bitdefender
INTERNET SECURITY 2011

Manual de utilizare

Copyright© 2010 BitDefender

BitDefender Internet Security 2011
Manual de utilizare

Publicat 2010.09.21

Copyright© 2010 BitDefender

Termeni legali

Toate drepturile rezervate. Nicio parte a acestui document nu va putea fi reprodusă sau transmisă sub nicio formă și prin niciun mijloc, fie el electronic sau mecanic, inclusiv fotocopiere, înregistrare, sau orice sistem de stocare și recuperare de date, fără acordul scris al unui reprezentant autorizat al BitDefender. Este posibilă includerea unor scurte citate în recenzii, dar numai cu condiția menționării sursei citate. Conținutul documentului nu poate fi modificat în niciun fel.

Avertisment și declinarea responsabilității. Acest produs și documentația aferentă sunt protejate de legea drepturilor de autor. Informațiile incluse în acest document sunt furnizate „ca atare", fără nicio garanție. Deși s-au luat toate măsurile de prevedere în momentul alcătuirii acestui document, autorii săi nu vor fi în niciun fel ținuți responsabili față de nicio persoană fizică sau juridică pentru pierderi sau daune cauzate sau care se presupune a fi fost cauzate, direct sau indirect, de informațiile cuprinse în acest material.

Acest document conține linkuri către siteuri web aparținând unor terți, care nu se află sub controlul BitDefender; prin urmare, BitDefender nu este responsabilă pentru conținutul respectivelor siteuri. Responsabilitatea accesării oricăruia dintre siteurile terților al căror link este furnizat în acest document vă aparține în totalitate. Aceste linkuri sunt furnizate exclusiv pentru ușurarea consultării documentului și prezența lor nu presupune faptul că BitDefender susține sau își asumă responsabilitatea pentru conținutul siteurilor către care duc acestea.

Mărci înregistrate. Acest manual poate conține nume de mărci înregistrate. Toate mărcile comerciale înregistrate sau neînregistrate din acest document aparțin exclusiv proprietarilor acestora și sunt redate ca atare.

bitdefender

Cuprins

Instalare și dezinstalare 1

1. Cerințe de sistem 2
1.1. Cerințe de sistem minime 2
1.2. Cerințe de sistem recomandate 2
1.3. Cerințe software 2

2. Pregătirea pentru instalare 4

3. Instalarea BitDefender 5
3.1. Pasul 1 - Introducere 5
3.2. Pasul 2 - Pregătirea instalării 5
3.3. Pasul 3 - Înregistrare 7
3.4. Pasul 4 - Selectarea modului de vizualizare 9
3.5. Pasul 5 - Configurare 10
3.6. Pasul 6 - Opțiuni de asistență 15
3.7. Pasul 7 - Confirmare 15
3.8. Pasul 8 - Finalizare 15

4. Actualizarea unei versiuni anterioare a BitDefender 17

5. Repararea sau dezinstalarea BitDefender 18

Introducere 19

6. Descriere generală 20
6.1. Deschiderea BitDefender 20
6.2. Iconița din bara de sistem 20
6.3. Bara de scanare 21
6.3.1. Scanare fișiere și directoare 22
6.3.2. Dezactivarea/Reactivarea barei de scanare 22
6.4. Detecție automată unități 23

7. Fereastra principală a aplicației 25
7.1. Modul Novice 25
7.1.1. Zona de stare 26
7.1.2. Zona Protejați-vă calculatorul 27
7.1.3. Zona de ajutor 27
7.2. Modul Intermediar 27
7.2.1. Stare 28
7.2.2. Securitate 29
7.2.3. Rețea 30
7.3. Modul Expert 30

