραμμα πλοήγησης στον υπολογιστή σας και σας ζητά να εκκινήσετε το Bitdefender Safepay™.

Για να αποκτήσετε πρόσβαση στην κύρια πλατφόρμα του Bitdefender Safepay™, χρησιμοποιήστε μία από τις ακόλουθες μεθόδους:

● Από τη διεπαφή Bitdefender:

  1. Κάντε κλικ στο εικονίδιο ☺ στην αριστερή μπάρα του Bitdefender interface.
  2. Κάντε κλικ στο κουμπί 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.

**Σημείωση**
Αν το plugin Adobe Flash Player δεν έχει εγκατασταθεί ή δεν είναι πρόσφατο, θα εμφανιστεί ένα Bitdefender μήνυμα. Κάντε κλικ στο αντίστοιχο κουμπί για να συνεχίσετε.
Αφού ολοκληρωθεί η διαδικασία εγκατάστασης, θα πρέπει να ανοίξετε και πάλι χειροκίνητα το πρόγραμμα πλοήγησης Bitdefender Safepay™ για να συνεχίσετε την εργασία σας.

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 ανανέωστε τις σελίδες χρησιμοποιώντας το αντίστοιχα.
- Μπείτε στο Bitdefender 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.
Διαμόρφωση ρυθμίσεων

Κάντε κλικ ➕ και επιλέξτε Ρυθμίσεις για να ρυθμίσετε το Bitdefender Safepay™:

- Στα General Settings μπορείτε να ρυθμίσετε τα εξής:
  
  **Bitdefender Safepay™ συμπεριφορά**
  
  Επιλέξτε τι θα συμβεί, όταν μπαίνετε τακτικά στο ηλεκτρονικό κατάστημα ή στην τραπεζική ιστοσελίδα μέσω του κανονικού σας πλοηγού:
  - Αυτόματο άνοιγμα ιστοσελίδων στο Safepay.
  - Να προτείνετε η χρήση του Safepay.
  - Να μην προτείνετε η χρήση του Safepay.

- Λίστα Domains
  
  Επιλέξτε τον τρόπο που το Bitdefender Safepay™ θα συμπεριφερθεί όταν επισκέπτεστε ιστοσελίδες από συγκεκριμένα domains με τον κανονικό πλοηγό σας προσθέτοντας αυτές τις σελίδες στη λίστα των domains και επιλέγοντας την συμπεριφορά για κάθε ένα:
  - Ανοίγει αυτόματα στο Bitdefender Safepay™.
  - Αφήστε το Bitdefender να σας προτρέψει για δράση κάθε φορά.
  - Ποτέ μη χρησιμοποιείτε το Bitdefender Safepay™ όταν επισκέπτεστε μια σελίδα από το domain σε ένα κανονικό πρόγραμμα πλοήγησης.

**Αποκλεισμός αναδυόμενων παραθύρων**

Μπορείτε να επιλέξετε να αποκλείσετε τα αναδυόμενα παράθυρα κάνοντας κλικ στον αντίστοιχο διακόπτη.

ΣΗΜΕΙΩΣΗ
Για εναλλαγή μεταξύ Bitdefender Safepay™ και επιφάνεια εργασίας των Windows, πατήστε τα πλήκτρα Alt+Tab, ή κάντε κλικ στο κουμπί Minimize.
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.

**Ενεργοποίηση προστασίας Hotspot**

Μπορείτε να ενεργοποιήσετε ένα επιπλέον επίπεδο προστασίας, όταν συνδέεστε με μη ασφαλή Wi-Fi δίκτυα με ενεργοποίηση αυτής της δυνατότητας.

Μπείτε στο “Hotspot προστασία για μη ασφαλή δίκτυα” (p. 177) για περισσότερες πληροφορίες.

**Στην περιοχή Advanced Settings, οι παρακάτω επιλογές είναι διαθέσιμες:**

**Διαχειριστείτε τα 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.

Επιλέξτε Import certificates και ακολουθήστε τον οδηγό για να χρησιμοποιήσετε τα πιστοποιητικά στο Bitdefender Safepay™.

**Αυτόματη εκκίνηση Εικονικού πληκτρολόγιου σε πεδία κωδικών πρόσβασης**

Το εικονικό πληκτρολόγιο εμφανίζεται αυτόματα όταν επιλέγεται ένα πεδίο κωδικού πρόσβασης.

Χρησιμοποιήστε τον αντίστοιχο διακόπτη για να ενεργοποιήσετε ή να απενεργοποιήσετε τη λειτουργία.

**Ρωτήστε για επιβεβαίωση πριν από την εκτύπωση**

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 εικονίδιο δίπλα στη γραμμή διεύθυνσεων για να ανοίξετε τη σελίδα Σελιδοδείκτων.

2. Κάντε κλικ στο + κουμπί για να προσθέσετε ένα νέο σελιδοδείκτη.

3. Εισάγετε τη διεύθυνση URL και τον τίτλο του σελιδοδείκτη και πατήστε Δημιουργία . 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 .

Σημείωση
Η σελίδα σελιδοδείκτων 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 Δημιουργία . 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 .

Hotspot προστασία για μη ασφαλή δίκτυα

όταν χρησιμοποιείτε το Bitdefender Safepay™, ενώ συνδέεστε με ανασφαλή Wi-Fi δίκτυα (για παράδειγμα, ένα δημόσιο hotspot) η δυνατότητα προστασίας Hotspot σας προσφέρει ένα επιπλέον επίπεδο ασφάλειας Αυτή η υπηρεσία κρυπτογραφεί την επικοινωνία στο Διαδίκτυο μέσω μη ασφαλών συνδέσεων, βοηθώντας σας να διατηρήσετε τη μυστικότητά σας, σε όποιο δίκτυο και αν είστε συνδεδεμένοι.

Η προστασία Hotspot λειτουργεί μόνο αν ο υπολογιστής σας είναι συνδεδεμένος σε μη ασφαλές δίκτυο.

Η ασφαλής σύνδεση θα ξεκινήσει και ένα μήνυμα θα εμφανιστεί στο παράθυρο Bitdefender Safepay™ μόλις πραγματοποιηθεί η σύνδεση. Το σύμβολο εμφανίζεται μπροστά από τη διεύθυνση URL στη γραμμή διευθύνσεων για να σας βοηθήσει να αναγνωρίσετε εύκολα ασφαλείς συνδέσεις.
Μπορεί να χρειαστεί να αναγνωρίσετε τη ενέργεια.

4.12. Προστασία Δεδομένων

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 απαθηκευμένο 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 γρήγορα να καταστρέψετε τα αρχεία ή τους φακέλους από τον υπολογιστή σας χρησιμοποιώντας το αναδυόμενο μενού των Windows ακολουθώντας τα παρακάτω 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. Εμφανίζεται ένα παράθυρο επιβεβαίωσης. Επιλέξτε ΝΑΙ, ΔΙΑΓΡΑΦΗ για να ξεκινήσει ο οδηγός καταστροφή αρχείων. Περιμένετε να τελειώσει το Bitdefender την καταστροφή των αρχείων.
4. Τα αποτελέσματα εμφανίζονται. Επιλέξτε ΤΕΛΟΣ για να βγείτε από τον οδηγό.

Εναλλακτικά, μπορείτε να καταστρέψετε αρχεία από την οθόνη του Bitdefender με τα ακόλουθα βήματα:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα DATA PROTECTION, επιλέξτε File Shredder.
4. Ακολουθήστε τον οδηγό File Shredder:
   a. Επιλέξτε ΠΡΟΣΘΕΣΤΕ ΦΑΚΕΛΟ για να προσθέσετε τα αρχεία ή τους φακέλους που θα θέλατε να καταστραφούν μόνιμα.
Εναλλακτικά, μπορείτε να σύρετε τα αρχεία ή τους φακέλους σε αυτό το παράθυρο.

b. Επιλέξτε ΜΟΝΙΜΗ ΔΙΑΓΡΑΦΗ ΑΡΧΕΙΩΝ, 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. Επιλέξτε ΤΕΛΟΣ για να βγείτε από τον οδηγό.

4.13. ΓΟΝΙΚΟΣ ΕΛΕΓΧΟΣ

Η λειτουργία Γονικού Συμβουλού σας επιτρέπει να ελέγχετε την πρόσβαση στο Διαδίκτυο και σε ειδικές εφαρμογές για κάθε συσκευή στην οποία η δυνατότητα είναι εγκατεστημένη. Αφού έχετε ρυθμίσει το Γονικό Σύμβουλο, μπορείτε εύκολα να μάθετε τι κάνει το παιδί σας στις συσκευές που χρησιμοποιεί και που ήταν τις τελευταίες 24 ώρες. Επιπλέον, για να σας βοηθήσει να μάθετε καλύτερα τι κάνει το παιδί σας κάνει, η εφαρμογή σας δίνει στατιστικά στοιχεία σχετικά με τις δραστηριότητες και τα ενδιαφέροντά του.

Χρειάζεστε μόνο ένα υπολογιστή με πρόσβαση στο Internet και ένα πρόγραμμα περιήγησης στο web.

Μπορείτε να ρυθμίσετε τον Γονικό Σύμβουλο να αποκλείει:

- ακατάλληλες ιστοσελίδες.
- εφαρμογές, όπως παιχνίδια, άμεση συνομιλία (chat), τα προγράμματα μοιράσματος αρχείων ή άλλα.
- αποκλείει συγκεκριμένες επαφές που δεν επιτρέπεται να έρθουν σε επαφή μέσω τηλεφώνου με το παιδί σας.

Ελέγξτε τις δραστηριότητες των παιδιών σας και αλλάξτε τις ρυθμίσεις Γονικού Συμβουλού με τη χρήση του Bitdefender λογαρισμού από οποιονδήποτε υπολογιστή ή κινητή συσκευή που συνδέεται στο Διαδίκτυο.

Πρόσβαση στο Γονικό Σύμβουλο - MY CHILDREN

Μόλις αποκτήσετε πρόσβαση στην ενότητα Γονικός Σύμβουλος, το παράθυρο ΤΑ ΠΑΙΔΙΑ ΜΟΥ είναι διαθέσιμο. Εδώ μπορείτε να δείτε και να
επεξεργαστείτε όλα τα προφίλ που έχετε δημιουργήσει για τα παιδιά σας. Τα προφίλ εμφανίζονται ως κάρτες προφίλ, επιτρέποντάς σας να τις διαχειρίζεστε γρήγορα και να ελέγχετε την κατάστασή 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 του Γονικού Συμβουλίου από το Bitdefender Central από οποιονδήποτε υπολογιστή ή κινητή συσκευή που συνδέεται στο Internet.

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 την δυνατότητα Γονικός Έλεγχος.
4. Στο παράθυρο ΤΑ ΠΑΙΔΙΑ ΜΟΥ που εμφανίζεται, μπορείτε να διαχειριστείτε και να ρυθμίσετε τα προφίλ Γονικού Συμβουλίου για κάθε συσκευή.

● Από το Bitdefender περιβάλλον σας:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα Γονικός Έλεγχος, επιλέξτε Ρυθμίσεις.
   Θα μεταφερθείτε στην ιστοσελίδα του Bitdefender λογαριασμού. Βεβαιωθείτε ότι έχετε συνδεθεί με τους κωδικούς σας.
4. Επιλέξτε την δυνατότητα Γονικός Έλεγχος.
5. Στο παράθυρο ΤΑ ΠΑΙΔΙΑ ΜΟΥ που εμφανίζεται, μπορείτε να διαχειριστείτε και να ρυθμίσετε τα προφίλ Γονικού Συμβουλίου για κάθε συσκευή.
Σημείωση
Βεβαιωθείτε ότι έχετε συνδεθεί στον υπολογιστή με ένα λογαριασμό
dιαχειριστή. Μόνο οι χρήστες με δικαιώματα διαχειριστή συστήματος
μπορούν να έχουν πρόσβαση και να διαμορφώσουν το Γονικό Σύμβουλο.

Προσθέτοντας το προφίλ του παιδιού σας

Για να ξεκινήσετε την παρακολούθηση των δραστηριοτήτων του παιδιού
σας, θα πρέπει να διαμορφώσετε ένα προφίλ και να εγκαταστήσετε τον
Γονικό Σύμβουλο Bitdefender στις συσκευές που χρησιμοποιεί.

Για να προσθέσετε το προφίλ του παιδιού σας στο Γονικό Σύμβουλο:
1. Συνδεθείτε στο Parental Advisor μέσω του Bitdefender Central.
2. Κάντε κλικ στο ADD PROFILE στη δεξιά πλευρά του παραθύρου MY
CHILDREN.
3. Ορίστε συγκεκριμένες πληροφορίες στα αντίστοιχα πεδία, όπως: όνομα,
φύλο, και ημερομηνία γέννησης. Για να προσθέσετε φωτογραφία στο
προφίλ, επιλέξτε τον σύνδεσμο ΠΡΟΣΘΗΚΗ ΑΡΧΕΙΟΥ. Κάντε κλικ στο
ΕΠΟΜΕΝΟ για να συνεχίσετε.

Με βάση τα πρότυπα ανάπτυξης των παιδιών, τον καθορισμό της ηλικίας
tου παιδιού φορτώνονται οι αυτόματα προδιαγραφές που θεωρούνται
κατάλληλες για την κατηγορία της ηλικίας του.
4. Εάν η συσκευή του παιδιού σας έχει ήδη εγκατεστημένο το Bitdefender
Total Security, επιλέξτε τη συσκευή του από τη διαθέσιμη λίστα, και στη
συνέχεια επιλέξτε το λογαριασμό που θέλετε να ελέγχετε. Κάντε κλικ
στο SAVE.

Εάν το παιδί σας χρησιμοποιεί συσκευή Android ή iOS και o Bitdefender
Γονικός Έλεγχος δεν είναι εγκατεστημένος, επιλέξτε ΠΡΟΣΘΗΚΗ
ΣΥΣΚΕΥΗΣ. Εάν το παιδί σας χρησιμοποιεί μια συσκευή Mac και η
εφαρμογή Bitdefender Antivirus για Mac δεν είναι εγκατεστημένη, κάντε
κλικ στο ίδιο κουμπί. Επιλέξτε το λειτουργικό σύστημα που θέλετε να
eγκαταστήσετε την εφαρμογή και, στη συνέχεια, κάντε κλικ στο κουμπί
ΕΠΟΜΕΝΟ ΒΗΜΑ για να συνεχίσετε.

5. Πληκτρολογήστε την email διεύθυνση που θα θέλατε να λάβετε τον
σύνδεσμο λήψης και εγκατάστασης της εφαρμογής Bitdefender Γονικού
Έλεγχου, και στη συνέχεια επιλέξτε ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ
ΕΓΚΑΤΑΣΤΑΣΗΣ.
Σημαντικό
Στις συσκευές που βασίζονται στα Windows, πρέπει να λάβετε και να εγκαταστήσετε το Bitdefender Total Security που έχετε συμπεριλάβει στη συνδρομή σας.
Στις macOS συσκευές, το προϊόν Bitdefender Antivirus για Mac πρέπει να κατέβει και να εγκατασταθεί.
Σε συσκευές Android και iOS, θα πρέπει να κατεβάσετε και να εγκαταστήσετε τον Bitdefender Γονικό Σύμβουλο.

Αντιστοιχιση πολλαπλών συσκευών στο ίδιο προφίλ
Μπορείτε να αντιστοιχίσετε πολλές συσκευές στο ίδιο προφίλ, έτσι ώστε να εφαρμόζονται οι ίδιοι περιορισμοί, ως εξής:
1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε την δυνατότητα Γονικός Έλεγχος.
3. Κάντε κλικ στο εικονίδιο στην κάρτα του προφίλ που επιθυμείτε και στη συνέχεια, επιλέξτε Συσκευές.
4. Επιλέξτε από τη λίστα των συσκευών ekeinη που tha thelate na oristei stis syseuves.

Εάν το παιδί σας χρησιμοποιεί συσκευή Android ή iOS και ο Bitdefender Γονικός Έλεγχος δεν είναι εγκατεστημένος, επιλέξτε ΠΡΟΣΘΗΚΗ ΣΥΣΚΕΥΗΣ. Εάν το παιδί σας χρησιμοποιεί μια συσκευή Mac και η εφαρμογή Bitdefender Antivirus για Mac δεν είναι εγκατεστημένη, κάντε κλικ στο ίδιο κουμπί. Επιλέξτε το λειτουργικό σύστημα που θέλετε να εγκαταστήσετε την εφαρμογή και, στη συνέχεια, κάντε κλικ στο κουμπί ΕΠΟΜΕΝΟ ΒΗΜΑ για να συνεχίσετε.

Πληκτρολογήστε την email διεύθυνση που θα θέλατε να λάβετε τον σύνδεσμο λήψης και εγκατάστασης της εφαρμογής Bitdefender Γονικού Έλεγχου, και στη συνέχεια επιλέξτε ΑΠΟΣΤΟΛΗ ΣΥΝΔΕΣΜΟΥ ΕΓΚΑΤΑΣΤΑΣΗΣ.

5. Μετά την ολοκλήρωση της διαδικασίας εγκατάστασης για τη νέα συσκευή, επιλέξτε την από τη λίστα για να εφαρμόσετε το προφίλ.
6. Επιλέξτε SAVE.
Σύνδεση του Γονικού Σύμβουλου με το Bitdefender Central

Για την παρακολούθηση της ηλεκτρονικής δραστηριότητας του παιδιού σας σε Android και iOS, θα πρέπει να συνδέσετε τη συσκευή του στο Bitdefender λογαριασμό σας κάνοντας σύνδεση στο λογαριασμό σας από την εφαρμογή.

Για να συνδέσετε τη συσκευή με το Bitdefender λογαριασμό:

● Σε Android:

1. Επιλέξτε το κουμπί που εμφανίζεται στο e-mail που στέλνει ο server μας. Θα μεταφερθείτε στην Google Play Store εφαρμογή.
   
   Εάν δεν έχετε επιλέξει από το Bitdefender λογαριασμό να σταλεί ένα download link στην e-mail διεύθυνση του παιδιού σας, πηγαίνετε στο Google Play και αναζητήσετε την εφαρμογή Bitdefender Parental Advisor.

2. Επιλέξτε ΕΓΚΑΤΑΣΤΑΣΗ στο παράθυρο Bitdefender Γονικός έλεγχος και, στη συνέχεια, πατήστε ΑΠΟΔΟΧΗ αν 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. Ανοίξτε την εφαρμογή Γονικού Συμβούλου.

4. Διαβάστε την Άδεια Χρήσης Τελικού Χρήστη, και στη συνέχεια πιέστε ΣΥΝΕΧΕΙΑ.

5. Συνδεθείτε στο υπάρχοντα λογαριασμό σας Bitdefender.
   
   Αν δεν έχετε λογαριασμό, επιλέξτε να δημιουργήσετε ένα νέο λογαριασμό χρησιμοποιώντας την αντίστοιχη επιλογή.

6. Πατήστε Ενεργοποίηση πρόσβασης χρήσης και επιλέξτε το αντίστοιχο κουμπί.

7. Πατήστε Ενεργοποίηση προσβασιμότητας και επιλέξτε το αντίστοιχο κουμπί.

8. Ενεργοποιήστε τα δικαιώματα διαχειριστή συσκευής από την εφαρμογή πατώντας ACTIVATE.
   
   Αυτό θα αποτρέψει το παιδί σας από την απεγκατάσταση του Γονικού Συμβούλου.
9. Επιλέξτε ΟΛΟΚΛΗΡΩΘΗΚΕ για να ολοκληρώσετε τη διαδικασία εγκατάστασης.

Σημείωση
Σε Android 4.4 και νεότερες εκδόσεις, για να μπορείτε να παρακολουθείτε τα μηνύματα SMS του παιδιού σας, το Bitdefender χρειάζεται να αλλάξει τις ενσωματωμένες ρυθμίσεις της εφαρμογής μηνυμάτων. Σας συνιστούμε να επιλέξετε Ναι στο αναδυόμενο παράθυρο που εμφανίζεται αφού πατήσετε ΟΛΟΚΛΗΡΩΘΗΚΕ στην εφαρμογή.

● Σε iOS:
1. Επιλέξτε το κουμπί που εμφανίζεται στο e-mail που έχει σταλεί από τον server μας και στη συνέχεια εγκαταστήστε την εφαρμογή.
2. Ανοίξτε την εφαρμογή Γονικού Συμβουλίου.
3. Εμφανίζεται ένας οδηγός εισαγωγής που περιέχει λεπτομέρειες σχετικά με τις λειτουργίες του προϊόντος. Κάντε κλικ στο Επόμενο για να συνεχίσετε.
4. Συνδεθείτε στο Bitdefender λογαρισμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
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.
7. Αντιστοιχίστε την συσκευή με το προφίλ του παιδιού σας.

Παρακολούθηση δραστηριότητας του παιδιού

Το Bitdefender σας βοηθά να παρακολουθείτε τι κάνουν τα παιδιά σας στο Διαδίκτυο.

Με αυτόν τον τρόπο, μπορείτε πάντα να βρείτε ακριβώς ποιες ιστοσελίδες έχουν επισκεφθεί, ποιες εφαρμογές έχουν χρησιμοποιηθεί ή ποιες δραστηριότητες έχουν αποκλειστεί από το Γονικό Σύμβουλο. Ανάλογα με τις ρυθμίσεις που κάνετε, οι αναφορές 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 την παρακολούθηση της κίνησης στο Διαδίκτυο, τις εφαρμογές που είχε πρόσβαση ή τη δραστηριότητα του Facebook του παιδιού σας, ακολουθήστε τα παρακάτω βήματα:

1. Συνδεθείτε στο Parental Advisor μέσω του Bitdefender Central.
2. Επιλέξτε την επιθυμητή κάρτα συσκευής.

Στο παράθυρο Δραστηριότητα μπορείτε να δείτε τις πληροφορίες που σας ενδιαφέρουν. Εναλλακτικά, επιλέξτε τον σύνδεσμο Συνολική δραστηριότητα ημέρας πάνω στην ελεγχόμενη συσκευή για να μεταφέρθει στο παράθυρο της Δραστηριότητας.

Διαμόρφωση των Γενικών Ρυθμίσεων

Από προεπιλογή, όταν είναι ενεργοποιημένος ο Γονικός Σύμβουλος, οι δραστηριότητες των παιδιών σας καταγράφονται.

Για να λαμβάνετε ειδοποιήσεις μέσω ηλεκτρονικού ταχυδρομείου:

1. Συνδεθείτε στο Parental Advisor μέσω του Bitdefender Central.
2. Επιλέξτε την καρτέλα Ρυθμίσεις στην πάνω δεξιά γωνία.
3. Ενεργοποιήστε την αντίστοιχη επιλογή για να λαμβάνετε αναφορές δραστηριότητας.
4. Εισάγετε τη διεύθυνση e-mail στην οποία θα στέλνονται οι ειδοποιήσεις.
5. Λήψη ειδοποιήσεων e-mail για τα εξής:
   ● Αποκλεισμένες ιστοσελίδες
   ● Αποκλεισμένες εφαρμογές
   ● Περιοχές περιορισμένης πρόσβασης
   ● Εισερχόμενη κλήση ή SMS από έναν αποκλεισμένο αριθμό τηλεφώνου.
   ● Αφαίρεση του Γονικού Συμβουλου της εφαρμογής του Facebook
6. Κάντε κλικ στο SAVE.

Επεξεργασία ενός προφίλ

 Για να επεξεργαστείτε ένα υπάρχον προφίλ:
1. Πρόσβαση στο Bitdefender Central.
2. Επιλέξτε τον πίνακα Γονικός Σύμβουλος.
3. Κάντε κλικ στο εικονίδιο στην κάρτα του προφίλ που επιθυμείτε και στη συνέχεια, επιλέξτε Επεξεργασία.
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. Κάντε κλικ στο εικονίδιο στην κάρτα του προφίλ που επιθυμείτε και στη συνέχεια, επιλέξτε Διαγραφή.
4. Επιβεβαιώστε την επιλογή σας.

**Ρυθμίζοντας το προφίλ Γονικού Ελέγχου**

Για να ξεκινήσετε να παρακολουθείτε το παιδί σας, θα πρέπει να οριστεί ένα προφίλ σε μια συσκευή που έχει εγκατεστημένο το Γονικό Έλεγχο Bitdefender.

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 από το παράθυρο ΤΑ ΠΑΙΔΙΑ ΜΟΥ.

Κάντε κλικ σε μια καρτέλα για να διαμορφώσετε την αντίστοιχη λειτουργία Γονικού Συμβουλού για τη συσκευή:

- **Δραστηριότητα** - εμφανίζει όλες τις δραστηριότητες, τα ενδιαφέροντα, τις τοποθεσίες και τις αλληλεπιδράσεις με τους φίλους, της τρέχουσας ημέρας.
- **Εφαρμογές** - σας δίνει τη δυνατότητα να εμποδίσετε την πρόσβασή σε ορισμένες εφαρμογές, όπως παιχνίδια, λογισμικό ανταλλαγής μηνυμάτων, ταινίες, κ.λπ.
- **Websites** - σας επιτρέπει να ψηφίσετε την πλοήγηση στο Διαδίκτυο.

Διαχείριση της ασφάλειας σας
Τηλεφωνικές επαφές - εδώ μπορείτε να καθορίσετε ποιες επαφές από τη λίστα του παιδιού σας επιτρέπεται να έρθουν σε επαφή μαζί του μέσω τηλεφώνου.

Τοποθεσία παιδιού - εδώ μπορείτε να ορίσετε τις τοποθεσίες που είναι ασφαλείς ή όχι για το παιδί σας.

Κοινωνικά - σας δίνει τη δυνατότητα να εμποδίσετε την πρόσβαση σε κοινωνικά δίκτυα.

Το Χρονοδιάγραμμα - σας επιτρέπει να αποκλείσετε την πρόσβαση σε συσκευές συνδεδεμένες στο προφίλ του παιδιού σας.

Δραστηριότητα

Η καρτέλα Δραστηριότητας σας παρέχει λεπτομερείς πληροφορίες σχετικά με τις δραστηριότητες των παιδιών σας τις τελευταίες 24 ώρες, μέσα και έξω από το σπίτι. Για να δείτε τις δραστηριότητες προηγούμενων ημερών κάντε κλικ στο εικονίδιο του ημερολογίου στην πάνω αριστερή γωνία του παραθύρου.

Ανάλογα με τη δραστηριότητα, αυτό το παράθυρο μπορεί να περιλαμβάνει πληροφορίες σχετικά με:

- Τοποθεσίες - εδώ μπορείτε να δείτε τις τοποθεσίες όπου το παιδί σας βρισκόταν κατά τη διάρκεια της ημέρας.
- Ενδιαφέροντα - εδώ μπορείτε να δείτε πληροφορίες σχετικά με τις κατηγορίες δικτυακών τόπων που επισκέφθηκε το παιδί σας. Κάντε κλικ στο Ανασκόπηση ακατάλληλου περιεχομένου για να επιτρέψετε ή να αρνηθείτε την πρόσβαση σε συγκεκριμένα ενδιαφέροντα.
- Κοινωνική Αλληλεπιδράσεις - εδώ μπορείτε να δείτε τις επαφές που το παιδί σας επικοινωνεί Κάντε κλικ στην καρτέλα Τηλεφωνικές επαφές για να επιλέξετε τις επαφές που το παιδί σας θα μπορεί να επικοινωνήσει σε επαφή ή όχι.
- Εφαρμογές - εδώ μπορείτε να δείτε τις εφαρμογές που χρησιμοποιήθηκαν από το παιδί σας. Κάντε κλικ στο σύνδεσμο Review app restrictions για να επιλέξετε επαφές που το παιδί σας θα μπορεί να επικοινωνήσει σε συγκεκριμένες εφαρμογές.
- Δραστηριότητα ημέρας - εδώ μπορείτε να δείτε το χρόνο που ήταν online το παιδί σας σε όλες τις συσκευές που διαθέτει, και την τοποθεσία. Οι πληροφορίες που συλλέγονται είναι από την τρέχουσα ημέρα.

Διαχείριση της ασφάλειας σας
Εφαρμογές

Η καρτέλα Εφαρμογών σας βοηθά να αποκλείσετε οποιαδήποτε εφαρμογή από την εκτέλεση της. Παιχνίδια, μέσα ενημέρωσης και λογισμικό ανταλλαγής μηνυμάτων, καθώς και άλλες κατηγορίες λογισμικού μπορούν να αποκλειστούν με αυτό τον τρόπο.

Η λειτουργία μπορεί να ενεργοποιηθεί ή να απενεργοποιηθεί χρησιμοποιώντας τον αντίστοιχο διακόπτη.

Για να ρυθμίσετε το Application control ενός συγκεκριμένου λογαριασμού χρήστη:
1. Μια λίστα με κάρτες εμφανίζεται. Οι κάρτες αντιπροσωπεύουν τις εφαρμογές χρησιμοποιεί το παιδί σας.
2. Επιλέξτε την κάρτα με την εφαρμογή που θέλετε το παιδί σας να σταματήσει να χρησιμοποιεί.
   
   Το σύμβολο που εμφανίζεται υποδεικνύει ότι το παιδί σας δεν θα είναι σε θέση να χρησιμοποιήσει την εφαρμογή.

Websites

Το παράθυρο Websites σας βοηθά να αποκλείσετε ιστοσελίδες με ακατάλληλο περιεχόμενο. 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 το παιδί 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 σύμβολο που εμφανίζεται υποδεικνύει ότι το παιδί σας δεν θα είναι σε θέση να έχει πρόσβαση σε περιεχόμενο που σχετίζεται με μια 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 ΟΛΟΚΛΗΡΩΣΗ 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 Τηλεφωνικές Επαφές σας δίνει τη δυνατότητα να καθορίσετε ποιοι φίλοι από τη λίστα του παιδιού σας επιτρέπεται ή όχι να έρθουν σε επαφή μαζί του μέσω τηλεφώνου.

Για να αποκλείσετε την πρόσβαση του τηλεφώνου μιας επαφής, καταρχήν πρέπει να προσθέσετε στο προφίλ του παιδιού σας την android συσκευή που χρησιμοποιεί, ακολουθώντας τα παρακάτω βήματα:
1. Επιλέξτε το Parental Advisor απο το Bitdefender Central.
2. Επιλέξτε τον σύνδεσμο Εγκατάσταση Parental Advisor σε device στην επιθυμητή κάρτα.
3. Κάντε κλικ στο ΠΡΟΣΘΗΚΗ ΣΥΣΚΕΥΗΣ στο παράθυρο που εμφανίζεται.
4. Η επιλογή Bitdefender Parental Advisor για Android είναι προεπιλεγμένη. Κάντε κλικ στο ΕΠΟΜΕΝΟ για να συνεχίσετε.
5. Επιλέξτε το προφίλ του παιδιού που θέλετε να ορίσετε περιορισμούς.
6. Επιλέξτε την καρτέλα Επαφές τηλεφώνου.

Μια λίστα με κάρτες εμφανίζεται. Οι κάρτες αντιπροσωπεύουν τις επαφές από το Android smartphone του παιδιού σας.
7. Επιλέξτε την κάρτα με τον αριθμό τηλεφώνου που θέλετε αποκλείσετε.

Το σύμβολο που εμφανίζεται υποδεικνύει ότι το παιδί σας δεν θα είναι να λάβει τηλεφωνήματα από το συγκεκριμένο τηλεφωνικό αριθμό.
Για να αποκλείσετε άγνωστους αριθμούς τηλεφώνου, ενεργοποιήστε το διακόπτη Αποκλεισμός αλληλεπιδράσεων με άγνωστους (χωρίς αναγνώριση κλήσης).

Σημείωση
Οι περιορισμοί τηλεφωνικών κλήσεων μπορούν να οριστούν μόνο για συσκευές Android που έχουν προστεθεί στο προφίλ του παιδιού σας.

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 δικτυακά 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 συμβουλίου, ζητώντας να επιβεβαιωθεί ότι είναι ασφαλής. Πατώντας το πλήκτρο ΕΦΤΑΣΑ ΜΕ ΑΣΦΑΛΕΙΑ ενημερώνετε 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. Κάντε κλικ στο Συσκευές στο πλαίσιο που έχετε στο παράθυρο Τοποθεσία παιδιού.
2. Κάντε κλικ στο ΕΠΙΛΟΓΗ ΣΥΣΚΕΥΗΣ και στη συνέχεια, επιλέξτε τη συσκευή που θέλετε να διαμορφώσετε.
3. Στο παράθυρο ΠΕΡΙΟΧΕΣ, κάντε κλικ στο κουμπί ΠΡΟΣΘΗΚΗ ΠΕΡΙΟΧΗΣ.
4. Επιλέξτε το είδος της τοποθεσίας, SAFE ή RESTRICTED.
5. Πληκτρολογήστε ένα έγκυρο όνομα για την περιοχή όπου το παιδί σας έχει δικαίωμα πρόσβασης ή όχι.
6. Ορίστε το εύρος που πρέπει να εφαρμοσθεί για την παρακολούθηση από τη γραμμή ολίσθησης Ακτίνα.
7. 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 Parental Advisor.

Κοινωνικά δίκτυα
Ο Γονικός Σύμβουλος παρακολουθεί το λογαριασμό Facebook του παιδιού σας και αναφέρει τις κύριες δραστηριότητες που λαμβάνουν χώρα.

Αυτές οι διαδικτυακές δραστηριότητες ελέγχονται και θα λάβετε μια προειδοποίηση, εάν αποδειχθεί ότι είναι μια απειλή για την ιδιωτικότητα του παιδιού σας.

Τα στοιχεία του διαδικτυακού λογαριασμού που παρακολουθούνται περιλαμβάνουν:
● Πληροφορίες Λογαριασμού
● Οπως σελίδες
● Δημοσιευμένες φωτογραφίες
Гια να διαμορφώσετε την προστασία του Facebook για ένα συγκεκριμένο λογαριασμό χρήστη, πληκτρολογήστε το e-mail του λογαριασμού του παιδιού που θέλετε να παρακολουθείτε, και στη συνέχεια κάντε κλικ SEND.

Ενημερώστε το παιδί σας για τις προθέσεις σας, και ζητήστε του να κάνει κλικ στο PROTECT ACCOUNT κουμπι που έλαβε από εμάς στο e-mail του.

Για να αποκτήσετε πρόσβαση στο λογαριασμό στο Facebook που παρακολουθείτε, κάντε κλικ στο View on Facebook link.

Για να διακόψετε την παρακολούθηση του λογαριασμού στο Facebook, χρησιμοποιήστε το κουμπί UNLINK ACCOUNT από πάνω.

Για να σας ανακοινωθεί μέσω e-mail όταν το παιδί σας αφαιρεί το εφαρμογή Γονική Συμβούλου από τη συσκευή του, επιλέξτε το αντίστοιχο πλαίσιο ελέγχου.

Χρονοδιάγραμμα

Η καρτέλα Χρονοδιάγραμμα σας επιτρέπει να περιορίσετε την πρόσβαση σε συσκευές συνδεδεμένες στο προφίλ του παιδιού σας. Οι περιορισμοί μπορούν να ρυθμιστούν όποιον ώρα κατά τη διάρκεια της σχολικής φοίτησης και τα Σαββατοκύριακα μόνο για συσκευές Android και Windows.

Για να ξεκινήσετε να διαμορφώνετε τους χρονικούς περιορισμούς κατά την διάρκεια της νύχτας:

1. Στην περιοχή Ήρα Ύπνου, επιλέξτε τα Νύχτες Σχολείου και Βραδιές Σαββατοκύριακου check boxes.
2. Επιλέξτε το eikonidio από τα αντίστοιχα πεδία, και μετά χρησιμοποιήστε τα πάνω και κάτω βέλη του πληκτρολογίου για να ορίσετε τα χρονικά διαστήματα που θα θέλατε η πρόσβαση να αποκλειστεί.

Για να ξεκινήσετε να διαμορφώνετε τους χρονικούς περιορισμούς κατά την διάρκεια της ημέρας:

1. Στην περιοχή Όρια της ημέρας έχετε τις ακόλουθες επιλογές:

● ΣΩΡΕΥΤΙΚΑ
  a. Επιλέξτε τα Όρια σχολικής ημέρας and Όρια χρόνου Σαββατοκύριακου check boxes.
  b. Τραβήξτε την κλίμακα προς τα δεξιά ή αριστερά για να ορίσετε τον επιτρεπόμενο χρόνο πρόσβασης στις συσκευές.

Διαχείριση της ασφάλειας σας 192
ΣΥΓΚΕΚΡΙΜΕΝΑ

a. Επιλέξτε τα Ορια σχολικής ημέρας and Ορια χρόνου Σαββατοκύριακου check boxes.

b. Επιλέξτε από το πλέγμα τα χρονικά διαστήματα κατά τα οποία η πρόσβαση στο Διαδίκτυο θα θέλατε να είναι αποκλεισμένη.

Σημείωση
Οι ρυθμίσεις ΣΥΓΕΝΤΡΩΤΙΚΑ and ΣΥΓΚΕΚΡΙΜΕΝΑ δεν είναι σχεδιασμένες να λειτουργούν ταυτόχρονα.

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 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 επανακινδυνεύει 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 αποκτήσει 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 επανακινδυνεύει 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 οποιοδήποτε 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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο Anti-Theft κουμπί.

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:


2. Συνδεθείτε στο Bitdefender λογαρισμό χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.

3. Επιλέξτε το Οι συσκευές μου.

4. Κάντε κλικ στη συσκευή σας 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 αυτόματης εκτέλεσης που είναι ενσωματωμένη στο λειτουργικό σύστημα Windows, είναι πολύ χρήσιμο εργαλείο που επιτρέπει στους υπολογιστές να εκτελούν αυτόματα ένα αρχείο από μέσο που
συνδέονται με αυτό. Για παράδειγμα, η εγκατάσταση λογισμικού μπορεί να ξεκινήσει αυτόματα όταν τοποθετηθεί ένα CD στη μονάδα οπτικού δίσκου.

Δυστυχώς, αυτό το χαρακτηριστικό μπορεί επίσης να χρησιμοποιηθεί από κακόβουλο λογισμικό για την αυτόματη εκκίνηση και να διεισδύει στον υπολογιστή σας με δυνατότητα επανεγγραφής, όπως σε USB flash drives και κάρτες μνήμης που συνδέονται σε συσκευές ανάγνωσης καρτών. Πολυάριθμες επιθέσεις έχουν δημιουργηθεί με βάση το Autorun, τα τελευταία χρόνια.

Με USB Immunizer μπορείτε να αποτρέψετε οποιαδήποτε NTFS, FAT32 ή FAT διαμορφωμένη μονάδα flash από αυτόματα εκτέλεσης κακόβουλου λογισμικού. Μόλις μια συσκευή USB γίνει immunized, το κακόβουλο λογισμικό δεν μπορεί πλέον να ρυθμιστεί για να εκτελεί μια συγκεκριμένη εφαρμογή, όταν η συσκευή είναι συνδεδεμένη σε έναν υπολογιστή με Windows.

Για την ανοσοποίηση μια συσκευή USB:
1. Συνδέστε τον αφαιρούμενο δίσκο στον υπολογιστή σας.
2. Περιηγηθείτε στον υπολογιστή σας για να εντοπίσετε την αφαιρούμενη συσκευή αποθήκευσης και κάντε δεξί κλικ στο εικονίδιό 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 τον υπολογιστή σας από την έναρξη των κακόβουλων προγραμμάτων από συσκευές USB που δεν είναι Immunized, απενεργοποιήστε τη δυνατότητα αυτόματης εκτέλεσης των μέσων. Για περισσότερες πληροφορίες παρακολούθησε αναφερθείτε στο “Χρήση της αυτόματης παρακολούθησης ευπάθειας” (p. 146).
5. ΒΕΛΤΙΣΤΟΠΟΪΗΣΗ ΣΥΣΤΗΜΑΤΟΣ

5.1. Εργαλεία

Το Bitdefender έρχεται με μια TuneUp επέκταση που σας βοηθά να διατηρήσετε την ακεραιότητα του συστήματός σας. Τα εργαλεία συντήρησης που προσφέρονται είναι αναγκαία για τη βελτίωση της απόκρισης του συστήματος σας και την αποτελεσματική διαχείριση του χώρου στο σκληρό δίσκο.

Το Bitdefender παρέχει τα εξής PC tune-up εργαλεία:

- Το OneClick Optimizer αναλύει και βελτιώνει την ταχύτητα του συστήματός σας, εκτελόντας πολλές εργασίες με ένα μόνο κλικ.
- Το Startup Optimizer μειώνει τον χρόνο εκκίνησης του συστήματος σας, με τη διακοπή περιττών εφαρμογών, όταν ο υπολογιστής επανεκκινείται.
- Disk Cleanup προσδιορίζει τα μεγαλύτερα αρχεία και φακέλους που δεν έχουν χρησιμοποιηθεί για μεγάλο χρονικό διάστημα.

Βελτιστοποίηση της ταχύτητας του συστήματος σας με ένα μόνο κλικ

Ζητήματα όπως οι βλάβες των σκληρών δίσκων, εναπομείναντα αρχεία μητρώου και το ιστορικό του προγράμματος περιήγησης, μπορεί να επιβραδύνει την εργασία στον υπολογιστή σας, η οποία μπορεί να γίνει πρόβλημα για εσάς. Όλα αυτά μπορούν τώρα να διορθωθούν με ένα μόνο κλικ.

OneClick Optimizer σας επιτρέπει να αναγνωρίσετε και να αφαιρέσετε άρρητα αρχεία εκτελώντας ταυτόχρονα πολλαπλές εργασίες καθαρισμού. Για να ξεκινήσετε τη διαδικασία OneClick Optimizer:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο OneClick Optimizer κουμπί.
   α. Γίνεται Ανάλυση του

   Περιμένετε το Bitdefender για να ολοκληρώσει την αναζήτηση για θέματα του συστήματος.
● Disk Cleanup - εντοπίζει μεγάλα αρχεία και τους φακέλους που δεν χρησιμοποιείτε πια.
● 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.

Αν θέλετε ολοκληρωμένες πληροφορίες για τη διαδικασία βελτιστοποίησης, κάντε κλικ στο κουμπί VIEW DETAILED REPORT.

βελτιστοποίηση του χρόνου εκκίνησης του PC σας

Ο εκτεταμένος χρόνος εκκίνηση του συστήματος είναι ένα πρόβλημα που οφείλεται σε εφαρμογές που έχουν ρυθμιστεί να τρέχουν χωρίς να είναι απαραίτητες. Η αναμονή αρκετών λεπτών για την εκκίνηση ενός συστήματος μπορεί να σας κοστίσει πολύ τόπο χρόνο και παραγωγικότητα.

Το παράθυρο Startup Optimizer εμφανίζει ποιες εφαρμογές εκτελούνται κατά την εκκίνηση του συστήματος και σας επιτρέπει να διαχειριστείτε τη συμπεριφορά τους σε αυτό το σημείο.

Για να ξεκινήσετε τη διαδικασία Startup Optimizer:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο Startup Optimizer κουμπί.
   a. Επιλέξτε εφαρμογές
Μπορείτε να δείτε μια λίστα με τις εφαρμογές που εκτελούνται κατά την εκκίνηση του συστήματος. Επιλέξτε αυτά που θέλετε να απενεργοποιήσετε ή να καθυστερήσουν κατά την εκκίνηση.

b. Επιλογή Κοινότητας
Δείτε τι άλλο έχουν αποφασίσει να κάνουν οι χρήστες της Bitdefender με την εφαρμογή που έχετε επιλέξει.

c. Χρόνος εκκίνησης του συστήματος
Ελέγξτε το πεδίο κύλισης στο επάνω μέρος του παραθύρου για να δείτε το χρόνο που απαιτείται τόσο από το σύστημα σας όσο και απο τις επιλεγμένες εφαρμογές, που χρειάζονται για να τρέξουν κατά την εκκίνηση.

Μια επανεκκίνηση του συστήματος απαιτείται για να μπορούν να ανακτηθούν πληροφορίες σχετικά με το χρόνο εκκίνησης του συστήματος και των εφαρμογών.

d. Στοιχεία εκκίνησης

- **Επιτρέπω.** Επιλέξτε αυτήν την επιλογή όταν θέλετε μια εφαρμογή να ξεκινάει κατά την εκκίνηση του συστήματος. Αυτή η επιλογή είναι ενεργοποιημένη από προεπιλογή.

- **Καθυστ.** Επιλέξτε αυτήν την επιλογή για την αναβολή εκτέλεσης ενός προγράμματος κατά την εκκίνηση του συστήματος. Αυτό σημαίνει ότι οι επιλεγμένες εφαρμογές θα ξεκινήσουν με πέντε λεπτά καθυστέρηση έπειτα από την σύνδεση του χρήστη στο σύστημα. Η καθυστέρηση στην λειτουργικότητα είναι προκαθορισμένη και δεν μπορεί να ρυθμιστεί από τον χρήστη.

- **Απενεργοποίησε.** Επιλέξτε αυτήν την επιλογή για την αναβολή εκτέλεσης ενός προγράμματος κατά την εκκίνηση του συστήματος.

e. Αποτελέσματα
Πληροφορίες όπως ο εκτιμώμενος χρόνος εκκίνησης του συστήματος μετά την καθυστέρηση ή την απενεργοποίηση των προγραμμάτων εμφανίζονται.

Μια επανεκκίνηση του συστήματος μπορεί να απαιτείται για να δείτε όλες αυτές τις πληροφορίες.

Κάντε κλικ στο OK για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.
Σημείωση
Σε περίπτωση που λήξει η συνδρομή σας ή αν αποφασίσετε να απεγκαταστήσετε το Bitdefender, τα προγράμματα που έχετε προγραμματίσει να σταματήσει η εκτέλεσή τους από την εκκίνηση θα να αποκατασταθούν στις προεπιλεγμένες ρυθμίσεις εκκίνησης τους.

Βελτιστοποίηση του δίσκου σας

Περιττά αρχεία και φάκελοι που καταλαμβάνουν χώρο στο δίσκο σας μπορεί να προκαλέσουν επιβράδυνση του συστήματος. Ως εκ τούτου, συνιστάται να βελτιώσετε την ταχύτητα του συστήματός σας με τον καθαρισμό του σε τακτά χρονικά διαστήματα.

Το Bitdefender Disk Cleanup σας βοηθά να ελευθερώσετε χώρο στο δίσκο με τον εντοπισμό μεγάλων αρχείων και φακέλων που δεν χρησιμοποιείτε πια.

Για να ξεκινήσετε τον καθαρισμό του σύστημά σας:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο κουμπί Disk Cleanup.
3. Ένα παράθυρο με πληροφορίες σχετικά με το τι μπορεί να κάνει το Disk Cleanup για το σύστημά σας έτσι ώστε να κάνει χώρο για νέα δεδομένα γίνεται ορατό. Κάντε κλικ στο CONTINUE.

a. Συσκευές και Οδηγοί

Μπορείτε να δείτε μια λίστα των διαθέσιμων δίσκων. Εκτός από τους δίσκους των Windows, οι εξωτερικοί σκληροί δίσκοι και οι συσκευές USB σαρώνονται και εμφανίζονται στη λίστα. Κάντε κλικ στο VIEW για να έχετε πρόσβαση στους φακέλους που ανήκουν στην επιλεγμένη τοποθεσία. Κάντε κλικ στο SCAN από την περιοχή του δίσκου που θέλετε να καθαρίσετε.

b. Σάρωση μονάδας

Ο επιλεγμένος δίσκος αναλύεται. Περιμένετε το Bitdefender για να ολοκληρώσει την αναζήτηση για τα μεγάλα αρχεία και φακέλους.

c. Ζητήματα

Εδώ είναι όπου μπορείτε να δείτε τα αποτελέσματα της λειτουργίας χωρίσμενο σε φακέλους. Στην αριστερή πλευρά του παραθύρου, ένα
5.2. Προφίλ

Οι καθημερινές δραστηριότητες εργασίας, όπως παρακολουθώντας ταινίες ή παίζοντας παιχνίδια μπορεί να προκλήσουν επιβράδυνση του συστήματος, ειδικά αν εκτελούνται ταυτόχρονα με τις διαδικασίες ενημέρωσης των Windows και τις εργασίες συντήρησης. Με το Bitdefender, μπορείτε να επιλέξετε και να εφαρμόσετε το προτιμόμενο 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.

Ο Σύμβουλος Αναζήτησης είναι απενεργοποιημένος.

Οι ειδοποιήσεις ειδικών προσφορών είναι απενεργοποιημένες.

Ο Σύμβουλος Αναζήτησης είναι απενεργοποιημένος.

Οι ειδοποιήσεις 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 το Web Protection έχουν ενεργοποιηθεί:
  - Σάρωση SSL
  - Προστασία κατά της απάτης
  - Προστασία από phishing
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 απόδοσή του συστήματός σας. Το Προφίλ Εργασίας έχει σχεδιαστεί για να σας βοηθήσει να βελτιώσετε την αποδοτικότητα της εργασίας σας, απενεργοποιώντας κάποιες υπηρεσίες του παρασκήνιου σας και εργασίες συντήρησης.

Διαμόρφωση Προφίλ Εργασίας

Για να ρυθμίσετε τις ενέργειες που πρέπει να ληφθούν, ενώ είστε στο Προφίλ Εργασία:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Profiles.
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.

Για να προσθέσετε χειροκίνητα τις εφαρμογές στη Λίστα Εφαρμογών στο Προφίλ Εργασίας:
1. Κάντε κλικ στο εικονίδιο ☂ στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Profiles.
3. Κάντε κλικ στο κουμπί CONFIGURE στο χώρο του προφίλ εργασία.
4. Στο παράθυρο WORK PROFILE, κάντε κλικ στο σύνδεσμο Applications list.
5. Κάντε κλικ στο Προσθήκη για να προσθέσετε μια νέα εφαρμογή στη Λίστα Εφαρμογών.

Εμφανίζεται ένα νέο παράθυρο. Περιηγηθείτε στο εκτελέσιμο αρχείο της εφαρμογής, επιλέξτε το και κάντε κλικ στο OK για να το προσθέσετε στη λίστα.

**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. Κάντε κλικ στο εικονίδιο ☂ στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Profiles.
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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Profiles.
3. Κάντε κλικ στο κουμπί CONFIGURE στο χώρο του προφίλ Ταινία.
4. Στο παράθυρο MOVIE PROFILE κάντε κλικ στο σύνδεσμο Players list.
5. Κάντε κλικ στο Προσθήκη για να προσθέσετε μια νέα εφαρμογή στη Λίστα Προγραμμάτων Αναπαραγωγής.

Εμφανίζεται ένα νέο παράθυρο. Περιηγηθείτε στο εκτελέσιμο αρχείο της εφαρμογής, επιλέξτε το και κάντε κλικ στο OK για να το προσθέσετε στη λίστα.

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. Κάντε κλικ στο εικονίδιο ☀ στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Profiles.
3. Κάντε κλικ στο κουμπί CONFIGURE στο χώρο του προφίλ Παιχνίδι.
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. Κάντε κλικ στο εικονίδιο ☀ στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Profiles.
3. Κάντε κλικ στο κουμπί CONFIGURE στο χώρο του προφίλ Παιχνίδι.
4. Στο παράθυρο GAME PROFILE κάντε κλικ στο σύνδεσμο Games list.
5. Κάντε κλικ στο Προσθήκη για να προσθέσετε ένα νέο παιχνίδι στη Λίστα Παιχνιδιών.

Εμφανίζεται ένα νέο παράθυρο. Περιηγηθείτε στο εκτελέσιμο αρχείο του παιχνιδιού, επιλέξτε το και κάντε κλικ στο OK για να το προσθέσετε στη λίστα.
Προφίλ Δημόσιο Wi-Fi

Αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου, πληκτρολογήσει ευαισθητών δεδομένων ή online αγορές, ενώ συνδέονται 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 συνδέονται με μη ασφαλές ασύρματο δίκτυο:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Profiles.
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.

Προφίλ Battery Mode

Το προφίλ λειτουργία με μπαταρία είναι ειδικά σχεδιασμένο για χρήστες φορητού υπολογιστή και tablet. Ο σκοπός του είναι η ελαχιστοποίηση τόσο του συστήματος όσο και του Bitdefender σχετικά με τις επιπτώσεις στην κατανάλωση ενέργειας όταν το επίπεδο φόρτισης της μπαταρίας είναι χαμηλότερο από το επίπεδο φόρτισης της μπαταρίας επιλέξτε.

Διαμόρφωση Λειτουργίας με Μπαταρία

Για να διαμορφώσετε το προφίλ Λειτουργία με μπαταρία:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Επιλέξτε την καρτέλα Profiles.
3. Κάντε κλικ στο κουμπί **CONFIGURE** στο χώρο του προφίλ Battery mode.

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 και να λειτουργεί σε κατάσταση Battery mode. Από προσπελογή, 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.
- Ο Οδηγός Ασφαλείας έχει απενεργοποιηθεί.

Το Bitdefender ανιχνεύει όταν ο φορητός υπολογιστής σας αλλάζει σε τροφοδοσία μέσω μπαταρίας και με βάση το επίπεδο φόρτισης της μπαταρίας εισέρχεται αυτόματα σε λειτουργία μπαταρίας. Παραμοίως, το Bitdefender εξέρχεται αυτόματα από τη λειτουργία της Μπαταρίας όταν ανιχνεύει ο φορητός υπολογιστής δεν τροφοδοτείται πλέον με μπαταρία.

**Βελτιστοποίηση σε πραγματικό χρόνο**

Το Real-Time Optimization του Bitdefender είναι ένα plugin που βελτιώνει σιωπηλά στο παρασκήνιο την απόδοση του συστήματος 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 έναν υψηλότερο φορτίο, για να τις προσαρμόσει στις ανάγκες σας.
Για να ενεργοποιήσετε ή να απενεργοποιήσετε την βελτιστοποίηση σε πραγματικό χρόνο:

1. Κάντε κλικ στο εικονίδιο 🐝 στην αριστερή μπάρα του Bitdefender interface.

2. Επιλέξτε την καρτέλα Profiles.

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.
6. ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΡΟΒΛΗΜΑΤΩΝ

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.

- “Το σύστημα μου φαίνεται να είναι αργό” (p. 211)
- “Η Σάρωση δεν ξεκινάει” (p. 212)
- “Δεν μπορώ πλέον να χρησιμοποιήσω μια εφαρμογή” (p. 215)
- “Τι να κάνετε όταν το Bitdefender εμποδίζει μια ασφαλή ιστοσελίδα ή μια διαδικτυακή εφαρμογή” (p. 216)
- “Τι να κάνετε αν το Bitdefender εντοπίζει μια ασφαλή εφαρμογή ως ransomware” (p. 217)
- “Πώς να ενημερώσετε το Bitdefender σε μια αργή σύνδεση στο Internet” (p. 222)
- “Οι Υπηρεσίες του Bitdefender δεν ανταποκρίνονται” (p. 223)
- “Το Antispam φίλτρο δεν λειτουργεί σωστά” (p. 224)
- “Η λειτουργία αυτόματης συμπλήρωσης στο Πορτοφόλι μου δεν λειτουργεί” (p. 229)
- “Η αφαίρεση του Bitdefender απέτυχε” (p. 231)
- “Το σύστημα μου δεν ξεκινάει μετά την εγκατάσταση του Bitdefender” (p. 232)

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. 327).
6.1.1. Το σύστημά 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.**
  
  Αν και το Bitdefender ερευνά και αφαιρεί 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 παρακολούθηστε την ενότητα “Πώς μπορώ να καταργήσω τις άλλες λύσεις ασφάλειας;” (p. 93).

- **Οι Ελάχιστες Απαιτήσεις του Συστήματος για την εκτέλεση του Bitdefender δεν πληρούνται.**
  
  Αν το μηχάνημά σας δεν πληροί τις Ελάχιστες Απαιτήσεις του Συστήματος, ο υπολογιστής θα γίνει υποτονικός, ειδικά όταν πολλαπλές εφαρμογές εκτελούνται ταυτόχρονα. Για περισσότερες πληροφορίες παρακολούθηστε την ενότητα “Ελάχιστες απαιτήσεις συστήματος” (p. 3).

- **Έχετε εγκαταστήσει εφαρμογές που δεν χρησιμοποιείτε.**
  
  Κάθε υπολογιστής διαθέτει προγράμματα ή εφαρμογές που δεν χρησιμοποιείτε. Κατά παράλληλα, ανεπιθύμητα προγράμματα εκτελούνται στα παράσκευη 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 συσταστικό 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. Τα Spyware, οι Ιοί, τα Trojans (Δούρειοι Ίπποι) και προγράμματα διαφήμισης (adware), όλα εισπράττουν διόδια από τις επιδόσεις του υπολογιστή σας. Σιγουρευτείτε ότι σαρώνετε το σύστημά σας σε τακτά χρονικά διαστήματα, τουλάχιστον μία φορά την εβδομάδα. Συνιστάται να χρησιμοποιήσετε τη σάρωση του συστήματος του Bitdefender, γιατί σαρώνει για όλους τους τύπους κακόβουλου λογισμικού που απειλούν την ασφάλεια του συστήματός σας.

Για να ξεκινήσετε τη σάρωση του συστήματος:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα Antivirus επιλέξτε 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 παρακολουθείτε στο “Πώς μπορώ να καταργήσω τις άλλες λύσεις ασφάλειας;” (p. 93).

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 εικονίδιο 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 επικοινωνήσετε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα “Ζητήσετε βοήθεια” (p. 327).

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 προσπαθεί να χρησιμοποιήσετε.

Αυτό το status εμφανίζεται όταν το Advanced Threat Defense ανιχνεύει λάθη από χρήστες εφαρμογές ως κακόβουλες.

To Advanced Threat Defense είναι μια λειτουργία του Bitdefender που αναλύει συνεχώς τις εφαρμογές που τρέχουν στο σύστημά σας και αναφέρει ekeίna ίσως κάποιες από τις εφαρμογές ως κακόβουλες. Αυτό το status εμφανίζεται όταν το Advanced Threat Defense ανιχνεύει λάθη από χρήστες εφαρμογές ως κακόβουλες.
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 Εξαιρέσεις:

1. Κάντε κλικ στο εικονίδιο [ɪ] στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο [ο] στην κάτω δεξιά γωνία του παραθύρου ADVANCED THREAT DEFENSE.
4. Στο παράθυρο WHITELIST, κάντε κλικ στην επιλογή Προσθήκη εφαρμογών στη λίστα επιτρεπτών εφαρμογών.
5. Βρείτε και επιλέξτε την εφαρμογή που θέλετε να εξαιρέσετε και, στη συνέχεια, κάντε κλικ στο κουμπί OK.
Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήσετε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα “Ζητήσετε βοήθεια” (p. 327).

6.1.4. Τι να κάνετε όταν το Bitdefender εμποδίζει μια ασφαλή ιστοσελίδα ή μια διαδικτυακή εφαρμογή

Το Bitdefender προσφέρει μια ασφαλή εμπειρία περιήγησης στο Web ψηφιοποιώντας όλες τις κινήσεις στο Δίκτυο και εμποδίζοντας κάθε κακόβουλο περιεχόμενο. Ωστόσο, είναι πιθανό ότι το Bitdefender να θεωρήσει ότι μια ασφαλής ιστοσελίδα ή online αίτηση είναι αναασφαλής, γεγονός το οποίο θα προκαλέσει HTTP κίνηση σάρωσης του Bitdefender για να τις εμποδίσει λανθασμένα.

Σε περίπτωση που η ίδια σελίδα ή εφαρμογή μπλοκαριστεί κατ’ επανάληψη, μπορείτε να τις προσθέσετε σε μια εγκατεστημένη λίστα (whitelist), ούτως ώστε να μην σαρώνει από τις Bitdefender μηχανές, εξασφαλίζοντας έτσι μια ομαλή εμπειρία περιήγησης στο web.

Για να προσθέσετε μια ιστοσελίδα στο Whitelist:

1. Κάντε κλικ στο εικονίδιο [ɪ] στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο WEB PROTECTION, επιλέξτε Επιτρεπτή λίστα (Whitelist).
4. Δώστε τη διεύθυνση της αποκλεισμένης ιστοσελίδας ή διαδικτυακής εφαρμογής στο αντίστοιχο πεδίο και κάντε κλικ στο Προσθήκη.
5. Κάντε κλικ στο Αποθήκευση για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

Μόνο οι ιστοσελίδες και εφαρμογές που έμπιστοποιήσατε πλήρως θα πρέπει να προστατεύονται στον κατάλογο αυτό. Αυτά θα πρέπει να εξαρθρώνουν από τον έλεγχο από τις ακόλουθες μηχανές: κακόβουλο λογισμικό, phishing και απάτη.

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήσετε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα “Ζητήστε βοήθεια” (p. 327).

6.1.5. Τι να κάνετε αν το Bitdefender εντοπίζει μια ασφαλή εφαρμογή ως ransomware

Το Ransomware είναι ένα κακόβουλο πρόγραμμα που προσπαθεί να κερδίσει χρήματα από τους χρήστες κλειδώνοντας τα ευπαθή συστήματά τους. Για να διατηρήσετε το σύστημά σας ασφαλή από δυσάρεστες καταστάσεις, το Bitdefender ασφαλίσετε ότι δίνεται τη δυνατότητα να ασφαλίσετε τα προσωπικά σας αρχεία.

Όταν μια εφαρμογή προσπαθεί να αλλάξει ή να διαγράψει ένα από τα προστατευμένα αρχεία σας, θα θεωρηθεί ως μη ασφαλής και το Bitdefender θα μπλοκάρει τη λειτουργία της.

Σε περίπτωση που μια τέτοια εφαρμογή, έχει προστεθεί στην λίστα των μη αξιόπιστων εφαρμογών και να είστε σίγουροι ότι είναι ασφαλής να το χρησιμοποιήσετε, ακολουθήστε τα παρακάτω βήματα:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο ΑΣΦΑΛΗ ΑΡΧΕΙΑ, επιλέξτε Πρόσβαση εφαρμογών.
4. Εφαρμογές που έχουν ζητήσει να αλλάξουν αρχεία στους προστατευμένους φακέλους σας θα εμφανιστούν εδώ. Κάντε κλικ στο διακόπτη Επέτρεψε που βρίσκεται δίπλα στην εφαρμογή για την οποία είστε σίγουροι ότι είναι ασφαλής.
6.1.6. 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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου FIREWALL.
4. Επιλέξτε την καρτέλα Κανόνες.
5. Για να προσθέσετε έναν κανόνα εφαρμογής, κάντε κλικ στον σύνδεσμο Προσθήκη κανόνα.
6. Ένα νέο παράθυρο εμφανίζεται, όπου μπορείτε να προσθέσετε τις λεπτομέρειες. Βεβαιωθείτε ότι έχετε επιλέξει όλους τους διαθέσιμους τύπους δικτύου και στην ενότητα Αδεια 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 επικοινωνήσετε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα “Ζητήστε βοήθεια” (p. 327).

6.1.7. Δεν μπορώ να αποκτήσω πρόσβαση σε μια συσκευή στο δίκτυό μου

Ανάλογα με το δίκτυο που είστε συνδεδεμένοι, το τείχος προστασίας του Bitdefender μπορεί να εμποδίσει τη σύνδεση μεταξύ του συστήματός σας και μιας άλλης συσκευής (όπως έναν άλλο υπολογιστή ή εκτυπωτή). 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. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου FIREWALL.

4. Κάντε κλικ στο σύνδεσμο Προσθήκη κανόνα στο επάνω μέρος του παραθύρου ΚΑΝΟΝΕΣ.

5. Στο παράθυρο ΡΥΘΜΙΣΕΙΣ, ενεργοποιήστε την επιλογή Εφαρμογή αυτού του κανόνα σε όλες τις εφαρμογές.

6. Επιλέξτε την καρτέλα ΓΙΑ ΠΡΟΧΩΡΗΜΕΝΟΥΣ.

7. Στο πλαίσιο Προσαρμοσμένη απομακρυσμένη διεύθυνση πληκτρολογήστε τη διεύθυνση IP του υπολογιστή ή του εκτυπωτή στον οποίο θέλετε να έχετε πρόσβαση χωρίς περιορισμούς.

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 στον άλλον υπολογιστή μπορεί να μπλοκάρει 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 εικονίδιο 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 συνδέθει σε ένα λογαριασμό ως διαχειριστής των Windows για να αποκτήσετε πρόσβαση στον κοινόχρηστο εκτυπωτή.

● Εξούν καθοριστεί δικαιώματα για τον κοινόχρηστο εκτυπωτή ώστε να επιτρέψει την πρόσβαση σε υπολογιστές και χρήστες μόνο. Εάν μοιράζεστε τον εκτυπωτή σας, ελέγξτε τα δικαιώματα που έχουν ρυθμιστεί στον εκτυπωτή για να δείτε αν επιτρέπεται η πρόσβαση του χρήστη του άλλου υπολογιστή στον εκτυπωτή. Εάν προσπαθείτε να συνδέθετε σε έναν κοινόχρηστο εκτυπωτή, ελέγξτε με τον χρήστη στον άλλο υπολογιστή αν έχετε άδεια για να συνδέθετε στον εκτυπωτή.

● Ο εκτυπωτής που είναι συνδεδεμένος με τον υπολογιστή σας ή με τον άλλον υπολογιστή δεν είναι κοινόχρηστος.

● Ο κοινόχρηστος εκτυπωτής δεν έχει προστεθεί στον υπολογιστή.
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 σε συγκεκριμένους υπολογιστές ή χρήστες μόνο. 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 επικοινωνήσετε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα “Ζητήσετε βοήθεια” (p. 327).

6.1.8. Η σύνδεσή μου στο Internet είναι αργή

Αυτή η κατάσταση μπορεί να εμφανιστεί μετά την εγκατάσταση του Bitdefender. Το θέμα θα μπορούσε να οφείλεται σε σφάλματα στη διαμόρφωση του Bitdefender firewall.

Για να αντιμετωπίσετε αυτή την κατάσταση:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στο παράθυρο FIREWALL, κάντε κλικ στον διακόπτη ON / OFF για να απενεργοποιήσετε τη λειτουργία.
4. 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 προκαλέεται από το Bitdefender. Θα πρέπει να επικοινωνήσετε με τον παρόχο σύνδεσης Internet για να ελέγξετε εάν η σύνδεσή σας είναι λειτουργική από την πλευρά τους.

Εάν λάβετε επιβεβαίωση από τον παρόχο υπηρεσιών Διαδικτύου σας ότι η σύνδεσή σας είναι λειτουργική στο πλευρό τους και το πρόβλημα συνεχίζει, επικοινωνήστε με το Bitdefender όπως περιγράφεται στην ενότητα “Ζητήσετε βοήθεια” (p. 327).
Εάν η σύνδεση στο Internet βελτιώθηκε μετά την απενεργοποίηση του Bitdefender firewall:

a. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

b. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

c. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου FIREWALL.

d. Μεταβείτε στην καρτέλα ΠΡΟΣΑΡΜΟΓΕΙΣ ΔΙΚΤΥΟΥ και ρυθμίστε τη σύνδεση στο διαδίκτυο στο Home / Office.

e. Στην καρτέλα ΓΙΑ ΠΡΟΧΩΡΗΜΕΝΟΥΣ, κάντε κλικ στην επιλογή Αποκλεισμός σάρωσης θυρών στο δίκτυο. Στην περιοχή Stealth Mode, κάντε κλικ στην επιλογή Επεξεργασία συνδέσεων stealth. Ενεργοποιήστε τη λειτουργία Stealth για τον προσαρμογέα δικτύου στον οποίο είστε συνδεδεμένοι.

f. Κλείστε το Bitdefender, κάντε επανεκκίνηση του συστήματος και να ελέγξετε την ταχύτητα σύνδεσης στο Internet.

Εάν αυτές οι πληροφορίες δεν ήταν χρήσιμες, μπορείτε να επικοινωνήσετε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα “Ζητήσετε βοήθεια” (p. 327).

6.1.9. 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 τους πιο πρόσφατες Bitdefender υπογραφές malware:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Επιλέξτε την καρτέλα Ενημέρωση.

3. Δίπλα στο Κανόνες Επεξεργασίας Ενημέρωσης, επιλέξτε Ερώτηση πριν από τη λήψη από το αναπτυσσόμενο μενού.
4. Πηγαίνετε πίσω στο κύριο παράθυρο και κάντε κλικ στο κουμπί δράσης 
Ενημέρωση από τη διεπαφή Bitdefender.
5. Επιλέξτε μόνο Signatures updates, και στη συνέχεια κάντε κλικ στο OK.
6. Το Bitdefender θα κατεβάσει και θα εγκαταστήσει μόνο τις ενημερώσεις 
υπογραφής για κακόβουλο λογισμικό.

6.1.10. 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 στον υπολογιστή σας 
  ταυτόχρονα 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 τον υπολογιστή και περιμένετε λίγα λεπτά μέχρι να 
  φορτωθεί το Bitdefender. Ανοίξτε το Bitdefender για να δείτε εάν το 
  πρόβλημα παραμένει. Η επανεκκίνηση του υπολογιστή συνήθως λύνει 
  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 εγκαταστήσετε ξανά το Bitdefender.

Για περισσότερες πληροφορίες παρακολούθησε τη σελίδα “Πώς 
μπορώ να καταργήσω τις άλλες λύσεις ασφάλειας;” (p. 93).
Εάν το σφάλμα παραμένει, επικοινωνήστε με τους εκπροσώπους υποστήριξης μας για βοήθεια όπως περιγράφεται στην ενότητα "Ζητήσετε βοήθεια" (p. 327).

6.1.11. Το Antispam φίλτρο δεν λειτουργεί σωστά

Αυτό το άρθρο σας βοηθά να αντιμετωπίσετε τα ακόλουθα προβλήματα που αφορούν την Bitdefender Antispam λειτουργία φίλτραρίσματος:

- 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 συμβουν 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. 129).

Προσθήκη επαφών στη λίστα φίλων

Εάν χρησιμοποιείτε μία υποστηριζόμενη εφαρμογή ηλεκτρονικού ταχυδρομείου, μπορείτε εύκολα να προσθέσετε τους αποστολείς των νόμιμων μηνυμάτων στη λίστα φίλων. Ακολουθείτε 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 Επαφή 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 Ακολουθείτε αυτά τα βήματα:

1. Κάντε κλικ στο εικονίδιο Β στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα ANTISPAM, επιλέξτε Διαχείριση φίλων.

Εμφανίζεται ένα παράθυρο διαμόρφωσης.
4. Πληκτρολογήστε τη διεύθυνση e-mail από την οποία θέλετε να λαμβάνετε πάντοτε τα μηνύματα ηλεκτρονικού ταχυδρομείου 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.

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 Βitdefender.
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. 129).

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 μηνυμάτων
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. Ακολουθείτε αυτά τα βήματα:
1. Ανοίξτε την εφαρμογή του ηλεκτρονικού ταχυδρομείου σας.
2. Πηγαίνετε στο φάκελο Εισερχόμενα.
3. Επιλέξτε τα μη ανιχνευθέντα spam μηνύματα

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. Ακολουθείτε αυτά τα βήματα:
1. Ανοίξτε την εφαρμογή του ηλεκτρονικού ταχυδρομείου σας.
2. Πηγάνετε 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 Μεταφορά της γραμμής e-mail προσανατολισμένης σε spam.

5. Μπορεί να σας ζητηθεί να επικυρώσετε τις διευθύνσεις που προστίθενται στη λίστα Spammers. Οποιαδήποτε διεύθυνση που έχει ήδη εμφανισθεί και διαγράφεται από τη λίστα Spammers, δεν εμφανίζεται μία διεύθυνση που έχει προστίθενται στη λίστα Spammers από τη διεπαφή του Bitdefender Eίναι βολικό να το κάνετε αυτό μόνο όταν έχετε πληροφόρηση πολλά μηνύματα spam από την ίδια διεύθυνση ήλεκτρονικού ταχυδρομείου. Ακολουθείται αυτά τα βήματα:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Στην ενότητα ΑΝΤΙΣΠΑΜ, επιλέξτε Διαχείριση Spammers.

4. Εμφανίζεται ένα παράθυρο διαμόρφωσης.

5. Κάντε κλικ στο OK για να αποθηκεύσετε τις αλλαγές και να κλείσετε το παράθυρο.

Το antispam φίλτρο δεν ανιχνεύει κανένα μηνύμα 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 προστασίας antispam, κάντε κλικ στο ικονίδιο στην αριστερή μπάρα του Bitdefender interface, και στη συνέχεια επιλέξτε το σύνδεσμο ΠΡΟΒΟΛΗ ΕΝΟΤΗΤΩΝ. Κάντε κλικ στο
γρανάζι από τον πίνακα του ANTISPAM, στη συνέχεια, ελέγξτε στην επάνω πλευρά του παραθύρου εάν είναι ενεργοποιημένη η επιλογή..
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 φίλτραρονται 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
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:

**Σε Microsoft Edge**
1. Ανοίξτε το Microsoft Edge.
2. Κάντε κλικ στην επιλογή Περισσότερα.
3. Κάντε κλικ στο Επεκτάσεις.
4. Επιλέξτε το Bitdefender Wallet και κάντε κλικ στο κουμπί Enable.

**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 Εργαλεία.
3. Κάντε κλικ στο Add-ons.
4. Κάντε κλικ στο Επεκτάσεις.
5. Επιλέξτε το Bitdefender Wallet και κάντε κλικ στο κουμπί Enable.

**Στον Google Chrome:**
1. Ανοίξτε το Google Chrome.
2. Μεταβείτε στο εικονίδιο του Μενού.
3. Κάντε κλικ στο Ρυθμίσεις.
4. Κάντε κλικ στο Επεκτάσεις.
5. Επιλέξτε το Bitdefender Wallet και κάντε κλικ στο κουμπί Enable.

**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. 327).

6.1.13. 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 αποτυχάνει, 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 εικονίδιο 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.

6.1.14. Το σύστημα μου δεν ξεκινάει 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. 94).

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 προϊόντος 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. 94).

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 Πολιτικές.

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 εικονίδιο 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, πηγάνετε στην ιστοσελίδα τους και εκτελέστε το εργαλείο της απεγκατάστασης τους ή επικοινωνήστε απευθείας μαζί τους με σκοπό να σας δώσουν τις κατευθυντήριες γραμμές για την απεγκατάστασή τους.

3. Επανεκκινήστε το σύστημά σας σε κανονική λειτουργία και επανεγκαταστήστε 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. 94).

2. Χρησιμοποιήστε την επιλογή System Restore από τα Windows για να επαναφέρετε τον υπολογιστή σε προγενέστερη ημερομηνία πριν από την εγκατάσταση του Bitdefender προϊόντος.

3. Επανεκκινήστε το σύστημα σε κανονική λειτουργία και επικοινωνήστε με τους εκπροσώπους υποστήριξης μας για βοήθεια, όπως περιγράφεται στην ενότητα “Ζητήσετε βοήθεια” (p. 327).
6.2. Αφαίρεση κακόβουλου λογισμικού από το σύστημά σας

Το κακόβουλο λογισμικό μπορεί να επηρεάσει το σύστημά σας με πολλούς διαφορετικούς τρόπους και η προσέγγιση του Bitdefender εξαρτάται από το είδος της επίθεσης του κακόβουλου λογισμικού. Επειδή οι ιοί 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.

- "Bitdefender Λειτουργία διάσωσης (Περιβάλλον διάσωσης στα Windows 10)” (p. 237)
- “Τι να κάνετε όταν το Bitdefender βρίσκει ιούς στον υπολογιστή σας;” (p. 241)
- “Πώς μπορώ να καθαρίσω έναν ιό αρχείο;” (p. 243)
- “Πώς μπορώ να καθαρίσω έναν ιό σε ένα αρχείο archive e-mail;” (p. 244)
- "Τι πρέπει να κάνω αν υποπτεύομαι έναν αρχείο ως επικίνδυνο;” (p. 245)
- “Ποιά είναι τα αρχεία που προστατεύονται με κωδικό πρόσβασης στο αρχείο καταγραφής της σάρωσης;” (p. 246)
- “Ποια είναι τα στοιχεία που έχουν παραλειφθεί στο αρχείο καταγραφής της σάρωσης;” (p. 246)
- “Ποια είναι τα υπερ-συμπιεσμένα αρχεία στο αρχείο καταγραφής της σάρωσης;” (p. 247)
- "Γιατί το Bitdefender διέγραψε αυτόματα ένα μολυσμένο αρχείο;” (p. 247)

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. 327).
6.2.1. Bitdefender Λειτουργία διάσωσης (Περιβάλλον διάσωσης στα Windows 10)

Η Λειτουργία Διάσωσης είναι ένα χαρακτηριστικό του Bitdefender που σας επιτρέπει να σαρώσετε και να καθαρίσετε όλα τα υπάρχοντα διαμερίσματα του σκληρού δίσκου.


Σε Windows 10, το περιβάλλον διάσωσης του Bitdefender είναι ενσωματωμένο στα Windows RE, πράγμα που σημαίνει ότι δεν χρειάζεται να κάνετε λήψη οποιασδήποτε εικόνας λειτουργίας διάσωσης σε αυτό το λειτουργικό σύστημα και η λειτουργία δεν μπορεί να χρησιμοποιηθεί σε περίπτωση προβλημάτων εκκίνησης. Για να καθαρίσετε το σύστημα πριν τη φόρτωση των υπηρεσιών των Windows, σας συνιστούμε να χρησιμοποιήσετε το CD διάσωσης του Bitdefender.

Το Bitdefender CD διάσωσης είναι ένα δωρεάν εργαλείο που σαρώνει και καθαρίζει τον υπολογιστή σας κάθε φορά που υποψιάζεστε ότι μια απειλή κακοβουλου λογισμικού επηρεάζει τη λειτουργία του. Χρήσιμα άρθρα που περιέχουν λεπτομέρειες σχετικά με τον τρόπο δημιουργίας και χρήσης τους είναι διαθέσιμα στην πλατφόρμα του Κέντρου υποστήριξης Bitdefender στο https://www.bitdefender.com/support/consumer.html.

Κατεβάζοντας το αρχείο εικόνας διάσωσης του Bitdefender

Για να μπορείτε να χρησιμοποιήσετε τη λειτουργία Διάσωσης σε Windows 7, Windows 8 και Windows 8.1, πρώτα πρέπει να κάνετε λήψη του αρχείου εικόνας ως εξής:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα ANTIVIRUS επιλέξτε Λειτουργία Διάσωσης.
4. Επιλέξτε ΝΑΙ στο παράθυρο επιβεβαίωσης που εμφανίζεται για να επανεκκινήσετε τον υπολογιστή.
Περιμένετε μέχρι να κατέβει το αρχείο εικόνας διάσωσης του Bitdefender, από τους Bitdefender servers. Μόλις το αρχείο κατέβει, ο υπολογιστής θα επανεκκινηθεί.

Μία οθόνη θα εμφανιστεί όπου θα πρέπει να επιλεγεί το λειτουργικό σύστημα. Σε αυτό το βήμα θα πρέπει να επιλέξετε αν θα θέλατε να εκκινήσει μέσω της διαδικασίας διάσωσης ή σε κανονική λειτουργία.

Σημείωση
Λόγω της ενοποίησης με το περιβάλλον αποκατάστασης των Windows στα Windows 10, δεν χρειάζεται να κάνετε λήψη οποιουδήποτε αρχείου εικόνας διάσωσης σε αυτό το λειτουργικό σύστημα.

Ξεκινήστε το σύστημά σας στη λειτουργία διάσωσης στα Windows 7, Windows 8 και Windows 8.1

Μπορείτε να μπείτε σε Κατάσταση Διάσωσης με έναν από τους δύο τρόπους:

Από τη διεπαφή Bitdefender

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
3. Στην ενότητα ΑΝΤΙΒΙΡΟΣ επιλέξτε Λειτουργία Διάσωσης.
4. Επιλέξτε ΝΑΙ στο παράθυρο επιβεβαίωσης που εμφανίζεται για να επανεκκινήσετε τον υπολογιστή.
5. Μετά την επανεκκίνηση του υπολογιστή, εμφανίζεται ένα μενού που σας προτρέπει να επιλέξετε ένα λειτουργικό σύστημα. Επιλέξτε το Bitdefender Rescue Mode να εκκινήσετε σε ένα Bitdefender περιβάλλον από όπου μπορείτε να καθαρίσετε την κατάτμηση των Windows.
6. Εάν σας ζητηθεί, πατήστε το πλήκτρο Enter και επιλέξτε την ανάλυση οθόνης που βρίσκεται πλησιέστερα προς εκείνη που συνήθως χρησιμοποιείτε. Στη συνέχεια, πατήστε Enter ξανά. Το Bitdefender Rescue Mode θα φορτώσει σε λίγα λεπτά.
Εκκίνηση του υπολογιστή σας απευθείας σε Λειτουργία Διάσωσης

Εάν τα Windows ξεκινούν πια, μπορείτε να εκκινήσετε τον υπολογιστή σας απευθείας στην Λειτουργία Διάσωσης του Bitdefender, ακολουθώντας τα παρακάτω βήματα:

● Στα Windows 7:
  1. Πατήστε το πλήκτρο F8 μέχρι να εμφανιστεί η οθόνη Advanced Boot Options .
  2. Χρησιμοποιήστε τα πλήκτρα βέλους για να επιλέξετε τη λειτουργία Bitdefender Διάσωση και στη συνέχεια πατήστε Enter .
   
   Η Λειτουργία Διάσωσης του Bitdefender θα φορτώσει σε λίγα λεπτά.

● Στα Windows 8 και στα Windows 8.1:
  1. Πατήστε το πλήκτρο Shift μέχρι να εμφανιστεί η οθόνη Advanced Startup Options .
  2. Επιλέξτε τη δυνατότητα Χρήση άλλου λειτουργικού συστήματος και στη συνέχεια τη λειτουργία Bitdefender Λειτουργία Διάσωσης.
   
   Η Λειτουργία Διάσωσης του Bitdefender θα φορτώσει σε λίγα λεπτά.

Σημείωση
Μόνο όταν έχει κατέβει το αρχείο εικόνας διάσωσης όπως περιγράφηκε στο “Κατεβάζοντας το αρχείο εικόνας διάσωσης του Bitdefender” (p. 237), είναι εφικτό να ξεκινήσει ο υπολογιστής με τη λειτουργία διάσωσης.

Ξεκινήστε το σύστημά σας στο περιβάλλον διάσωσης στα Windows 10

Μπορείτε να εισέρθετε στο περιβάλλον διάσωσης μόνο μέσω του Bitdefender σας, ως εξής:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

2. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

3. Στην ενότητα ΑΝΤΙΒΙΡΟΣ επιλέξτε Περιβάλλον Διάσωσης.
4. Κάντε κλικ στο Επανεκκίνηση στο παράθυρο που εμφανίζεται.

Το Bitdefender περιβάλλον διάσωσης θα φορτώσει σε λίγα λεπτά.

Σάρωση του συστήματός σας στη λειτουργία διάσωσης (Περιβάλλον διάσωσης στα Windows 10)

Για να σαρώσετε το σύστημά σας στη λειτουργία Διάσωσης (Περιβάλλον Διάσωσης):

- **Στα Windows 7, Windows 8 και στα Windows 8.1:**
  1. Μπείτε σε Κατάσταση Διάσωσης, όπως περιγράφεται στο “Ξεκινήστε το σύστημά σας στη λειτουργία διάσωσης στα Windows 7, Windows 8 και Windows 8. 1” (p. 238).
  2. Το λογότυπο του Bitdefender θα εμφανιστεί και οι μηχανές antivirus θα αρχίσουν να αντιγράφονται.
  3. Τότε θα εμφανιστεί ένα παράθυρο καλωσορίσματος. Κάντε κλικ στο Συνέχεια.
  4. Μια ενημέρωση των υπογραφών antivirus έχει ξεκινήσει.
  5. Αφού ολοκληρωθεί η ενημέρωση, ένα παράθυρο Σαρωτή Antivirus On-demand του Bitdefender εμφανίζεται.
  6. Κάντε κλικ στο Scan Now, επιλέξτε το στόχο σάρωσης στο παράθυρο που εμφανίζεται και κάντε κλικ στο Open για να ξεκινήσει η σάρωση.

Συνιστάται να σαρώσει ολόκληρο το διαμέρισμα των Windows σας.

### Σημείωση

Όταν εργάζεστε σε λειτουργία διάσωσης, έχετε να κάνετε με τα ονόματα διαμερισμάτων τύπου Linux. Τα διαμερίσματα του δίσκου θα εμφανιστούν ως sda1 πιθανώς αντιστοιχούν στο (C:) τύπο διαμερίσματος των Windows, sda2 αντιστοιχούν στο (D:) και ούτω καθεξής.

7. Περιμένετε να ολοκληρωθεί η σάρωση. Εάν εντοπιστεί οποιαδήποτε κακόβουλο λογισμικό, ακολουθήστε τις οδηγίες για να αφαιρέσετε την απειλή.

8. Για να βγείτε από τη Λειτουργία Διάσωσης, κάντε δεξί κλικ σε μια κενή περιοχή της επιφάνειας εργασίας, επιλέξτε Exit στο μενού που
εμφανίζεται και στη συνέχεια επιλέξετε εάν θα επανεκκινήσετε ή θα
tερματίσετε τη λειτουργία του υπολογιστή.

● Στα Windows 10:

1. Μπείτε σε Περιβάλλον Διάσωσης, όπως περιγράφεται στο “Ξεκινήστε
tο σύστημά σας στο περιβάλλον διάσωσης στα Windows 10” (p. 239)
2. Η διαδικασία σάρωσης του Bitdefender ξεκινά αυτόματα μόλις το
σύστημα φορτωθεί στο περιβάλλον διάσωσης.
3. Περιμένετε να ολοκληρωθεί η σάρωση. Εάν εντοπιστεί οποιαδήποτε
κακόβουλο λογισμικό, ακολουθήστε τις οδηγίες για να αφαιρέσετε
tην απειλή.
4. Για έξοδο από το περιβάλλον διάσωσης, κάντε κλικ στο κουμπί
ΕΞΟΔΟΣ στο παράθυρο με τα αποτελέσματα της σάρωσης.

6.2.2. Τι να κάνετε όταν το Bitdefender βρίσκει ιούς στον
υπολογιστή σας;

Μπορείτε να διαπιστώσετε ότι ένας ιός είναι στον υπολογιστή σας με έναν
από τους παρακάτω τρόπους:
● Σαρώσατε τον υπολογιστή σας και το Bitdefender βρήκε μολυσμένα
αντικείμενα πάνω σε αυτόν.
● Μια προειδοποίησης σχετικά με ιούς σας ενημερώνει ότι το Bitdefender
απέκλεισε έναν ή πολλούς ιούς στον υπολογιστή σας.

Σε τέτοιες περιπτώσεις, ενημερώστε το Bitdefender για να βεβαιωθείτε
ότι έχετε τις πιο πρόσφατες υπογραφές για κακόβουλο λογισμικό και να
εκτελέσετε 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
tων Windows ή ότι δεν είναι μολυσμένο αρχείο, μην ακολουθήσετε αυτά τα
βήματα και επικοινωνήστε με την Εξυπηρέτηση Πελατών του Bitdefender
to 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. Κάντε κλικ στο εικονίδιο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ στην αριστερή μπάρα του Bitdefender ΑΣΠΙΔΑ.
   b. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.
   c. Κάντε κλικ στο εικονίδιο ΑΝΤΙΒΟΥΤΛΑ στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS.
   d. Στο παράθυρο ΑΣΠΙΔΑ, κάντε κλικ στον διακόπτη ΟΝ/ΟΦ.
2. Εμφάνιση κρυφών αντικειμένων στα Windows. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο “Εμφάνιση κρυφών αντικειμένων στα Windows.” (p. 92).
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. 94).
2. Εμφάνιση κρυφών αντικειμένων στα Windows. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο “Εμφάνιση κρυφών αντικειμένων στα Windows.” (p. 92).
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. 327).
6.2.3. Πώς μπορώ να καθαρίσω έναν ιό σε ένα αρχείο;

Ένα συμπιεσμένο αρχείο (archive) είναι ένα αρχείο ή μια συλλογή αρχείων 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 νέων κειμένων, αλλά δεν είναι σε θέση να λάβει οποιαδήποτε άλλα μέτρα.

Εάν το Bitdefender σας ενημερώνει ότι ένας ιός έχει ανιχνευθεί μέσα σε ένα αρχείο και καμία ενέργεια δεν είναι διαθέσιμη, αυτό σημαίνει ότι η κατάργηση του ιού δεν είναι δυνατή λόγω των περιορισμών σχετικά με τις ρυθμίσεις άδειας του αρχείου.

Εδώ είναι ο τρόπος που μπορείτε να καθαρίσετε έναν ιό αποθηκευμένο σε ένα αρχείο:

1. Προσδιορίστε το αρχείο που περιλαμβάνει τον ιό εκτελώντας ένα σύστημα σάρωσης του συστήματος.

2. Απενεργοποιήστε την προστασία από τους ιούς του Bitdefender:

   a. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.

   b. Κάντε κλικ στο σύνδεσμο ΠΡΟΒΟΛΗ ΧΑΡΑΚΤΗΡΙΣΤΙΚΩΝ.

   c. Κάντε κλικ στο εικονίδιο στην κάτω δεξιά γωνία του παραθύρου ANTIVIRUS

   d. Στο παράθυρο ΑΣΠΙΔΑ, κάντε κλικ στον διακόπτη ON/OFF.

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 αφανεθεί.
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 ένας ιός αποθηκευμένος σε ένα αρχείο δεν είναι μια άμεση απειλή για το σύστημά σας, δεδομένου ότι ο ιός 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 “Ζητήστε βοήθεια” (p. 327).

6.2.4. Πώς μπορώ να καθαρίσω έναν ιό σε ένα αρχείο archive e-mail;

To Bitdefender μπορεί επίσης να προσδιορίσει τους ιούς σε βάσεις δεδομένων e-mail και τα archive ηλεκτρονικού ταχυδρομείου που αποθηκεύονται στο δίσκο.

Μερικές φορές είναι απαραίτητο να προσδιοριστούν τα μολυσμένα μήνυματα χρησιμοποιώντας τις πληροφορίες που παρέχονται στην αναφορά σάρωσης και να διαγράψετε με το χέρι.

Εδώ είναι ο τρόπος που μπορείτε να καθαρίσετε έναν ιό αποθηκευμένο σε ένα archive 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. Κάντε κλικ στο εικονίδιο interface στην αριστερή μπάρα του Bitdefender
   b. Κάντε κλικ στον διακόπτη ON/OFF.

   c. Κάντε κλικ στο εικονίδιο ANTIVIRUS στην κάτω δεξιά γωνία του παραθύρου

   d. Στο παράθυρο ΑΣΠΙΔΑ, κάντε κλικ στον διακόπτη ON/OFF.
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 επικοινωνήσετε με το Bitdefender για υποστήριξη όπως περιγράφεται στην ενότητα "Ζητήστε βοήθεια" (p. 327).

6.2.5. Τι πρέπει να κάνω αν υποπτεύομαι ένα αρχείο ως επικίνδυνο;

Μπορεί να υποψήφιο 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. 67).
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 μπορέσουμε να σας βοηθήσουμε. Για να μάθετε πώς να το κάνετε αυτό, ανατρέξτε στο "Ζητήστε βοήθεια" (p. 327).

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 είναι προστατευμένα 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 που πρέπει να εξαχθούν αυτά τα περιεχόμενα, ο σαρωτής του Bitdefender θα τα σαρώσει αυτόματα σε πραγματικό χρόνο για να προστατεύσει τον υπολογιστή σας. 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 μπόρεσαν 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 παρέληφε 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 malware, 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 αναγνωρίσετε τέτοια κατάσταση, κατεβάστε το αρχείο εγκατάστασης από την ιστοσελίδα του κατασκευαστή ή άλλη έμπιστη ιστοσελίδα.
ANTIVIRUS ΓΙΑ MAC
7. ΕΓΚΑΤΑΣΤΑΣΗ ΚΑΙ ΑΦΑΙΡΕΣΗ

Αυτό το κεφάλαιο περιλαμβάνει τα ακόλουθα θέματα:

● “Απαιτήσεις συστήματος” (p. 249)
● “Εγκατάσταση του Bitdefender Antivirus for Mac” (p. 249)
● “Αφαίρεση Bitdefender Antivirus for Mac” (p. 254)

7.1. Απαιτήσεις συστήματος

Μπορείτε να εγκαταστήσετε το Bitdefender Antivirus for Mac μόνο σε Intel Macintosh υπολογιστές με OS X Mavericks (10.9.5), OS X Yosemite (10.10 ή νεότερο), OS X El Capitan (10.11), OS X Sierra(10.12) εγκατεστημένο. Ο Mac σας πρέπει επίσης να πληρεί όλες αυτές τις πρόσθετες απαιτήσεις:

● Ελάχιστο 1 GB μνήμης RAM
● 600ΜΒ ελάχιστο διαθέσιμο χώρο στον σκληρό δίσκο

Μια σύνδεση στο Internet είναι απαραίτητη για να εγγραφείτε και να ενημερώσετε το Bitdefender Antivirus for Mac.

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 More Info 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. Συνδέθετε ως διαχειριστής.
3. Συνδέθετε στο λογαριασμό Bitdefender σας χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.
4. Στο παράθυρο MY DEVICES κάντε κλικ στο INSTALL Bitdefender.
5. Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:

- **ΛΗΨΗ**
  Κάντε κλικ στο κουμπί και αποθηκεύσετε το αρχείο εγκατάστασης.

- **Σε άλλη συσκευή**
  Επιλέξτε macOS να κατεβάσετε το Bitdefender προϊόν σας, και, στη συνέχεια, κάντε κλικ στο ΣΥΝΕΧΕΙΑ. Πληκτρολογήστε μια διεύθυνση e-mail στο αντίστοιχο πεδίο και πατήστε ΣEND.

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](image.png)

**Κάντε κλικ στο Συνέχεια.**
Βήμα 2 - Διαβάστε την Άδεια Χρήσης

Η Άδεια χρήσης είναι μια νομικά δεσμευτική συμφωνία ανάμεσα σε εσάς και την Bitdefender για τη χρήση του Bitdefender Antivirus for Mac. Μπορείτε να εκτυπώσετε ή να αποθηκεύσετε την Άδεια Χρήσης, ώστε να μπορείτε να τη ξαναδιαβάσετε σε μεταγενέστερο χρόνο.

Παρακαλούμε διαβάστε προσεκτικά την Άδεια χρήσης. Για να συνεχίσετε την εγκατάσταση του λογισμικού θα πρέπει να συμφωνήσετε με τους όρους της άδειας χρήσης λογισμικού. Κάντε κλικ στο Continue, και στη συνέχεια κάντε κλικ στο κουμπί Agree.

Σημαντικό

Εάν δεν συμφωνείτε με αυτούς τους όρους, κάντε κλικ στο Continue και στη συνέχεια, κάντε κλικ στην επιλογή Disagree για να ακυρώσετε την εγκατάσταση και να κλείσετε το πρόγραμμα εγκατάστασης.
Βήμα 3 - Ξεκινήστε την Εγκατάσταση

To Bitdefender Antivirus for Mac θα εγκατασταθεί στο Macintosh HD/Library/Bitdefender. Η διαδρομή εγκατάστασης δεν μπορεί να αλλάξει. Κάντε κλικ στο Install 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 Continue.

Βήμα 5 - Τέλος

ΤΕΛΟΣ

Κάντε κλικ στο Close για να κλείσετε το παράθυρο.
Η διαδικασία απεγκατάστασης έχει ολοκληρωθεί.

Κατά την πρώτη εγκατάσταση του Bitdefender Antivirus for Mac, εμφανίζονται τα Ασφαλή Αρχεία και ο οδηγός της Προστασίας Time Machine. Για περισσότερες πληροφορίες, ανατρέξτε στα "Ασφαλή Αρχεία" (p. 272) και "Προστασία Time Machine" (p. 261).

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 Finder παράθυρο, μεταβείτε στο Applications φάκελο και επιλέξτε το Utilities.
2. Κάντε διπλό κλικ στο Bitdefender για Mac Κατάργηση για να το ανοίξετε.
3. Κάντε κλικ στο κουμπί Uninstall και περιμένετε να ολοκληρωθεί η διαδικασία.
4. Κάντε κλικ στο Close για να τελειώσει.

Σημαντικό
Αν υπάρχει κάποιο λάθος, μπορείτε να επικοινωνήσετε με την Bitdefender Εξυπηρέτηση Πελατών, όπως περιγράφεται στο “Ζητήσετε βοήθεια” (p. 327).
8. ΞΕΚΙΝΩΝΤΑΣ

Αυτό το κεφάλαιο περιλαμβάνει τα ακόλουθα θέματα:

● “Σχετικά με Bitdefender Antivirus for Mac” (p. 255)
● “Άνοιγμα Bitdefender Antivirus for Mac” (p. 255)
● “Κεντρικό Παράθυρο Εφαρμογής” (p. 256)
● “Εικονίδιο Application Dock” (p. 257)

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 ("malware"), μεταξύ των οποίων:

● ransomware
● adware
● ιοί
● spyware
● Trojans
● keyloggers
● worms

Η εφαρμογή αυτή εντοπίζει και αφαιρεί όχι μόνο κακόβουλο λογισμικό Mac, αλλά και τα Windows malware, εμποδίζοντάς έτσι την από λάθος αποστολή μολυσμένων αρχείων στην οικογένεια σας, στους φίλους σας και τους συναδέλφους σας που χρησιμοποιώντας PC.

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 Finder στη γραμμή μενού και επιλέξτε Open Main Window.
● Άνοιξτε ένα παράθυρο Finder, μεταβείτε στο Applications και κάντε διπλό κλικ στο εικονίδιο Bitdefender Antivirus for Mac.
8.3. Κεντρικό Παράθυρο Εφαρμογής

Στην κεντρικό παράθυρο της εφαρμογής μπορείτε να ελέγχετε την κατάσταση ασφαλείας του υπολογιστή σας, να εκτελέσετε σάρωση στο σύστημα, να διασφαλίσετε την εμπειρία περιήγησης στο web, ή να συνδεθείτε στον λογαριασμό Bitdefender σας.

Η επιλογή Autopilot που βρίσκεται στην επάνω δεξιά μέρος του κύριου παραθύρου, παρακολουθεί συνεχώς τις εφαρμογές που εκτελούνται στον υπολογιστή, ψάχνει για malware, και αποτρέπει την είσοδο σε νέες απειλές κακόβουλου λογισμικού στο συστήμα τους.

Για λόγους ασφαλείας, συνιστάται να διατηρείτε ενεργοποιημένο τον αυτόματο πιλότο. Αν ο αυτόματο πιλότος είναι απενεργοποιημένος, δεν θα προστατεύεστε αυτόματα από απειλές κακόβουλου λογισμικού.

Η γραμμή κατάσταση 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 κίτρινο. Κάντε κλικ στο κουμπί View Issues για να προβάλετε τα θέματα που επηρεάζουν την ασφάλεια του συστήματός σας. Για λεπτομερείς
πληροφορίες σχετικά με τα θέματα και πώς να τα διορθώσετε, ανατρέξτε στην "Διόρθωση θεμάτων" (p. 264).

Κάτω από τη γραμμή κατάστασης, τρία κουμπιά σάρωσης είναι διαθέσιμα για να σας βοηθήσουν να ελέγξετε το Mac σας:

- **Quick Scan** - ελέγχει για malware στα πιο ευάλωτα σημεία του σύστημά σας (για παράδειγμα, οι φάκελοι που περιέχουν τα έγγραφα, downloads, downloads του ταχυδρομείου και τα προσωρινά αρχεία του κάθε χρήστη).

- **Full Scan** - εκτελεί έναν ολοκληρωμένο έλεγχο για κακόβουλο λογισμικό σε όλο το σύστημα. Όλες οι συνδεδεμένες συσκευές θα σαρωθούν επίσης.

- **Custom Scan** - σας βοηθά να ελέγξετε συγκεκριμένα αρχεία, φακέλους ή αποθηκευτικούς χώρους για κακόβουλο λογισμικό.

Για περισσότερες πληροφορίες, ανατρέξτε στην “Σάρωση του Mac σας” (p. 260).

Εκτός από τα κουμπιά σάρωσης, πρόσθετες επιλογές είναι διαθέσιμες:

- **Web Protection** - φιλτράρει όλη την κυκλοφορία στο web και μπλοκάρει οποιοδήποτε κακόβουλο περιεχόμενο για να εξασφαλίσει την ασφαλή εμπειρία σας. Για περισσότερες πληροφορίες, ανατρέξτε στην “ΠΡΟΣΤΑΣΙΑ Web” (p. 296).

- **Go to Bitdefender account** - κάντε κλικ στο Go to your account σύνδεσμο στο κάτω δεξιά μέρος της κύριας οθόνης για να έχετε πρόσβαση στο λογαριασμό Bitdefender. Για περισσότερες πληροφορίες, ανατρέξτε στην “Bitdefender Central” (p. 277).

- **Number of days left** - εμφανίζει το χρόνο που απομένει πριν από τη λήξη της συνδρομής σας. Όταν φτάσει η ημερομηνία λήξης, κάντε κλικ στο σύνδεσμο για να αποκτήσετε πρόσβαση σε μια ιστοσελίδα από όπου μπορείτε να ανανεώσετε τη συνδρομή σας.

- **Buy** - σας ανακατευθύνει στην Bitdefender ιστοσελίδα όπου μπορείτε να ελέγξετε τις διαθέσιμες προσφορές ή να αγοράσετε μια συνδρομή.

- **Feedback** - ανοίγει ένα νέο παράθυρο στο προεπιλεγμένο προγράμματος e-mail σας από όπου μπορείτε να επικοινωνήσετε μαζί μας.

### 8.4. Εικονίδιο Application Dock

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.
9. ΠΡΟΣΤΑΣΙΑ ΑΠΌ ΚΑΚΌΒΟΥΛΟ ΛΟΓΙΣΜΙΚΌ

Αυτό το κεφάλαιο περιλαμβάνει τα ακόλουθα θέματα:

● “Βέλτιστες πρακτικές” (p. 259)
● “Σάρωση του Mac σας” (p. 260)
● “Ενεργοποίηση ή απενεργοποίηση του Autopilot” (p. 261)
● “Προστασία Time Machine” (p. 261)
● “Οδηγός Σάρωσης” (p. 263)
● “Διόρθωση θεμάτων” (p. 264)
● “ΠΡΟΣΤΑΣΙΑ Web” (p. 296)
● “ενημερώσεις” (p. 267)

9.1. Βέλτιστες πρακτικές

Για να διατηρήσετε το σύστημά σας ελεύθερο από malware και για την πρόληψη τυχαίας μόλυνσης και άλλων συστημάτων, ακολουθήστε αυτές τις βέλτιστες πρακτικές:

● Κρατήστε τον Autopilot ενεργοποιημένο, ώστε να επιτρέπει να σαρώνονται τα αρχεία του συστήματος από το Bitdefender Antivirus for Mac.

● Διατηρήστε το Bitdefender Antivirus for Mac το προϊόν σας ενημερωμένο με τις τελευταίες υπογραφές malware και ενημερώσεις προϊόντων, ενώ έχετε τον Autopilot ενεργοποιημένο.

● Ελέγξτε και να διορθώσετε τα ζητήματα που αναφέρθηκαν από το Bitdefender Antivirus for Mac τακτικά. Για αναλυτικές πληροφορίες, ανατρέξτε στο “Διόρθωση θεμάτων” (p. 264).

● 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 “Ιστορικό” (p. 275).

● 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. 269).

9.2. Σάρωση του Mac σας

Εκτός από τη λειτουργία του Autopilot, η οποία παρακολουθεί συνεχώς τις εφαρμογές που εκτελούνται στον υπολογιστή, ψάχνοντας για malware και αποτρέπει νέες απειλές κακόβουλου λογισμικού από την είσοδο του συστήματός σας, μπορείτε να σαρώσετε τον Mac σας ή συγκεκριμένα αρχεία όποτε 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. Άνοιγμα Bitdefender Antivirus for Mac.
2. Κάντε κλικ σε ένα από τα τρία κουμπιά σάρωσης για να ξεκινήσει η επιθυμητή σάρωση.

- **Quick Scan** - ελέγχει για malware στα πιο ευάλωτα σημεία του σύστημά σας (για παράδειγμα, οι φάκελοι που περιέχουν τα έγγραφα, downloads, downloads του ταχυδρομείου και τα προσωρινά αρχεία του κάθε χρήστη).

- **Full Scan** - εκτελεί έναν ολοκληρωμένο έλεγχο για κακόβουλο λογισμικό σε όλο το σύστημα. Όλες οι συνδεδεμένες συσκευές θα σαρωθούν επίσης.
Σημείωση

Ανάλογα με το μέγεθος του σκληρού σας δίσκου, σαρώνοντας όλο 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 Exclusions από το παράθυρο Προτιμήσεις.

● Custom Scan - σας βοηθά να ελέγξετε συγκεκριμένα αρχεία, φακέλους ή αποθηκευτικούς χώρους για κακόβουλο λογισμικό.

9.3. Ενεργοποίηση ή απενεργοποίηση του Autopilot

Για να ενεργοποιήσετε ή να απενεργοποιήσετε τον Autopilot, κάντε ένα από τα παρακάτω:

● Ανοίξτε το Bitdefender Antivirus for Mac και κάντε κλικ στο διακόπτη για να ενεργοποιήσετε ή να απενεργοποιήσετε Autopilot.

● Κάντε κλικ στο εικονίδιο στη γραμμή μενού και επιλέξτε Turn OFF Autopilot.

Προειδοποίηση

Σας συνιστούμε να απενεργοποιήσετε τον αυτόματο πιλότο για όσο το δυνατό λιγότερο χρόνο. Αν ο αυτόματο πιλότος είναι απενεργοποιημένος, δεν θα προστατεύσετε αυτόματα από απειλές κακόβουλου λογισμικού.

9.4. Προστασία Time Machine

Η Bitdefender Time Machine Protection χρησιμοποιεί ως ένα επιπέδο 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.
Οδηγός Time Machine Protection

Ο οδηγός του Bitdefender Time Machine Protection εμφανίζεται μόλις εγκαταστήσετε το Bitdefender Antivirus for Mac για πρώτη φορά στον υπολογιστή σας Macintosh.

Οδηγός Time Machine Protection

Θα πρέπει να ρυθμίσετε την εφαρμογή του Time Machine backup πριν ενεργοποιήσετε την Bitdefender προστασία.

Εάν η λειτουργία του Time Machine δεν είναι ενεργοποιημένη στον υπολογιστή σας:

1. Κάντε κλικ στην Go to Time Machine επιλογή.

   Εμφανίζεται το παράθυρο του Time Machine απο το System Preferences.

2. Ενεργοποιήστε τη λειτουργία, και στη συνέχεια, επιλέξτε πού θα κρατήσει τα αρχεία αντιγράψεων ασφαλείας.

Αν χρειάζεστε πρόσθετες οδηγίες για το πώς να ενεργοποιήσετε την εφαρμογή του Time Machine στο σύστημά σας, κάντε κλικ στο Find out how to configure Time Machine σύνδεσμο από τον οδηγό.

Για να ενεργοποιήσετε την Bitdefender Time Machine προστασία για τα αντίγραφα ασφαλείας σας:

1. Κάντε κλικ στην Enable Protection επιλογή.

   Εμφανίζεται ένα παράθυρο επιβεβαίωσης.

2. Επιλέξτε Close.
Ενεργοποίηση ή απενεργοποίηση της Time Machine προστασίας

1. Άνοιγμα Bitdefender Antivirus for Mac.
2. Κάντε κλικ στο κουμπί του Bitdefender Antivirus for Mac στη γραμμή μενού και επιλέξτε Preferences.
3. Κάντε κλικ στην καρτέλα Προστασία.
4. Επιλέξτε ή καταργήστε την επιλογή του πλαισίου ελέγχου της Time Machine Protection.

9.5. 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.

9.6. 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
dιορθώσετε 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:

- Οι νέες υπογραφές των malware και ενημερώσεις του προϊόντος δεν
  έχουν κατεβάσει από τους servers μας, γιατί το Autopilot είναι
  απενεργοποιημένο.

- Ανεπίλυτες απειλές έχουν εντοπιστεί στο σύστημά σας.

- Το Autopilot είναι απενεργοποιημένο.

Για να ελέγξετε και να διορθώσετε θέματα που ανιχνευτήκαν:

1. Άνοιγμα Bitdefender Antivirus for Mac.

2. Εάν το Bitdefender δεν έχει προειδοποιήσεις, η γραμμή κατάστασης
eίναι πράσινη. Όταν έχει εντοπιστεί ένα ζήτημα ασφαλείας, η γραμμή
kατάστασης αλλάζει το χρώμα του προς το κίτρινο.

3. Ελέγξτε την περιγραφή για περισσότερες πληροφορίες

4. Όταν ένα θέμα έχει εντοπιστεί, κάντε κλικ στο View Issues κουμπί για
  να δείτε πληροφορίες σχετικά με το τι είναι αυτό που επηρεάζει την
  ασφάλεια του συστήματος σας. Μπορείτε να κάνετε ενέργειες στο
  παράθυρο που εμφανίζεται.
Παράθυρο Άλυτων Απειλών

Ο κατάλογος των ανεπίλυτων απειλών ενημερώνεται μετά από κάθε σάρωση του συστήματος.

Μπορείτε να επιλέξετε να κάνετε τις ακόλουθες ενέργειες για τις άλυτες απειλές:

● Εμφάνιση στο Finder. Επιλέξτε αυτή την ενέργεια για να αφαιρέσει τις απειλές χειροκίνητα.

● Add to Exclusions. Η ενέργεια αυτή δεν είναι διαθέσιμη για κακόβουλο λογισμικό που βρέθηκαν μέσα σε συμπιεσμένα αρχεία.

9.7. ΠΡΟΣΤΑΣΙΑ Web

Το Bitdefender Antivirus for Mac χρησιμοποιεί τις επεκτάσεις του 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.

Μια σειρά από χαρακτηριστικά είναι διαθέσιμα για να σας προστατεύσει από όλα τα είδη απειλών που μπορεί να συναντήσετε κατά την περιήγηση στο διαδίκτυο:

● Advanced Threat Filter - σας αποτρέπει από την πρόσβαση σε ιστοσελίδες που χρησιμοποιούνται για απάτες και επιθέσεις phishing.
Search Results Analyzer - παρέχει έγκαιρη προειδοποίηση των επικίνδυνων ιστοσελίδων στα αποτελέσματα αναζήτησης σας.

Ειδοποίηση Tracker - εντοπίζει ίχνη στις ιστοσελίδες που επισκέπτεστε και σας ενημερώνει για την παρουσία τους.

Ενεργοποίηση επεκτάσεων Traffic Light

Για να ενεργοποιήσετε τις επεκτάσεις TrafficLight, ακολουθήστε τα εξής βήματα:

1. Άνοιγμα Bitdefender Antivirus for Mac.
2. Κάντε κλικ στο Fix Now για να ενεργοποιήσετε την προστασία Web.
3. Το Bitdefender Antivirus for Mac θα εντοπίσει ποιο web browser έχετε εγκαταστήσει στο σύστημά σας. Για να εγκαταστήσετε την επέκταση Κυκλοφορίας Φως στο πρόγραμμα περιήγησης σας, κάντε κλικ στην επιλογή Get Extension.
4. Θα μεταφερθείτε σε αυτή την online τοποθεσία: https://bitdefender.com/solutions/trafficlight.html
5. Επιλέξτε FREE DOWNLOAD.
6. Ακολουθήστε τα βήματα για να εγκαταστήσετε την επέκταση TrafficLight που αντιστοιχεί στο web browser σας.

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 από την ιστοσελίδα αμέσως. Εναλλακτικά, μπορείτε να επιλέξετε μία από τις διαθέσιμες επιλογές:
9.8. ενημερώσεις

Νέο κακόβουλο λογισμικό ανιχνεύεται και προσδιορίζεται κάθε μέρα. Γι ’αυτό είναι πολύ σημαντικό να διατηρήσουμε το Bitdefender Antivirus for Mac ενημερωμένο με τις τελευταίες υπογραφές κακόβουλου λογισμικού (malware).

Κρατήστε το Autopilot ενεργοποιημένο για να επιτρέψει τις malware υπογραφές και τις ενημερώσεις προϊόντων να κατέβουν αυτόματα στο σύστημά σας. Αν εντοπιστεί μια ενημερωμένη έκδοση, μεταφορτώνεται και εγκαθίσταται αυτόματα στον υπολογιστή σας.

Η ενημέρωση των υπογραφών κακόβουλου λογισμικού γίνεται τάχιστα, πράγμα που σημαίνει ότι τα αρχεία που πρέπει να ενημερωθούν αντικαθίστανται σταδιακά. Με τον τρόπο αυτό, η ενημέρωση δεν θα επηρεάσει τη λειτουργία του προϊόντος και, ταυτόχρονα, κάθε ευπάθεια θα αποκλείεται.

Όταν το Bitdefender Antivirus for Mac είναι ενημερωμένο, μπορεί να ανιχνεύεσε τις πιο πρόσφατες απειλές και να καθαρίσει τυχών μολυσμένα αρχεία.

Εάν το Bitdefender Antivirus for Mac δεν ενημερώνετε, δεν θα είναι σε θέση να εντοπίζει και να απομακρύνει την τελευταία malware που ανακαλύφθηκε από τα Bitdefender Labs.

9.8.1. Ζητώντας ενημέρωση

Μπορείτε να ζητήσετε μια ενημέρωση χειροκίνητα όποτε θέλετε. Μια ενεργή σύνδεση στο Internet είναι απαραίτητη για να ελέγξετε για διαθέσιμες ενημερώσεις και να τις κατεβάσετε.

Για να ζητήσετε μια ενημερωμένη έκδοση χειροκίνητα:
1. Άνοιγμα Bitdefender Antivirus for Mac.
2. Κάντε κλικ στο κουμπί Actions στη γραμμή μενού.
3. Επιλέξτε Update Virus Database.
Εναλλακτικά, μπορείτε να ζητήσετε μια ενημέρωση χειροκίνητα πατώντας CMD + U.

Μπορείτε να δείτε την πρόοδο της ενημέρωσης και την λήψη των αρχείων.

9.8.2. 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 λάβει τις malware ενημερώσεις.

9.8.3. Αναβάθμιση σε νέα έκδοση

Περιστασιακά, έχουμε δημοσιεύσει ενημερώσεις του προϊόντος για να προσθέσετε νέα χαρακτηριστικά και βελτιώσεις ή και να διορθώσουμε ζητήματα του προϊόντος. Αυτές οι ενημερώσεις μπορεί να 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.
10. ΔΙΑΜΟΡΦΩΣΗ ΠΡΟΤΙΜΗΣΕΩΝ

Αυτό το κεφάλαιο περιλαμβάνει τα ακόλουθα θέματα:
- "Προτιμήσεις Πρόσβασης" (p. 269)
- "Πληροφορίες Λογαριασμού" (p. 269)
- "Προτιμήσεις Προστασίας" (p. 269)
- "Σάρωση Εξαιρέσεων" (p. 271)
- "Ασφαλή Αρχεία" (p. 272)
- "Ιστορικό" (p. 275)
- "Καραντίνα" (p. 276)

10.1. Προτιμήσεις Πρόσβασης

Για να ανοίξετε το παράθυρο Προτιμήσεις του Bitdefender Antivirus for Mac:
1. Άνοιγμα Bitdefender Antivirus for Mac.
2. Κάντε κάτι από τα εξής:
   - Κάντε κλικ στο κουμπί του Bitdefender Antivirus for Mac στη γραμμή μενού και επιλέξτε Preferences.
   - Κάντε κλικ στο εικονίδιο στη γραμμή μενού και επιλέξτε Preferences.
   - Πατήστε Command- κόμμα (,).

10.2. Πληροφορίες Λογαριασμού

Το παράθυρο πληροφοριών του λογαριασμού σας δίνει τις πληροφορίες σας σχετικά με τη συνδρομή σας και το Bitdefender λογαριασμό.

Κάθε φορά που θέλετε να συνδεθείτε με ένα άλλο λογαριασμό Bitdefender, κάντε κλικ στο Switch account κουμπί, πληκτρολογήστε τη νέα διεύθυνση e-mail σας και τον κωδικό πρόσβασης στο λογαριασμό Bitdefender παράθυρο της εφαρμογής, στη συνέχεια, κάντε κλικ SIGN IN.

10.3. 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
genikés ruhmíseis.

Ενέργεια για μολυσμένα αρχεία. Όταν το Bitdefender Antivirus for Mac εντοπίσει έναν ιό ή άλλο κακόβουλο λογισμικό, 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 καθαριστούν μετακινούνται στην quarantine προκειμένου να απομονωθεί η μόλυνση. Αν και δεν συνιστάται, μπορείτε να ρυθμίσετε την εφαρμογή να μην αναλάβει καμία δράση για μολυσμένα αρχεία. Τα μολυσμένα αρχεία καταγράφονται μόνο.

Το Autopilot εξασφαλίζει καλή προστασία από κακόβουλο λογισμικό, με ελάχιστη επίπτωση στην απόδοση του συστήματος. Αν υπάρχουν απειλές που δεν αντιμετωπίστηκαν, μπορείτε να τις δείτε και να αποφασίσετε τι θα γίνει με αυτές.
Ενέργεια για 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.

Από προεπιλογή, τα ύποπτα αρχεία μετακινηθεί στην καραντίνα. Όταν ένας ιός είναι σε καραντίνα δεν μπορεί να κάνει οποιαδήποτε ζημιά, διότι δεν μπορεί να εκτελεστεί ή να διαβαστεί.

Αν προτιμάτε, μπορείτε να επιλέξετε να αγνοήσετε τα ύποπτα αρχεία. Τα μολυσμένα αρχεία καταγράφονται μόνο.

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 σάρωσή τους.

Μπορείτε να επιλέξετε να μην εφαρμόσει αυτή τη ρύθμιση για την drag&drop σάρωση επιλέγοντας 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.

Προστασία Time Machine. Επιλέξτε αυτό το πλαίσιο ελέγχου για να προστατεύσετε τα αρχεία που είναι αποθηκευμένα στο Time Machine. 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.

10.3.1. Σάρωση Εξαιρέσεων

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
Σάρωση Εξαιρέσεων

Η λίστα εξαιρέσεων περιέχει τα paths που έχουν αποκλειστεί από τη σάρωση.

Υπάρχουν δύο τρόποι για να ορίσετε μια εξαίρεση σάρωσης:

● Με Drag&drop ένα αρχείο, το φάκελο ή τον volume 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 volume που πρέπει να εξαιρεθούν από τη σάρωση.

Για να αφαιρέσετε μια εξαίρεση σάρωσης, επιλέξτε το από τη λίστα και κάντε κλικ στο κουμπί με το σύμβολο μείον (-), που βρίσκεται κάτω από τη λίστα εξαιρέσεων.

10.4. Ασφαλή Αρχεία

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.

Οδηγός Ασφαλών Αρχείων

Ο οδηγός του Bitdefender Time Machine Protection εμφανίζεται μόλις εγκαταστήσετε το Bitdefender Antivirus for Mac για πρώτη φορά στον υπολογιστή σας Macintosh. Επιλέξτε ή προσθέστε νέες τοποθεσίες που θέλετε να προστατεύσετε και, στη συνέχεια, κάντε κλικ στο κουμπί Ενεργοποίηση ασφαλών αρχείων.
Ασφαλή Αρχεία

Υπάρχουν δύο τρόποι για να προσθέσετε τα ακόλουθα αρχεία στο προστατευμένο περιβάλλον:

● Με Drag&drop ένα αρχείο, το φάκελο ή τον volume 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, τον φάκελο ή τον τόμο που θα προστατεύσετε σε περίπτωση που οι επιθέσεις ransomware θα προσπαθήσουν να έχουν πρόσβαση σε αυτές.

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.

10.4.1. Διαχείριση εφαρμογών

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". Εάν μια τέτοια εφαρμογή έχει αποκλειστεί και είστε βέβαιοι ότι η συμπεριφορά της είναι φυσιολογική, μπορείτε να την επιτρέψετε κάνοντας κλικ Το
κουμπί Διαχείριση Εφαρμογών ... και, στη συνέχεια, την αλλαγή της κατάστασης στην επιλογή Να επιτρέπεται.

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.

10.5. Ιστορικό

Το Bitdefender διατηρεί ένα λεπτομερές αρχείο καταγραφής των γεγονότων σχετικά με τη δραστηριότητά του στον υπολογιστή σας. Κάθε φορά που κάτι σχετικό με την ασφάλεια του συστήματος ή των δεδομένων σας συμβαίνει, ένα νέο μήνυμα, προστίθεται στο Bitdefender Antivirus for Mac Ιστορικό, με ένα παρόμοιο τρόπο που ένα νέο e-mail εμφανίζονται στα Εισερχόμενα σας.

Τα Γεγονότα 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 έγινε με επιτυχία, αν κακόβουλο λογισμικό βρέθηκε στον υπολογιστή σας, εάν μια μη εξουσιοδοτημένη εφαρμογή προσπάθησε να έχει πρόσβαση στον Time Machine δίσκο σας, κ.λπ.

Λεπτομέρειες σχετικά με τη δραστηριότητα του προϊόντος απεικονίζονται.
Κάθε φορά που θέλετε να διαγράψετε το αρχείο καταγραφής του ιστορικού, κάντε κλικ στο Clear History.

Το κουμπί Copy σας δίνει τη δυνατότητα να αντιγράψετε αυτές τις πληροφορίες στο clipboard.

10.6. Καραντίνα

Το Bitdefender Antivirus for Mac επιτρέπει την απομόνωση των προσβεβλημένων ή ύποπτων αρχείων σε μια ασφαλή περιοχή, που ονομάζεται καραντίνα. Όταν ένας ιός 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.
11. BITDEFENDER CENTRAL

Αυτό το κεφάλαιο περιλαμβάνει τα ακόλουθα θέματα:

● "σχετικά με Bitdefender Central" (p. 277)
● "Οι Συνδρομές μου" (p. 278)
● "Οι συσκευές μου" (p. 279)

11.1. σχετικά με 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 ημερήσιες εργασίες σε συσκευές όπου το Bitdefender είναι εγκατεστημένο. Μπορείτε να συνδεθείτε στο Bitdefender λογαριασμό από οποιονδήποτε υπολογιστή ή κινητή συσκευή που συνδέεται στο Internet μεταβαίνοντας στο https://central.bitdefender.com. Μόλις έχετε πρόσβαση σε αυτό, μπορείτε να αρχίσετε να κάνετε τα εξής:

● Λήψη και εγκατάσταση του Bitdefender σε λειτουργικά συστήματα macOS, Windows και Android. Τα προϊόντα που διατίθενται για λήψη είναι:
   ● Bitdefender Antivirus for Mac
   ● Η σειρά προϊόντων Bitdefender για Windows
   ● Bitdefender Ασφάλεια Κινητού
   ● Bitdefender Γονικός Έλεγχος
   ● Διαχειριστείτε και ανανέωστε τις Bitdefender συνδρομές σας.
   ● Προσθέστε νέες συσκευές στο δίκτυό σας και διαχειριστείτε τις από όπου κι αν βρίσκεστε.

11.2. 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.
3. Συνδεθείτε στο λογαριασμό σας χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασής σας.

11.3. Οι Συνδρομές μου

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

11.3.1. 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 My Subscriptions πάνελ.
3. Κάντε κλικ στο κουμπί ΚΩΔΙΚΟΣ ΕΝΕΡΓΟΠΟΙΗΣΗΣ, στη συνέχεια, πληκτρολογήστε τον κωδικό στο αντίστοιχο πεδίο.
4. Κάντε κλικ στο ΥΠΟΒΟΛΗ.

Η συνδρομή ενεργοποιήθηκε.

Για να ξεκινήσετε την εγκατάσταση του προϊόντος στις συσκευές σας, ανατρέξτε στο “Εγκατάσταση του Bitdefender Antivirus for Mac” (p. 249).
11.3.2. Αγοράστε μια συνδρομή

Μπορείτε να αγοράσετε μια συνδρομή απευθείας από το Bitdefender λογαριασμό σας ακολουθώντας τα παρακάτω βήματα:

1. Πρόσβαση στο Bitdefender Central.
2. Κάντε κλικ στο εικονίδιο που βρίσκεται στην επάνω αριστερή γωνία του παραθύρου και, στη συνέχεια, επιλέξτε το My Subscriptions πάνελ.
3. Κάντε κλικ στο Buy Now σύνδεσμο. Θα μεταφερθείτε σε μια ιστοσελίδα όπου μπορείτε να κάνετε την αγορά σας.

Μόλις ολοκληρωθεί η διαδικασία, η διαθεσιμότητα της συνδρομής θα είναι ορατό στην κάτω δεξιά γωνία της κύριας οθόνης του προϊόντος.

11.4. 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 της συσκευής σας εμφανίζουν το όνομα της συσκευής, το καθεστώς προστασίας και το υπόλοιπο διαθεσιμότητας της συνδρομής σας.

11.4.1. Προσαρμόστε το προϊόν σας

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

1. Πρόσβαση στο Bitdefender Central.
2. Στο MY DEVICES κάντε κλικ στο εικονίδιο με την επιθυμητή κάρτα της συσκευής, στη συνέχεια επιλέξτε Settings.
3. Αλλάξτε το όνομα της συσκευής όπως επιθυμείτε, και στη συνέχεια επιλέξτε SAVE.

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

1. Πρόσβαση στο Bitdefender Central.
2. Στο MY DEVICES κάντε κλικ στο εικονίδιο με την επιθυμητή κάρτα της συσκευής, στη συνέχεια επιλέξτε Profile.

3. Κάντε κλικ στο Προσθήκη ιδιοκτήτη, στη συνέχεια, συμπληρώστε τα αντίστοιχα πεδία, ορίστε το φύλο, την ημερομηνία γέννησης και προσθέστε ακόμη μια εικόνα προφίλ.

4. Κάντε κλικ στο ΠΡΟΣΘΗΚΗ για να αποθηκεύσετε ένα προφίλ.

5. Επιλέξτε τον επιθυμητό ιδιοκτήτη από τη λίστα Ιδιοκτήτης συσκευής και στη συνέχεια κάντε κλικ στο ΑΝΤΙΣΤΟΙΧΙΣΗ.

11.4.2. Ενέργειες εξ αποστάσεως

Για να ενημερώσετε εξ αποστάσεως το Bitdefender σε μια συσκευή, κάντε κλικ στο εικονίδιο στην επιθυμητή κάρτα της συσκευής, στη συνέχεια, επιλέξτε Update.

Για να ενεργοποιήσετε απομακρυσμένα τη λειτουργία Autopilot, κάντε κλικ στο εικονίδιο στην επιθυμητή κάρτα της συσκευής και επιλέξτε Settings. Κάντε κλικ στο αντίστοιχο διακόπτη για να ενεργοποιήσετε το Autopilot.

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

● Ταμπλώ. Σε αυτό το παράθυρο μπορείτε να ελέγξετε την κατάσταση της προστασίας των προϊόντων Bitdefender και τον αριθμό των ημερών που απομένουν για τη συνδρομή σας. Το καθεστώς προστασίας μπορεί να είναι πράσινο, όταν δεν υπάρχει κανένα πρόβλημα που να επηρεάζει το προϊόν σας, ή κόκκινο όταν η συσκευή βρίσκεται σε κίνδυνο. Όταν υπάρχουν προβλήματα που επηρεάζουν το προϊόν σας, κάντε κλικ στην επιλογή Προβολή προβλημάτων για να μάθετε περισσότερες λεπτομέρειες.

● 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. 260).
12. ΣΥΧΝΕΣ ΕΡΩΤΗΣΕΙΣ

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:
   - Πληκτρολογήστε τις απαιτούμενες πληροφορίες στα αντίστοιχα πεδία, και στη συνέχεια κάντε κλικ στο κουμπί ΔΗΜΙΟΥΡΓΙΑ ΛΟΓΑΡΙΑΣΜΟΥ.
   - Τα δεδομένα που εισαγάγατε εδώ παραμένουν εμπιστευτικά.

2. Κατεβάστε το Bitdefender Antivirus for Mac ως εξής:
   - Στο παράθυρο MY DEVICES κάντε κλικ στο INSTALL Bitdefender.
   - Επιλέξτε μία από τις δύο διαθέσιμες επιλογές:
     - ΛΗΨΗ
       - Κάντε κλικ στο κουμπί και αποθηκεύσετε το αρχείο εγκατάστασης.
     - Σε άλλη συσκευή
       - Επιλέξτε macOS να κατεβάσετε το Bitdefender προϊόν σας, και, στη συνέχεια, κάντε κλικ στο ΣΥΝΕΧΕΙΑ. Πληκτρολογήστε μια διεύθυνση e-mail στο αντίστοιχο πεδίο, και κάντε κλικ στο ΑΠΟΣΤΟΛΗ.
   - 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 My Subscriptions πάνελ.
3. Κάντε κλικ στο κουμπί ΚΩΔΙΚΟΣ ΕΝΕΡΓΟΠΟΙΗΣΗΣ, στη συνέχεια, πληκτρολογήστε τον κωδικό στο αντίστοιχο πεδίο.
4. Κάντε κλικ ξανά στο κουμπί ACTIVATION CODE button.

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

  Solution: Ενεργοποιήστε την επιλογή Don't scan content in backups στο Προτιμήσεις Προστασίας ή Add to Exclusions τα αρχεία 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.
Πού μπορώ να δω τις λεπτομέρειες σχετικά με τη δραστηριότητα της εφαρμογής;

To Bitdefender διατηρεί ένα αρχείο καταγραφής όλων των σημαντικών ενεργειών, αλλαγών κατάστασης και άλλων κρίσιμων μηνυμάτων που σχετίζονται με την δραστηριότητά του. Για να έχετε πρόσβαση σε αυτές τις πληροφορίες, ανοίξτε το παράθυρο Bitdefender Antivirus for Mac Προτιμήσεις:

1. Άνοιγμα Bitdefender Antivirus for Mac.
2. Κάντε κάτι από τα εξής:
   - Κάντε κλικ στο κουμπί του Bitdefender Antivirus for Mac στη γραμμή μενού και επιλέξτε Preferences.
   - Κάντε κλικ στο εικονίδιο στη γραμμή μενού και επιλέξτε Preferences.
   - Πατήστε Command- κόμμα (;).
3. Επιλέξτε την καρτέλα History.

Λεπτομέρειες σχετικά με τη δραστηριότητα του προϊόντος απεικονίζονται.

Μπορώ να ενημερώσω το Bitdefender Antivirus for Mac μέσω ενός Proxy Server?

To Bitdefender Antivirus for Mac μπορεί να πάρει 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 λάβει τις malware ενημερώσεις.

Πώς μπορώ να απεγκαταστήσω το Bitdefender Antivirus for Mac;

Για να αφαιρέσετε το Bitdefender Antivirus for Mac, ακολουθήστε τα εξής βήματα:

1. Άνοιξτε ένα Finder παράθυρο, μεταβείτε στο Applications φάκελο και επιλέξτε το Utilities.
2. Κάντε διπλό κλικ στο Bitdefender εφαρμογή κατάργηση εγκατάστασης.

3. Κάντε κλικ στο Uninstall για να συνεχίσετε.

4. Περιμένετε να ολοκληρωθεί η διαδικασία, στη συνέχεια κάντε κλικ Close για να τελειώσετε.

Σημαντικό
An υπάρχει κάποιο λάθος, μπορείτε να επικοινωνήσετε με την Bitdefender Εξυπηρέτηση Πελατών, όπως περιγράφεται στο "Ζητήστε βοήθεια" (p. 327).

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. Ανοίξτε το Mozilla Firefox browser σας.
   2. Πηγάνετε στο Tools και επιλέξτε Add-ons.
   3. Επιλέξτε Extensions στην αριστερή στήλη.
   4. Επιλέξτε την επέκταση και κάντε κλικ στο Remove.
   5. 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. Ανοίξτε το πρόγραμμα περιήγησης Google Chrome σας.
   2. Κάντε κλικ 🗿 στη γραμμή εργαλείων του προγράμματος περιήγησης.
   3. Πηγάνετε στο Tools και επιλέξτε Extensions.
   4. Επιλέξτε την επέκταση και κάντε κλικ στο Remove.
   5. Κάντε κλικ Uninstall για να επιβεβαιώσετε τη διαδικασία κατάργησης.

● Για να αφαιρέσετε το Bitdefender TrafficLight από το Safari, ακολουθήστε τα παρακάτω βήματα:
   1. Ανοίξτε το Safari browser σας.
2. Κάντε κλικ ☰ στη γραμμή εργαλείων του προγράμματος περιήγησης και κάντε κλικ στο Preferences.

3. Επιλέξτε το Extensions και βρείτε το Bitdefender TrafficLight στην Safari λίστα επεκτάσεων.

4. Επιλέξτε την επέκταση και κάντε κλικ στο Uninstall.

5. Κάντε κλικ Uninstall για να επιβεβαιώσετε τη διαδικασία κατάργησης.
MOBILE SECURITY ΓΙΑ ANDROID
13. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΠΡΟΣΤΑΣΙΑΣ

To Bitdefender Mobile Security & Antivirus προστατεύει την Android συσκευή σας με τα παρακάτω χαρακτηριστικά:

- Σαρωτής Κακόβουλου Λογισμικού
- Web Security
- Ιδιωτικότητα του λογαριασμού
- Anti-Theft, συμπεριλαμβανομένων:
  - Απομακρυσμένη τοποθεσία
  - Απομακρυσμένο κλείδωμα συσκευής
  - Απομακρυσμένη διαγραφή συσκευής
  - Απομακρυσμένες ειδοποιήσεις συσκευής
- Κλείδωμα Εφαρμογών
- Privacy Advisor
- 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.
14. ΞΕΚΙΝΩΝΤΑΣ

Απαιτήσεις Συσκευής

Bitdefender Mobile Security & Antivirus λειτουργεί σε κάθε συσκευή που έχει λογισμικό Android 4.0 και άνω. Απαιτείται ενεργή σύνδεση στο Internet για τη σάρωση κακόβουλου λογισμικού in-the-cloud.

Εγκατάσταση του Bitdefender Mobile Security & Antivirus

● Απο το Bitdefender Central

● Σε Android

2. Συνδεθείτε στον Bitdefender λογαριασμό σας.
3. Πατήστε στο εικονίδιο στην επάνω αριστερή γωνία της οθόνης, και στη συνέχεια επιλέξτε οι συσκευές μου.
4. Στο παράθυρο MY DEVICES πατήστε στο + εικονίδιο
5. Επιλέξτε Bitdefender Mobile Security από τη λίστα και, στη μετά, πατήστε GO TO GOOGLE PLAY.
6. Πατήστε ΕΓΚΑΤΑΣΤΑΣΗ στην οθόνη του Google Play.

● Σε Windows, macOS, iOS

2. Συνδεθείτε στον Bitdefender λογαριασμό σας.
3. Στο παράθυρο MY DEVICES κάντε κλικ στο INSTALL Bitdefender.
4. Επιλέξτε το Σε άλλη συσκευή link.
5. Επιλέξτε Android.
6. Επιλέξτε Bitdefender Mobile Security από τη λίστα και, στη μετά, πατήστε CONTINUE.
7. Πληκτρολογήστε μια διεύθυνση e-mail στο αντίστοιχο πεδίο και στη συνέχεια κάντε κλικ στο SEND.
8. Αποκτήστε πρόσβαση στο λογαριασμό e-mail σας από την Android συσκευή σας, στη συνέχεια, πατήστε το κουμπί GET IT ON Google Play.

Θα μεταφερθείτε στην Google Play εφαρμογή.

9. Πατήστε ΕΓΚΑΤΑΣΤΑΣΗ στην οθόνη του Google Play.

● Από το Google Play

Αναζητήστε το Bitdefender Mobile Security & Antivirus για να εντοπίσετε και να εγκαταστήσετε την εφαρμογή.

Εναλλακτικά, σαρώστε τον κωδικό QR:

Συνδεθείτε στον Bitdefender λογαριασμό σας

Για να χρησιμοποιήσετε το Bitdefender Mobile Security & Antivirus, θα πρέπει να συνδέσετε τη συσκευή σας σε ένα Bitdefender λογαριασμό ή σε ένα λογαριασμό Google, κάνοντας σύνδεση στο λογαριασμό μέσα από την εφαρμογή. Την πρώτη φορά που ανοίγετε την εφαρμογή, θα σας ζητηθεί να συνδεθείτε σε έναν λογαριασμό.

Εάν εγκαταστήσατε το Bitdefender Mobile Security & Antivirus από το Bitdefender λογαριασμό σας, η εφαρμογή θα προσπαθήσει να συνδεθεί αυτόματα σε αυτό το λογαριασμό.

Για να συνδέσετε τη συσκευή με το Bitdefender λογαριασμό:

1. Ανοίξτε το Bitdefender Mobile Security & Antivirus.

2. Πατήστε USE CENTRAL ACCOUNT, και μετά πληκτρολογήστε τον Bitdefender λογαριασμό, email διεύθυνση και κωδικό.
Σημείωση
Εάν δεν έχετε λογαριασμό, επιλέξτε τον αντίστοιχο σύνδεσμο. Για να συνδεθείτε χρησιμοποιώντας έναν λογαριασμό Google, πατήστε την επιλογή GOOGLE ACCOUNT.

3. Πατήστε ΣΥΝΔΕΣΗ.

Ενεργοποίηση Bitdefender Mobile Security & Antivirus

Για να είστε προστατευμένοι χρησιμοποιώντας το Bitdefender Mobile Security & Antivirus, 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.

Για να ενεργοποιήσετε το Bitdefender Mobile Security & Antivirus:
1. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Η εφαρμογή θα εμφανίσει πληροφορίες σχετικά με την τρέχουσα κατάσταση της συνδρομής.

Πατήστε ΕΧΩ ΕΝΑ ΚΩΔΙΚΟ.
3. Πληκτρολογήστε έναν κωδικό ενεργοποίησης στο αντίστοιχο πεδίο και πατήστε ΕΝΕΡΓΟΠΟΙΗΣΗ.

Για να επεκτείνετε την διαθέσιμη συνδρομή:
1. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το κουμπί Μενού και επιλέξτε ΠΛΗΡΟΦΟΡΙΕΣ ΛΟΓΑΡΙΑΣΜΟΥ από τη λίστα.
3. Στην ενότητα Extend subscription εισάγετε έναν κωδικό ενεργοποίησης και πατήστε ACTIVATE.

Εναλλακτικά, μπορείτε να επεκτείνετε την τρέχουσα συνδρομή σας χρησιμοποιώντας μια από τις διαθέσιμες προσφορές.

Ταμπλό

Πατήστε στο εικονίδιο Bitdefender Mobile Security & Antivirus στο πάνω μέρος της εφαρμογής της συσκευής σας για να ανοίξει το interface της εφαρμογής.
Το Ταμπλό προσφέρει πληροφορίες σχετικά με την κατάσταση της ασφάλειας της συσκευής σας και σας επιτρέπει να διαχειριστείτε εύκολα όλα τα χαρακτηριστικά ασφαλείας.

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 στα[Bitdefender Mobile Security & Antivirus χαρακτηριστικά και περιηγηθείτε εύκολα από τη μία ενότητα στην άλλη από το κουμπί Μενού που βρίσκεται στην επάνω αριστερή γωνία της οθόνης:

Σαρωτής Κακόβουλου Λογισμικού
Σας επιτρέπει να ξεκινήσετε μια σάρωση on-demand και να ενεργοποιήσετε ή να απενεργοποιήσετε την Σάρωση Αποθηκευτικού Μέσου. Για περισσότερες πληροφορίες, παρακολούμε αναφερθείτε στο “Σαρωτής Κακόβουλου Λογισμικού” (p. 293)

Web Security
Σας επιτρέπει να ενεργοποιήσετε ή να απενεργοποιήσετε το Web Security. Για περισσότερες πληροφορίες, παρακολούμε αναφερθείτε στο “ΠΡΟΣΤΑΣΙΑ Web” (p. 296)

Ιδιωτικότητα του λογαριασμού
Ελέγχει εάν έχει σημειωθεί διαρροή δεδομένων στους λογαριασμούς σας στο διαδίκτυο. Για περισσότερες πληροφορίες, παρακολούμε αναφερθείτε στο “Ιδιωτικότητα του λογαριασμού” (p. 298)

Anti-Theft
Σας επιτρέπει να ενεργοποιήσετε ή να απενεργοποιήσετε το Anti-Theft και να το ρυθμίσετε. Για περισσότερες πληροφορίες, παρακολούμε αναφερθείτε στο “Χαρακτηριστικά Anti-Theft” (p. 300)

Κλείδωμα Εφαρμογών
Σας επιτρέπει να προστατεύσετε τις εγκατεστημένες εφαρμογές σας με τον καθορισμό ενός κωδικού πρόσβασης PIN. Για περισσότερες πληροφορίες, παρακολούμε αναφερθείτε στο “Κλείδωμα Εφαρμογών” (p. 306)

Privacy Advisor
Σας προσφέρει πληροφορίες σχετικά με τις Android εφαρμογές έχουν εγκατασταθεί στη συσκευή σας και τις ενέργειες στο παρασκήνιο. Για
περισσότερες πληροφορίες, παρακολούμε αναφερθείτε στο "Privacy Advisor" (p. 312)

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, παρακολούμε αναφερθείτε στο "ΑΝΑΦΟΡΕΣ" (p. 314)

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, παρακολούμε αναφερθείτε στο "WearON" (p. 315)
15. ΣΑΡΩΤΉΣ ΚΑΚΌΒΟΥΛΟΥ ΛΟΓΙΣΜΙΚΟΥ

To Bitdefender προστατεύει τη συσκευή και τα δεδομένα από κακόβουλες εφαρμογές χρησιμοποιώντας σάρωση on-install και on-demand.

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 κάνετε εγκατάσταση μιας εφαρμογής, το Bitdefender Mobile Security & Antivirus σαρώνει αυτόματα χρησιμοποιώντας τεχνολογία in-the-cloud. Η ίδια διαδικασία σάρωσης ξεκινά κάθε φορά που ενημερώνονται οι εγκατεστημένες εφαρμογές.

Αυτός ο τύπος σάρωσης παρέχεται μέσω του Autopilot. Το Autopilot είναι ένας έξυπνος σαρωτής που σαρώνει όλες τις εφαρμογές που προσπαθείτε να εγκαταστήσετε ή να ενημερώσετε και σταματά τους ιούς.

Εάν η εφαρμογή είναι κακόβουλη, μια ειδοποίηση θα εμφανιστεί που θα σας ζητά να την απεγκαταστήσετε. Πατήστε Uninstall 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 on-demand.

Για να ξεκινήσετε μια σάρωση On-demand, απλά πατήστε στο κουμπί ΕΝΑΡΞΗ ΣΑΡΩΣΗΣ από την κάρτα Σαρωτής Κακόβουλου Λογισμικού που υπάρχει διαθέσιμη στο ταμπλό.

Εναλλακτικά, μπορείτε να εκτελέσετε μια σάρωση ακολουθώντας τα παρακάτω βήματα:

1. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το κουμπί Μενού και επιλέξτε Σαρωτής Κακόβουλου Λογισμικού από τη λίστα.
3. 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 μέρος στιγμή.

Από προεπιλογή, το Bitdefender Mobile Security & Antivirus 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. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το κουμπί Μενού και επιλέξτε Σαρωτής Κακόβουλου Λογισμικού από τη λίστα.
3. Πατήστε το αντίστοιχο διακόπτη.

Μπορείτε επίσης να ενεργοποιήσετε ή να απενεργοποιήσετε τη σάρωση αποθήκευσης από το Ρυθμίσεις πατώντας το κουμπί, και μετά τον αντίστοιχο διακόπτη.

Εάν εντοπιστούν τυχόν 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.
16. WEB SECURITY

Οι έλεγχοι ασφαλείας στο Web του Bitdefender πραγματοποιούνται μεσω των υπηρεσιών cloud που έχετε πρόσβαση με το προεπιλεγμένο πρόγραμμα περιήγησης Android, Google Chrome, Firefox, Opera, Opera Mini, Dolphin και τα ενσωματωμένα προγράμματα περιήγησης από εφαρμογές όπως το Facebook ή το Facebook Messenger. Μια πλήρης λίστα με τα υποστηριζόμενα προγράμματα περιήγησης διατίθεται στην ενότητα Ασφάλεια στο Web.

Αν ένα URL στοχεύει σε μία γνωστή phishing ή δόλια ιστοσελίδα, ή σε κακόβουλο περιεχόμενο, όπως spyware ή ιούς, η ιστοσελίδα είναι προσωρινά θα αποκλείεται και θα εμφανίζεται μια ειδοποίηση.

Στη συνέχεια μπορείτε να επιλέξετε να αγνοήσετε την προειδοποίηση και να προχωρήσετε στην ιστοσελίδα ή να επιστρέψετε σε μια ασφαλή σελίδα.

Σημείωση
Επιπλέον δικαιώματα απαιτούνται για το Android 6 για τη λειτουργία Web Security.

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.
To Web Security είναι ενεργοποιημένο

Web Security

Chrome
Dolphin
Messenger
Facebook
Firefox
17. ΙΔΙΩΤΙΚΟΤΗΤΑ ΤΟΥ ΛΟΓΑΡΙΑΣΜΟΥ

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 επικυρώση.

Οι αυτόματες επανέλεγκοι 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. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το κουμπί Μενού και επιλέξτε Εμπιστευτικότητα Λογαριασμού από τη λίστα.
3. Πατήστε τον μπλε κύκλο στην κάτω δεξιά γωνία της οθόνης.
4. Πληκτρολογήστε την e-mail διεύθυνσή σας στο αντίστοιχο πεδίο και στη συνέχεια κάντε κλικ στο ΕΠΟΜΕΝΟ.
   Το Bitdefender πρέπει να επικυρώσει αυτόν τον λογαριασμό πριν εμφανίσει ιδιωτικές πληροφορίες. Επομένως, αποστέλλεται ένα email με κωδικό επικύρωσης στην email διεύθυνση που ορίστηκε.
5. Ελέγξτε τα εισερχόμενα σας και, στη συνέχεια, πληκτρολογήστε τον κωδικό που λάβατε στην περιοχή Απόρρητο Λογαριασμού της εφαρμογής σας. Εάν δεν μπορείτε να βρείτε το email επικυρώσης 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 !.
18. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ 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.

Ακόμα και αν δεν μπορείτε να έχετε πρόσβαση στο Internet, μπορείτε να προστατέψετε τη συσκευή και τα δεδομένα σας με την αποστολή SMS commands από οποιοδήποτε κινητό τηλέφωνο στο smartphone σας μέσω κανονικών μηνυμάτων κειμένου.

Το Bitdefender Mobile Security & Antivirus προσφέρει τις ακόλουθες λειτουργίες Anti-Theft:

Απομακρυσμένη τοποθεσία
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.

Εμφάνιση IP
Εμφανίζει την τελευταία διεύθυνση IP για την επιλεγμένη συσκευή. Πατήστε SHOW IP ώστε να γίνει ορατή.
Απομακρυσμένη Διαγραφή
Αφαιρέστε όλα τα προσωπικά δεδομένα από την κλεμμένη συσκευή σας.

Απομακρυσμένο Κλείδωμα
Κλειδώστε την οθόνη του υπολογιστή σας και ορίστε έναν αριθμητικό κωδικό PIN για το ξεκλείδωμα του.

Αποστολή ειδοποίησης στη συσκευή (Scream)
Στείλετε ένα μήνυμα που θα εμφανίζεται στην οθόνη της συσκευής, από μακριά, 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 ολοκλήρωστε 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. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το κουμπί Μενού και επιλέξτε Anti-Theft από τη λίστα.
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:
Πατήστε Ενεργοποίηση Anti-Theft στη συνέχεια, πατήστε ΕΝΕΡΓΟΠΟΙΗΣΗ.

Επιτρέψτε δικαιώματα για τα εξής:

a. Επιτρέψτε το Antivirus να στέλνει και να βλέπει μηνύματα SMS;
b. Επιτρέψτε το Antivirus να αποκτήσει πρόσβαση στην τοποθεσία αυτής της συσκευής;
c. Επιτρέψτε το Antivirus να αποκτήσετε πρόσβαση στις επαφές σας;

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 βεβαιωθείτε ότι τυχόν αλλαγές που θα γίνουν στις ρυθμίσεις του Anti-Theft έχουν γίνει από εσάς, θα πρέπει να ορίσετε ένα PIN. Κάθε φορά που θα γίνεται μια προσπάθεια τροποποίησης των ρυθμίσεων Anti-Theft, ο κωδικός PIN θα πρέπει να εισάγεται πριν εφαρμοστούν οι αλλαγές. Εναλλακτικά σε συσκευές που υποστηρίζουν την επαλήθευση δακτυλικών αποτυπωμάτων, μπορεί να χρησιμοποιηθεί επιβεβαίωση δακτυλικών αποτυπωμάτων αντί του επιλεγμένου κωδικού PIN.

Σημείωση

Ο ίδιος κωδικός PIN χρησιμοποιείται από το App Lock για να προστατεύσει τις εγκατεστημένες εφαρμογές σας.

c. Ενεργοποίηση Στιγμιαία Φωτογράφιση

Κάθε φορά που κάποιος θα προσπαθήσει να αποκτήσει πρόσβαση στις εγκατεστημένες εφαρμογές σας ενώ είναι ενεργοποιημένη η επιλογή Στιγμιαία Φωτογράφιση, το Bitdefender θα τραβήξει ένα στιγμιότυπο του. Για περισσότερες λεπτομέρειες σχετικά με αυτό το χαρακτηριστικό, ανατρέξτε στο “Στιγμιαία Φωτογραφία” (p. 309).

d. Ορίστε αξιόπιστο αριθμό για το Anti-Theft

Επιλέξτε το SMS CONTROL πληκτρολογήστε έναν αξιόπιστο αριθμό τηλεφώνου ή επιλέξτε έναν από τη λίστα επαφών και στη συνέχεια πατήστε SAVE NUMBER. Ο αξιόπιστος αριθμός πρέπει να περιέχει
έναν κωδικό χώρας και πρέπει να είναι ο αριθμός κάποιος που
gνωρίζετε ή ο αριθμός άλλου τηλεφώνου που χρησιμοποιείτε.

Όταν μια διαφορετική κάρτα SIM εισάγεται στη συσκευή σας, το
Bitdefender Mobile Security & Antivirus στέλνει αυτόματα ένα μήνυμα
κειμένου στον αριθμό που έχετε επιλέξει ως αξιόπιστο με τον νέο
αριθμό τηλεφώνου.

Με αυτό τον τρόπο, μπορείτε να στείλετε εντολές SMS στο τηλέφωνό
σας, ακόμη και αν η κάρτα SIM έχει αλλαχθεί και ο αριθμός αλλάξει.

Σημαντικό
Αυτό δεν είναι υποχρεωτικό βήμα, αλλά συνιστάται να ορίσετε έναν
αξιόπιστο αριθμό κατά την αρχική ρύθμιση. Η εντολή ΔΙΑΓΡΑΦΗ
λειτουργεί μόνο όταν αποσταλεί από τον αριθμό που έχετε δηλώσει
ως αξιόπιστο

Μόλις ενεργοποιηθεί το Anti-Theft, μπορείτε να ενεργοποιήσετε ή να
απενεργοποιήσετε τις λειτουργίες ελέγχου Web και SMS ξεχωριστά από
την οθόνη Anti-Theft πατώντας τα αντίστοιχα κουμπιά.

Χρήση λειτουργιών Anti-Theft από το Bitdefender
Central (Web Control)

Σημείωση
Όλες οι λειτουργίες του Anti-Theft απαιτούν την επιλογή Background data
να είναι ενεργοποιημένη στις ρυθμίσεις χρήσης δεδομένων της συσκευής
σας.

Για να αποκτήσετε πρόσβαση στα Anti-Theft χαρακτηριστικά από το
Bitdefender λογαριασμό σας:
1. Πρόσβαση στο Bitdefender Central.
2. Πατήστε στο οικονόμιδι έπαινας αριστερής γωνία της οθόνης, και
στη συνέχεια επιλέξετε οι συσκευές μου.
3. Στην επιλογή MY DEVICES επιλέξτε την επιθυμητή κάρτα της συσκευής.
4. επιλέξτε το Anti-Theft πεδίο.
5. Στο πεδίο 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 συσκευής 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.

**Χρήση λειτουργιών Anti-Theft μέσω εντολών SMS (SMS Control)**

Μόλις ενεργοποιήθηκαν οι εντολές SMS, μπορείτε να στείλετε τις ακόλουθες εντολές στο smartphone σας μέσω SMS από οποιοδήποτε τηλέφωνο:

- **LOCATE** - στείλτε ένα μήνυμα που περιέχει τη θέση της συσκευής με τον αριθμό τηλεφώνου από τον οποίο εστάλη η εντολή. Το μήνυμα περιέχει μια σύνδεση Google Maps η οποία μπορεί να ανοιχθεί από το πρόγραμμα περιήγησης του κινητού τηλεφώνου.

- **SCREAM** - να παίξει ένα δυνατό ήχο στο ηχείο της συσκευής.

- **LOCK** - κλειδώστε την οθόνη της συσκευής με τον κωδικό PIN που έχετε ορίσει.

- **WIPE** - να διαγράψετε όλα τα δεδομένα από τη συσκευή σας.
Σημαντικό
Η εντολή ΔΙΑΓΡΑΦΗ λειτουργεί μόνο όταν αποσταλεί από τον αριθμό που 
έχετε δηλώσει ως αξιόπιστο

● CALLME - να καλέσετε τον αριθμό τηλεφώνου από τον οποίο η εντολή 
estάλη, σε ανοικτή ακρόαση. Με αυτό τον τρόπο μπορείτε να ακούσετε 
sωπηλά όποιον έχει το τηλέφωνο σας.
● HELP - να στείλετε ένα μήνυμα που περιέχει όλες τις διαθέσιμες εντολές 
στον αριθμό τηλεφώνου από τον οποίο εστάλη η εντολή.
● SIM Change - ο αξιόπιστος αριθμός που θα ορίσετε θα λάβει ένα SMS 
με τον νέο αριθμό τηλεφώνου μόλις αντικατασταθεί η κάρτα SIM με μια 
νέα. Για να ρυθμίσετε τον αριθμό τηλεφώνου του φίλου σας, πατήστε 
την επιλογή Έμπιστο νούμερο. Είτε πληκτρολογήστε τον αριθμό του, 
συμπεριλαμβανομένου του κωδικού χώρας, είτε επιλέξτε την κάρτα 
tου από τη λίστα επαφών.

Όλες οι εντολές SMS πρέπει να αποστέλλονται χρησιμοποιώντας την 
ακόλουθη μορφή:
bd-<PIN> <command>

Σημείωση
Οι αγκύλες υποδηλώνουν μεταβλητές και δεν θα πρέπει να εμφανίζονται 
stην εντολή.

Για παράδειγμα, εάν έχετε ορίσει έναν κωδικό PIN 123456 και θέλετε να 
lάβετε ένα μήνυμα με την τοποθεσία του τηλεφώνου σας, στείλτε το εξής 
mήνυμα κειμένου στον αριθμό τηλεφώνου σας:
BD-123456 LOCATE
19. ΚΛΕΪΔΩΜΑ ΕΦΑΡΜΟΓΩΝ

Εγκατεστημένες εφαρμογές όπως e-mail, φωτογραφίες, ή μηνύματα, μπορεί να περιέχουν προσωπικά δεδομένα που θα θέλατε να παραμείνουν προσωπικά περιορίζοντας επιλεκτικά την πρόσβασή 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 στο Ταμπλό μετά την ενεργοποίηση του Anti-Theft.

Εναλλακτικά, μπορείτε να ενεργοποιήσετε το App Lock ακολουθώντας τα παρακάτω βήματα:

1. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το κουμπί Μενού και επιλέξτε App Lock από τη λίστα.
3. Πατήστε ΕΝΕΡΓΟΠΟΙΗΣΗ, και κατόπιν επιτρέψτε την πρόσβαση στα δεδομένα χρήσης για το Bitdefender επιλέγοντας το αντίστοιχο πλαίσιο ελέγχου.

Σημείωση

Πρόσθετα δικαιώματα απαιτούνται για το Android 6 για τη λειτουργία στιγμαίας φωτογραφίας.

Για να την ενεργοποιήσετε, επιτρέψτε το Antivirus να παίρνει φωτογραφίες και βίντεο.

4. 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.

5. Ενεργοποιήστε την επιλογή Στιγμιαία Φωτογράφιση για να εντοπίσετε κάθε εισβολέα που θα προσπαθήσει να αποκτήσει πρόσβαση στα ιδιωτικά σας δεδομένα.

6. 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

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:

● Κλείδωμα κάθε φορά - ο κωδικός PIN ή το δακτυλικό αποτύπωμα που έχετε ρυθμίσει, θα πρέπει να χρησιμοποιείται κάθε φορά που θέλετε πρόσβαση στις κλειδωμένες εφαρμογές

● Ξεκλείδωμα ύστερα από τη θόλη σβήσει - η πρόσβαση στις εφαρμογές σας θα είναι έγκυρη μέχρι να απενεργοποιηθεί η οθόνη.
● Επιτρέψτε μια σύντομη έξοδο - μπορείτε να πραγματοποιήσετε έξοδο και να αποκτήσετε ξανά πρόσβαση στις ξεκλειδωμένες εφαρμογές σας μέσα σε 30 δευτερόλεπτα.

● Ενεργοποίηση έξυπνου ξεκλειδώματος - όταν είναι ενεργοποιημένη και συνδεθείτε σε δίκτυο που είναι αξιόπιστο, οι άλλες ρυθμίσεις δεν είναι διαθέσιμες. Αυτό σημαίνει ότι δεν απαιτείται επιβεβαίωση PIN ή δακτυλικών αποτυπωμάτων κατά την πρόσβαση στις κλειδωμένες εφαρμογές.

Ρυθμίσεις Κλειδώματος Εφαρμογών

Πατήστε το κουμπί στο μενού Χαρακτηριστικά App Lock, στη συνέχεια, επιλέξτε Ρυθμίσεις για μια διαμόρφωση του App Lock για προχωρημένους.

Με το App Lock Ρυθμίσεις μπορείτε να κάνετε τα εξής:

● Ενεργοποίηση Στιγμιαίας φωτογράφισης, όταν γίνουν τρεις αποτυχημένες προσπάθειες ξεκλειδώματος.

● Κλείδωμα ειδοποιήσεων για τις νέες εγκατεστημένες εφαρμογές.

● Αλλάξτε τον κωδικό PIN σας.

Στιγμιαία Φωτογραφία

Με την Bitdefender Στιγμιαία φωτογραφία, μπορείτε να ξαφνιάσετε τους φίλους ή τους συγγενείς σας. Με αυτό τον τρόπο μπορείτε να εκπαιδεύσετε τα περιέργα 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 εφαρμογογες 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 & Antivirus και κάνετε πρόσβαση στη λειτουργία App Lock.

Σημείωση

Αυτό το χαρακτηριστικό είναι διαθέσιμο μόνο για τα τηλέφωνα που έχουν μια μονόπλευρη κάμερα.
Για να ρυθμίσετε τη λειτουργία Στιγμιαίας φωτογράφησης:
1. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το Menu και επιλέξτε App Lock από τη λίστα.
3. Πατήστε το στο menu του App Lock, και μετά επιλέξτε Settings.
4. Ενεργοποίηση του Στιγμιαία φωτογραφία όταν γίνουν τρεις αποτυχημένες προσπάθειες ξεκλειδώματος. διακόπτη.

Εναλλακτικά, μπορούν να προβληθούν στον Bitdefender λογαριασμό:
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 από το ΟΙ ΣΥΣΚΕΥΕΣ ΜΟΥ και στη συνέχεια την καρτέλα Anti-Theft.

Oi φωτογραφίες εμφανίζονται.
oi 3 πιο πρόσφατες φωτογραφίες αποθηκεύονται μόνο.

**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 WiFi που συνήθως συνδέεστε και όταν συνδέεται με αυτά, το Lock App θα απενεργοποιηθεί για τις προστατευόμενες εφαρμογές.

Για να ενεργοποιήσετε τη λειτουργία Smart Unlock:
1. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το Menu και επιλέξτε App Lock από τη λίστα.
3. Επιλέξτε την καρτέλα ΛΕΙΤΟΥΡΓΙΑ ΚΛΕΙΔΩΜΑΤΟΣ και στη συνέχεια ενεργοποιήστε τον αντίστοιχο διακόπτη.

Εμφανίζεται το ασύρματο δίκτυο στο οποίο είστε συνδεδεμένοι.

Για να ρυθμίσετε τη σύνδεση WiFi που χρησιμοποιείτε αυτήν τη στιγμή ως αξιόπιστη, πατήστε το εικονίδιο.

**Σημείωση**
Αυτή η ρύθμιση είναι διαθέσιμη μόνο εάν είναι ενεργοποιημένη η λειτουργία Smart Unlock.

Κάθε φορά που αλλάζετε γνώμη, απενεργοποιήστε αυτή την δυνατότητα και τα δίκτυα WiFi που έχετε θέσει ως αξιόπιστα θα αντιμετωπίζονται ως μη αξιόπιστα.
20. PRIVACY ADVISOR

Το Privacy Advisor βασίζεται σε πληροφορίες ελέγχου από το Cloud για να προσφέρει συνεχώς έγκυρες πληροφορίες σχετικά με τις εφαρμογές του Android σας.

Οι περισσότερες εφαρμογές είναι νόμιμες, αλλά υπάρχουν και εφαρμογές που ίσως να εντοπίσουν τη θέση σας, την αποκτήσουν πρόσβαση και να μοιραστούν προσωπικές πληροφορίες σας. Το Privacy Advisor σας παρουσιάζει τα γεγονότα, αλλά τελικά εσείς θα είστε αυτός που θα πρέπει να αποφασίσει εάν μια εφαρμογή είναι ασφαλής να χρησιμοποιηθεί ή όχι.

Χρησιμοποιήστε το Privacy Advisor για να μάθετε περισσότερες πληροφορίες σχετικά με τις εφαρμογές που:
- έχουν πρόσβαση ή μεταφορτώνουν τις δικές σας επαφές στο cloud τους
- πιθανόν να μάθουν την πραγματική ταυτότητά σας
- να είναι απρόσεκτες, στέλνοντας τους κωδικούς πρόσβασης σας μέσω του Διαδικτύου και θέτοντας τους λογαριασμούς σας σε κίνδυνο
- πιθανόν να χρησιμοποιήσουν και να μεταφορτώσουν το μοναδικό αναγνωριστικό Συσκευής σας για να αναλύσουν τι κάνετε
- να συγκεντρώσουν αναλυτικά στοιχεία προκειμένου να σας παρακολουθούν
- Βρίσκουν την τοποθεσία σας
- εμφανίζουν διαφημίσεις
- Μπορεί να σας κοστίσει χρήματα

Πατήστε στο εικονίδιο του φίλτρου για να δείτε μια λίστα από τα πιο σημαντικά ιχνη.

Οι ακόλουθες πληροφορίες είναι διαθέσιμες σε αυτή τη λίστα:
- ποιές εφαρμογές είναι ιοί
- ποιές εφαρμογές αποστέλλουν την ταυτότητα σας σε αγνώστους.
- ποιες εφαρμογές χρησιμοποιούν πολύ ενοχλητικές διαφημίσεις
- Ποιες εφαρμογές αποστέλλουν τα προσωπικά σας δεδομένα σε αγνώστους.
ποιες εφαρμογές μπορεί να σας κοστίσουν χρήματα
ποιες εφαρμογές εφαρμογές στέλνουν τα δεδομένα σας κρυπτογραφημένα
ποιες εφαρμογές βρίσκουν την τοποθεσία σας
ποιες εφαρμογές έχουν πρόσβαση σε ευαίσθητα δεδομένα

Βαθμολογία Απορρήτου

Υπολογίζοντας τον Δείκτη Προστασίας Προσωπικών Δεδομένων για κάθε χρήστη, το Privacy Advisor παρέχει μια ακριβή και προσωπική επισκόπηση του πόσο ευάλωτοι είστε, έτσι ώστε να μπορείτε να αξιολογήσετε και να λάβετε τα κατάλληλα μέτρα για κάθε εγκατεστημένη εφαρμογή. Θα πρέπει να προσέξετε όταν ο Δείκτης Προστασίας Προσωπικών Δεδομένων είναι χαμηλός.

Εάν έχετε αμφιβολίες σχετικά με τις άδειες που απαιτούνται από μια συγκεκριμένη εφαρμογή, προσπαθήστε να βρείτε περισσότερες πληροφορίες σχετικά με αυτό πριν αποφασίσετε για το αν θα πρέπει ή όχι να συνεχίσετε να την χρησιμοποιείτε.
21. 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. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το κουμπί Μενού και επιλέξτε Αναφορές από τη λίστα.

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.

- **ΔΡΑΣΤΗΡΙΟΤΗΤΑ** - εδώ μπορείτε να ελέγξετε λεπτομερείς πληροφορίες σχετικά με τη δραστηριότητα της εφαρμογής σας Bitdefender Mobile Security & Antivirus από τότε που εγκαταστάθηκε στη συσκευή σας Android.

Για να διαγράψετε το διαθέσιμο αρχείο καταγραφής δραστηριότητας, πατήστε το κουμπί στην επάνω δεξιά γωνία της οθόνης. Και, στη συνέχεια, επιλέξτε ΔΙΑΓΡΑΦΗ ΔΡΑΣΤΗΡΙΟΤΗΤΑΣ.
22. 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 την εφαρμογή Bitdefender Mobile Security & Antivirus 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.

Εάν έχετε το SmartWatch μαζί σας, αυτό ανιχνεύει αυτόματα την εφαρμογή στο τηλέφωνο σας και δονείται κάθε φορά που βρίσκεστε σε απόσταση μικρότερη των δέκα μέτρων μακριά από τη συσκευή σας.

Για να ενεργοποιήσετε αυτή τη λειτουργία, ανοίξτε το Bitdefender Mobile Security & Antivirus, πατήστε Γενικές Ρυθμίσεις στο μενού και επιλέξτε το αντίστοιχο διακόπτη κάτω από την ενότητα WearON.

2. Συναγερμός Κραυγής

Το να βρείτε το τηλέφωνο σας δεν ήταν ποτέ ευκολότερο. Κάθε φορά που θα ξεχάσετε πού αφήσατε το τηλέφωνο σας, επιλέξτε την εντολή Scream στο ρολόι σας για να κάνετε το τηλέφωνο σας να φωνάξει.
23. 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 στο Bitdefender λογαριασμό από οποιονδήποτε υπολογιστή ή κινητή συσκευή που συνδέεται στο Internet μεταβαίνοντας στο https://central.bitdefender.com. Μόλις έχετε πρόσβαση σε αυτό, 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 & Antivirus
  ● 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

Για να αποκτήσετε πρόσβαση στον Bitdefender λογαριασμό σας, απλά:

1. Ανοίξτε ένα πρόγραμμα περιήγησης σε οποιαδήποτε συσκευή με πρόσβαση στο Διαδίκτυο.
3. Συνδεθείτε στο λογαριασμό σας χρησιμοποιώντας το e-mail σας και τον κωδικό πρόσβασης σας.

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 της συσκευής σας εμφανίζουν το όνομα της
συσκευής, το καθεστώς προστασίας και το υπόλοιπο διαθεσιμότητας της
συνδρομής σας.

Για να εντοπίσετε εύκολα τις συσκευές σας, μπορείτε να προσαρμόσετε
tο 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. Στο MY DEVICES κάντε κλικ στο εικονίδιο με την επιθυμητή κάρτα
   της συσκευής, στη συνέχεια επιλέξτε Settings.
4. Αλλάξτε το όνομα της συσκευής στο αντίστοιχο πεδίο, 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. Στο MY DEVICES κάντε κλικ στο εικονίδιο με την επιθυμητή κάρτα
   της συσκευής, στη συνέχεια επιλέξτε Profile.
4. Κάντε κλικ στο Add owner, στη συνέχεια, συμπληρώστε τα αντίστοιχα
   πεδία, ορίστε το φύλο, την ημερομηνία γέννησης και προσθέστε ακόμη
   μια εικόνα προφίλ.
5. Κάντε κλικ στο ADD για να αποθηκεύσετε ένα προφίλ.
6. Επλέξτε τον επιθυμητό ιδιοκτήτη από τη λίστα Device owner και στη
   συνέχεια κάντε κλικ στο ASSIGN.

Για περισσότερες ενέργειες εξ αποστάσεως 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
diαθέσιμες:

● Ταμπλώ. Σε αυτό το παράθυρο μπορείτε να ελέγξετe την κατάσταση
   της προστασίας των προϊόντων Bitdefender και τον αριθμό των ημερών

Bitdefender Total Security 2018
που απομένουν για τη συνδρομή σας. Το καθεστώς προστασίας μπορεί να είναι πράσινο, όταν δεν υπάρχει κανένα πρόβλημα που να επηρεάζει το προϊόν σας, ή κόκκινο όταν η συσκευή βρίσκεται σε κίνδυνο. Όταν υπάρχουν προβλήματα που αφορούν το προϊόν σας, κάντε κλικ στο View issues 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 SCAN 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 αυτό το χαρακτηριστικό, ανατρέξτε στο "Χαρακτηριστικά Anti-Theft" (p. 300).

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


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.
24. ΣΥΧΝΕΣ ΕΡΩΤΗΣΕΙΣ

Γιατί το Bitdefender Mobile Security & Antivirus απαιτεί σύνδεση στο Internet;

Η εφαρμογή θα πρέπει να επικοινωνήσει με τους Bitdefender servers προκειμένου να καθορίσει το καθεστώς ασφαλείας των εφαρμογών που σαρώνει και τις ιστοσελίδες που επισκέπτετε, 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 & Antivirus 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 Security διαγράφει κακόβουλες ιστοσελίδες από το ιστορικό περιήγησης.
- Διαβάστε τα αρχεία καταγραφής -> Το Bitdefender Mobile Security & Antivirus εντοπίζει ιχνη δραστηριότητας κακόβουλου λογισμικού από τα Android logs.
- Διαβάστε/Γράψτε SMS, επαφές, δεδομένα λογαριασμών και εξωτερικής αποθήκευσης μονάδας -> Απαιτείται για τη δυνατότητα απομακρυσμένης διαγραφής.
- Τοποθεσία -> απαιτείται για απομακρυσμένη τοποθεσία.
- Κάμερα -> απαιτείται για στιγμιαία φωτογραφία.
- Αποθήκευση -> χρησιμοποιεί για να επιτρέψει το Malware Scanner για να ελέγξει την κάρτα SD.

Πού μπορώ να δω τις λεπτομέρειες σχετικά με τη δραστηριότητα της εφαρμογής;
Το Bitdefender Mobile Security & Antivirus διατηρεί ένα αρχείο καταγραφής όλων των σημαντικών ενεργειών, αλλαγών κατάστασης και άλλων κρίσιμων μηνυμάτων που σχετίζονται με την δραστηριότητά του. Για να αποκτήσετε πρόσβαση σε αυτές τις πληροφορίες ανοίξτε το Bitdefender Mobile Security & Antivirus πατήστε το κουμπί Μenu, και στη συνέχεια, επιλέξτε Αναφορές από τη λίστα.

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. Στο MY DEVICES κάντε κλικ στο εικονίδιο με την επιθυμητή κάρτα της συσκευής, στη συνέχεια επιλέξτε Settings.
4. Ανακτήστε τον κωδικό PIN από το πεδίο PIN Εφαρμογής

Πώς το Bitdefender Mobile Security & Antivirus θα επηρεάσει την απόδοση και αυτονομία της μπαταρίας της συσκευής μου;

Κρατάμε την επίπτωση πολύ χαμηλά. Η εφαρμογή λειτουργεί μόνο όταν είναι απαραίτητο - μετά την εγκατάσταση μιας εφαρμογής, κατά την περιήγηση στο περιβάλλον της εφαρμογής ή όταν θέλετε έναν έλεγχο ασφαλείας. To Bitdefender Mobile Security & Antivirus δεν εκτελείται στο παρασκήνιο όταν καλείτε τους φίλους σας, πληκτρολογείτε ένα μήνυμα ή όταν παίζετε ένα παιχνίδι.

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;

An θέλετε να ορίσετε ένα άλλο ασύρματο δίκτυο ως αξιόπιστο:
1. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το κουμπί Μenu και επιλέξτε App Lock από τη λίστα.
3. Επιλέξτε την καρτέλα ΛΕΙΤΟΥΡΓΙΑ ΚΛΕΙΔΩΜΑΤΟΣ tab, και στη συνέχεια επιλέξτε το the εικονίδιο.
4. Επαληθεύστε το PIN ή το δακτυλικό αποτύπωμα για να επιβεβαιώσετε την επιλογή σας.

5. Πατήστε το εικονίδιο δίπλα στο δίκτυο που θέλετε να ορίσετε ως αξιόπιστο.

Τι μπορεί να μου πει ο Privacy Advisor σχετικά με τις εφαρμογές που εγκαθιστώ?

To Privacy Advisor σας λέει τι μπορεί να κάνει η κάθε εφαρμογή στο κινητό σας. Σας λέει αν μια εφαρμογή μπορεί να έχει πρόσβαση στα απόρρητα δεδομένα σας, να στείλει μηνύματα, να συνδεθεί στο Internet ή να εκτελέσει οποιαδήποτε άλλη λειτουργία που μπορεί μερικές φορές να δημιουργεί κινδύνους για την ασφάλεια σας.

Μπορώ να διαγράψω μια εφαρμογή που θεωρώ ότι είναι απειλή για την προστασία της ιδιωτικής ζωής μου;

Μπορείτε να αφαιρέσετε χειροκίνητα μια εφαρμογή χρησιμοποιώντας τον Privacy Advisor. Για να το κάνετε αυτό, πατήστε την εφαρμογή που επιθυμείτε, στη συνέχεια, πατήστε το κουμπί ΑΠΕΓΚΑΤΑΣΤΑΣΗ ΕΦΑΡΜΟΓΗΣ. Επιβεβαιώστε την επιλογή σας και περιμένετε τη διαδικασία απεγκατάστασης να ολοκληρωθεί.

Πώς απενεργοποιώ τις ειδοποιήσεις του Privacy Advisor?

Αν θέλετε να σταματήσετε να λαμβάνετε ειδοποιήσεις από τον Σύμβουλο Προστασίας Προσωπικών Δεδομένων:

1. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το κουμπί Μενού και επιλέξτε Ρυθμίσεις από τη λίστα.
3. Κάτω από την ενότητα Privacy Advisor, πατήστε στον αντίστοιχο διακόπτη.

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 ενημερωμένη την εφαρμογή προστασίας από ιούς.
- Υποβάλετε τις ηλεκτρονικές πληρωμές μόνο σε προστατευμένο περιβάλλον.
Χρησιμοποιήστε ένα 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://.

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. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το κουμπί Μενού και επιλέξτε Πληροφορίες λογαριασμού από τη λίστα.
3. Πατήστε LOGOUT, και στη συνέχεια επιβεβαιώστε την επιλογή σας.
4. Πατήστε USE CENTRAL ACCOUNT, και μετά πληκτρολογήστε τον νέο Bitdefender λογαρισμό, email διεύθυνση και κωδικό.

Τι είναι ο Device Administrator;

Ο Device Administrator είναι μία λειτουργία Android που δίνει στο Bitdefender Mobile Security & Antivirus 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.

Σε τι χρησιμεύει το αξιόπιστο νούμερο;

Εάν το τηλέφωνό σας πέσει στα χέρια κάποιου που δεν έχει καμία πρόθεση να το επιστρέψει στο νόμιμο ιδιοκτήτη του, είναι πιθανό ότι η κάρτα SIM θα αλλάξει γρήγορα. Κάθε φορά που το Bitdefender Mobile Security & Antivirus ανιχνεύει ότι η κάρτα SIM στο τηλέφωνό σας έχει αλλάξει, στέλνει αυτόματα ένα μήνυμα κειμένου που περιέχει το νέο αριθμό τηλεφώνου στον αριθμό που έχετε ορίσει. Με αυτό τον τρόπο, μπορείτε
να στείλετε εντολές SMS στο τηλέφωνό σας, ακόμη και αν η κάρτα SIM έχει αλλαχθεί και ο αριθμός αλλάξει. Αυτός μπορεί να είναι ο αριθμός τηλεφώνου κάποιου που γνωρίζετε και εμπιστεύεστε, ή ο αριθμός ενός άλλου τηλεφώνου που χρησιμοποιείτε.

Μπορεί να αλλάξει ο αξιόπιστος αριθμός αφού τον ορίσως; 
Για να ορίσετε έναν διαφορετικό αξιόπιστο αριθμό:
1. Ανοίξτε το Bitdefender Mobile Security & Antivirus.
2. Πατήστε το κουμπί Μενού και επιλέξτε Ρυθμίσεις από τη λίστα.
3. Κάτω από την ενότητα Anti-Theft, πατήστε το Αξιόπιστος αριθμός.

Θα σας ζητηθεί να δώσετε τον κωδικό PIN για να μπορέσετε να αλλάξετε τον αξιόπιστο αριθμό.

Πόσο θα μου κοστίσει να στείλω εντολές SMS; 
Οι εντολές SMS αποστέλλονται ως κανονικά μηνύματα κειμένου και ως εκ τούτου, χρεώνονται με το ίδιο τρόπο από τον φορέα σας. Το Bitdefender δεν έχει καμία επιπλέον χρέωση.

Πως να διορθώσω το σφάλμα "No Google Token" το οποίο εμφανίζεται όταν συνδέομαι στο Bitdefender Mobile Security & Antivirus.

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. Συχνές Ερωτήσεις

324

Bitdefender Total Security 2018
Σε ποιες γλώσσες είναι διαθέσιμο το Bitdefender Mobile Security & Antivirus;

Το Bitdefender Mobile Security & Antivirus είναι αυτή τη στιγμή διαθέσιμο στις ακόλουθες γλώσσες:

- Βραζιλία
- Ολλανδία
- Αγγλικά
- Γαλλικά
- Γερμανικά
- Ελληνικά
- Ιταλικά
- Ιαπωνικά
- Κορεάτικα
- Πολωνικά
- Πορτογαλικά
- Ρουμανικά
- Ρωσικά
- Ισπανικά
- Ταϊλανδικά
- Τουρκικά
- Βιετναμέζικα

Επιπλέον γλώσσες θα προστεθούν σε μελλοντικές εκδόσεις. Για να αλλάξετε τη γλώσσα της πλατφόρμας του Bitdefender Mobile Security & Antivirus, μεταβείτε στη συσκευή σας στη ρύθμιση Γλώσσα & πληκτρολογίου και ρυθμίστε τη συσκευή στη γλώσσα που θέλετε να χρησιμοποιήσετε.
ΣΤΕΙΛΤΕ ΜΑΣ ΤΑ ΣΧΟΛΙΑ ΣΑΣ
25. ΖΗΤΗΣΕΤΕ ΒΟΗΘΕΙΑ

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. Αντιπρόσωποι μας θα απαντήσουν στις ερωτήσεις σας εγκαίρως και θα σας δώσουν τη βοήθεια που χρειάζεστε.

Το “Επίλυση κοινών ζητημάτων” (p. 210) 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 πηγές, πάτε στο https://www.bitdefender.com/support/contact-us.html για να επικοινωνήσετε με τους εκπροσώπους υποστήριξης.

Μπορείτε επίσης να ελέγξετε το “Online πηγές” (p. 329) μας για περισσότερες συμβουλές ή πληροφορίες σχετικά με όλα τα Bitdefender προϊόντα.

Επικοινωνήστε μαζί μας άμεσα από το Bitdefender Total Security προϊόν σας

Εάν έχετε μια ενεργή σύνδεση στο Internet, μπορείτε να επικοινωνήσετε με το Bitdefender για απευθείας βοήθεια από το περιβάλλον του προϊόντος. Ακολουθείτε αυτά τα βήματα:

1. Κάντε κλικ στο εικονίδιο στην αριστερή μπάρα του Bitdefender interface.
2. Έχετε τις εξής επιλογές:
   ● Τεκμηρίωση του προϊόντος
     Αποκτήστε πρόσβαση στις βάσεις δεδομένων μας και ψάξτε τις απαραίτητες πληροφορίες.
   ● Επικοινωνήστε με την υποστήριξη
     Χρησιμοποιήστε το κουμπί Επικοινωνία στήριξης για την έναρξη του Εργαλείου Υποστήριξης του Bitdefender και επικοινωνήστε με το
Τμήμα Εξυπηρέτησης Πελατών. Μπορείτε να περιηγηθείτε μέσα από τον οδηγό χρησιμοποιώντας το κουμπί Επόμενο. Για να βγείτε από τον οδηγό, κάντε κλικ στο Άκυρο.

a. Επιλέξτε τους όρους στο κουτί επιλογής και κάντε κλικ στο Επόμενο.

b. Συμπληρώστε τη φόρμα υποβολής με τα απαραίτητα στοιχεία:
   i. Εισάγετε τη διεύθυνση e-mail σας.
   ii. Εισάγετε το πλήρες όνομά σας.
   iii. Πληκτρολογήστε μια περιγραφή του προβλήματος που αντιμετωπίσατε.
   iv. Ελέγξτε την επιλογή Προσπαθήστε να αναπαραγάγετε το ζήτημα πριν από την υποβολή σε περίπτωση που αντιμετωπίζετε ένα ζήτημα σχετικό με το προϊόν. Συνεχίστε με τα απαιτούμενα βήματα.

c. 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.

d. Κάντε κλικ στο Τέλος για την αποστολή πληροφοριών στο Τμήμα Εξυπηρέτησης Πελατών του Bitdefender. Θα επικοινωνήσουμε μαζί σας το συντομότερο δυνατό.

● Βρείτε βοήθεια online

Πρόσβαση στα onlineάρθρα μας.
26. ONLINE ΠΗΓΕΣ

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.

26.1. 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 bugfixing δραστηριότητες των ομάδων στήριξης και ανάπτυξης του Bitdefender, καθώς και περισσότερα γενικά άρθρα σχετικά με την πρόληψη του ιού, τη διαχείριση των λύσεων του Bitdefender με λεπτομερείς εξηγήσεις, και πολλά άλλα αντικείμενα.

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 βρίσκονται 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.

26.2. 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 συγκεκριμένους ιούς 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 υποστηρίξες 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.


26.3. HOTforSecurity Portal

Το HOTforSecurity είναι μια πλούσια πηγή πληροφοριών για την ασφάλεια του υπολογιστή. Εδώ μπορείτε να μάθετε για τις διάφορες απειλές που είναι εκτεθειμένοι 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.

27. ΠΛΗΡΟΦΟΡΙΕΣ ΕΠΙΚΟΙΝΩΝΙΑΣ

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.

27.1. 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 Ιών: virus_submission@bitdefender.com
Υποβολή Spam: spam_submission@bitdefender.com
Αναφορά κατάχρησης: abuse@bitdefender.com
Ιστοσελίδα: https://www.bitdefender.com

27.2. 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:

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 e-mail στη διεύθυνση sales@bitdefender.com. Παρακαλούμε γράψτε το e-mail σας στα αγγλικά, προκειμένου να είμαστε σε θέση να σας βοηθήσουμε άμεσα.
27.3. 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](https://www.bitdefender.com/support/consumer.html)
Web: [https://www.bitdefender.com](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/](https://www.bitdefender.co.uk/support/)
Web: [https://www.bitdefender.co.uk](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](https://www.bitdefender.de/support/consumer.html)
Web: [https://www.bitdefender.de](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
Ιστοσελίδα: https://www.bitdefender.es

Ρουμανία

BITDEFENDER SRL
Complex DV24, Building A, 24 Delea Veche Street, Sector 2
Bucharest
Fax: +40 21 2641799
Τηλέφωνο Πωλήσεων: +40 21 2063470
E-mail Πωλήσεων: sales@bitdefender.ro
Τεχνική Υποστήριξη: https://www.bitdefender.ro/support/consumer.html
Ιστοσελίδα: https://www.bitdefender.ro

Ηνωμένα Αραβικά Εμιράτα

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Τηλέφωνο Πωλήσεων: 00971-4-4588935 / 00971-4-4589186
E-mail Πωλήσεων: mena-sales@bitdefender.com
Τεχνική Υποστήριξη: https://www.bitdefender.com/support/consumer.html
Ιστοσελίδα: https://www.bitdefender.com
Γλώσσαρι

**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, χρησιμοποιώντας 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 οποία 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 οποία δηλώνει το σκοπό της εφαρμογής με αποτέλεσμα να μην διαπράττεται κανένα αδίκημα.

Ωστόσο, οι αναδυόμενες διαφημίσεις μπορούν να γίνουν ενοχλητικές και σε ορισμένες περιπτώσεις να υποβαθμίσουν την απόδοσή 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 οποία 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.
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 και 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.

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 παρακολούθουν 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 δήλωσε ότι σας ενδιαφέρει. Είναι δίκοπο μαχαίρι για πολλούς ανθρώπους από τη μία πλευρά, είναι αποτελεσματική και πάντα επίκαιρη, καθώς βλέπετε διαφημίσεις μόνο για ότι σας ενδιαφέρει. Από την άλλη προκείται 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 προσβλημένοι από την ιδέα ότι θεωρούνται ως “αριθμός SKU” (to bar code στο πίσω μέρος των συσκευασιών που σκανάρεται στο ταμείο του παντοπωλείου). Ενώ αυτή η άποψη μπορεί να είναι ακριβία, σε ορισμένες περιπτώσεις είναι ακριβής.

E-mail
Το ηλεκτρονικό ταχυδρομείο. Μια υπηρεσία που στέλνει μηνύματα σε υπολογιστές μέσω τοπικών ή παγκόσμιων 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)

Το keylogger είναι μια εφαρμογή που καταγράφει ό, τι 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 ιού υπολογιστών που κωδικοποιείται ως μακροεντολή ενσωματωμένο 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.

Malware

Ένα πρόγραμμα ή ένα κομμάτι του κώδικα που έχει φορτωθεί στον υπολογιστή σας χωρίς τη γνώση σας και εκτελείται ενάντια στη θέλησή σας. Οι περισσότεροι ιοί μπορούν επίσης να αναπαράγουν τον εαυτό τους. Ολοι οι ιοί υπολογιστών είναι ανθρωπογενειές. Ένας απλός ιός που μπορεί να αντιγράψει το ίδιο του τον εαυτό του και ξανά είναι σχετικά εύκολο να παραχθεί. Ακόμη και ένας τέτοιος απλός ιός είναι
επικίνδυνος επειδή θα χρησιμοποιήσει γρήγορα όλη τη διαθέσιμη μνήμη και να φέρει το σύστημα σε αδιέξοδο. Ένα ακόμη πιο επικίνδυνο είδος ιού είναι ένας που είναι ικανός να εκπέμπει ο ίδιος σε όλα τα δίκτυα και παρακάμπτει τα συστήματα ασφάλειας.

Non-heuristic (μη- ευρετικό)

Αυτή η μέθοδος σάρωσης στηρίζεται σε συγκεκριμένες υπογραφές ιών Το πλεονέκτημα της μη ευρετικής σάρωσης είναι ότι δεν ξεγέλιεται από ό,τι φαίνεται ότι θα μπορούσε να είναι ίδιος, και δεν παράγει ψευδείς συναγερμούς.

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 οποίους 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 καινοτόμας μη παρεμβατική τεχνολογία της Bitdefender, που αποσκοπεί στην ελαχιστοποίηση της επίδρασης στην απόδοση του υπολογιστή εξαιτίας της λειτουργίας προστασίας από ιούς. 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 ανεπιθύμητους 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 υπολογιστές, 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 κακόβουλο λογισμικό, τα rootkits συνιστούν σοβαρή απειλή για την εκκρεμότητα 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 δωρεάν (freeware) ή με δωρεάν δοκιμαστική χρήση (shareware) προγράμματα που μπορεί να κατεβάζεται 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 δούρειο ίππο (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 omότιμο δίκτυο (peer-to-peer) από τα διαθέσιμα σήμερα.

Εκτός από τα ζητήματα της ηθικής και της ιδιωτικότητας, το spyware κλέβει από το χρήστη 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 σύστημα ή και τη γενική αστάθεια του συστήματος.

TCP/IP


Trojan

Ένα καταστροφικό πρόγραμμα το οποίο μεταμφιέζεται ο καλοήθης εφαρμογή. Σε αντίθεση με τους ιούς, οι Trojans δεν αυτοαντιγράφονται αλλά μπορούν να είναι το ίδιο καταστροφικοί. Ένας από τους πιο ύπους τύπους των Trojan horse είναι ένα πρόγραμμα που ισχυρίζεται ότι θα απαλλάξει τον υπολογιστή σας από ιούς, αλλά αντ’αυτού εισάγει αυτούς στον υπολογιστή σας.

Ο όρος προέρχεται από μια ιστορία στην Ιλιάδα του Ομήρου, στην οποία ο Έλληνες δίνουν ένα τεράστιο ξύλινο άλογο στους εχθρούς, τους

Γλωσσάρι 339
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 άλογου 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.

**Χρήση Μνήμης**

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 έχεται με ένα συγκεκριμένο ποσό φυσικής μνήμης, που συνήθως αναφέρεται ως κύρια μνήμη ή RAM.

**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.

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.

Οι διαδρομές μεταξύ δύο σημείων, όπως το κανάλι επικοινωνίας μεταξύ δύο υπολογιστών.

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.

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.
Ένας ιός που αλλάζει μορφή με κάθε αρχείο που μολύνει. Δεδομένου ότι δεν διαθέτουν συνεπές δυαδικό μοτίβο (binary pattern), τέτοιοι ιόι είναι δύσκολοι 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 αυτού του malware.
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 του ιού στο δίκτυο είναι μέσω ενός αρχείου PDF ή ενός εγγράφου του Office που μοιάζει ακίνδυνο έτσι ώστε ο κάθε χρήστης μπορεί 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 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 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 εξαρτάται από τον χρήστη κατά την πρώτη αγορά.
Τομέας Εκκίνησης:
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
eπίσης ένα πρόγραμμα που φορτώνει το λειτουργικό σύστημα.

Τός τομέα εκκίνησης
Ένας ιός που μολύνει τον τομέα εκκίνησης ενός σταθερού δίσκου ή
dισκέτα. Μια προσπάθεια να εκκινήσετε από μια δισκέτα που έχουν
μολυνθεί με τον ιό τομέα εκκίνησης θα καταλήξει στην ενεργοποίηση
tου ιού στη μνήμη. Κάθε φορά που θα εκκινήσετε το σύστημά σας από
το σημείο αυτό και μετά, θα έχετε τον ιό ενεργό στη μνήμη.

Υπογραφές ιών
Το δυαδικό μοτίβο ενός ιού, χρησιμοποιείται από το πρόγραμμα
προστασίας από ιούς για τον εντοπισμό και την εξάλειψη του ιού.

Ψευδώς θετικά
Συμβαίνει όταν ένας σαρωτής εντοπίζει ένα αρχείο ως μολυσμένο,
eνώς 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.

eυρετική
Μια βασισμένη σε κανόνες μέθοδος εντοπισμού νέων ιών . Αυτή η
μέθοδος σάρωσης δεν στηρίζεται σε συγκεκριμένες υπογραφές ιών.
Το πλεονέκτημα της ευρετικής σάρωσης (heuristic) είναι ότι δεν
ξεγελίεται από μια νέα παραλλαγή ενός υπάρχοντος ιού. 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 (περιγηγητής) 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 περιορίζονται 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).