8. Instrumentele mele 33

9. Alerte și ferestre pop-up 36
9.1. Alerte antivirus 36
9.2. Alerte Active Virus Control 37

9.3. Alerte privind detectarea dispozitivelor ... 37
9.4. Ferestre pop-up și alerte referitoare la firewall ... 38
9.5. Alerte Antiphishing ... 39
9.6. Mesaje de alertă privind Controlul parental ... 40
9.7. Alerte privind controlul datelor personale ... 40
9.7.1. Alerte regiștri ... 40
9.7.2. Alerte de scripturi ... 41
9.7.3. Alerte fișiere cookie ... 41
10. Remedierea problemelor ... 42
10.1. Asistentul de remediere a problemelor ... 42
10.2. Configurarea alertelor de stare ... 43
11. Configurarea setărilor principale ... 45
11.1. Setări de securitate ... 45
11.2. Setări alerte ... 47
11.3. Setări generale ... 48
11.4. Reconfigurarea profilului de utilizare ... 49
12. Istoric și evenimente ... 51
13. Înregistrare și Contul meu ... 52
13.1. Înregistrarea BitDefender Internet Security 2011 ... 52
13.2. Activarea BitDefender ... 53
13.3. Achiziționarea sau reînnoirea unei serii de înregistrare ... 55
Configurare și administrare ... 56
14. Setări generale ... 57
15. Protecție antivirus ... 61
15.1. Protecție în timp real ... 61
15.1.1. Reglarea nivelului de protecție în timp real ... 62
15.1.2. Crearea unui nivel de protecție personalizat ... 63
15.1.3. Modificarea acțiunilor aplicate fișierelor detectate ... 64
15.1.4. Restaurarea setărilor implicite ... 65
15.1.5. Configurarea setărilor Active Virus Control ... 66
15.1.6. Configurarea sistemului de detectare a intruziunilor ... 68
15.2. Scanarea la cerere ... 68
15.2.1. Scanarea fișierelor și directoarelor ... 69
15.2.2. Programul asistent de scanare ... 70
15.2.3. Examinarea rapoartelor de scanare ... 73
15.2.4. Administrarea sarcinilor de scanare existente ... 73
15.3. Configurarea excepțiilor de scanare ... 80
15.3.1. Excluderea fișierelor sau directoarelor de la scanare ... 80
15.3.2. Excluderea extensiilor de fișiere de la scanare ... 82
15.3.3. Administrarea excepțiilor de scanare ... 83
15.4. Zona de carantină ... 83
16. Protecție antiphishing ... 86
16.1. Configurarea listei albe antiphishing ... 86

16.2. Administrarea protecției antiphishing BitDefender din Internet Explorer și Firefox ... 86
17. Consilier pentru căutare ... 88
17.1. Dezactivarea Consilierului pentru căutare ... 88
18. Antispam ... 89
18.1. Detalii privind modulul Antispam ... 89
18.1.1. Filtrele Antispam ... 89
18.1.2. Funcționarea modulului Antispam ... 91
18.1.3. Actualizări Antispam ... 92
18.2. Asistentul de optimizare Antispam ... 92
18.3. Utilizarea barei de instrumente antispam din fereastra clientului de e-mail ... 94
18.3.1. Indicarea erorilor de detecție ... 95
18.3.2. Indicarea mesajelor spam nedetectate ... 96
18.3.3. Resetarea Motorului de învățare (bayesian) ... 96
18.3.4. Salvarea și încărcarea bazei de date bayesiane ... 97
18.3.5. Configurarea setărilor generale ... 97
18.4. Reglarea nivelului de protecție ... 97
18.5. Configurați lista de prieteni ... 98
18.6. Configurarea listei de spammeri ... 99
18.7. Configurarea filtrelor și setărilor antispam ... 100
19. Control parental ... 102
19.1. Configurarea Controlului parental ... 102
19.1.1. Protejarea setărilor de Control parental ... 104
19.1.2. Control Web ... 105
19.1.3. Controlul aplicațiilor ... 107
19.1.4. Control cuvinte cheie ... 108
19.1.5. Controlul mesageriei instant ... 110
19.2. Monitorizarea activității copiilor ... 111
19.2.1. Verificarea jurnalelor de Control parental ... 111
19.2.2. Configurarea notificărilor prin e-mail ... 112
19.3. Control parental la distanță ... 114
19.3.1. Condiții preliminare privind utilizarea Controlului parental la distanță ... 114
19.3.2. Activarea Controlului parental la distanță ... 114
19.3.3. Accesarea Controlului parental la distanță ... 115
19.3.4. Monitorizarea activităților copiilor dumneavoastră de la distanță ... 115
19.3.5. Modificarea setărilor Controlului parental la distanță ... 116
20. Control date ... 119
20.1. Configurarea nivelului de protecție ... 119
20.2. Control identitate ... 120
20.2.1. Despre Controlul identității ... 120
20.2.2. Configurarea Controlului identității ... 122
20.2.3. Administrarea regulilor ... 124
20.3. Control regiștri ... 124
20.4. Controlul fișierelor cookie ... 125
20.5. Control scripturi ... 126

21. Firewall 128
21.1. Setări de protecție 128
21.1.1. Setarea acțiunii implicite 128
21.1.2. Configurarea setărilor avansate de firewall 129
21.2. Reguli privind accesul la aplicații 130
21.2.1. Se vizualizează regulile curente 130
21.2.2. Adăugarea automată a regulilor 132
21.2.3. Adăugarea manuală a regulilor 132
21.2.4. Adminstrarea avansată a regulilor 135
21.2.5. Ștergerea și resetarea regulilor 136
21.3. Setări rețea 136
21.3.1. Zone de rețea 137
21.4. Dispozitive 138
21.5. Control conexiuni 138
21.6. Depanarea firewallului 139
22. Vulnerabilitate 141
22.1. Căutare după vulnerabilități 141
22.2. Stare 142
22.3. Opțiuni 142
23. Criptare chat 144
23.1. Dezactivarea criptării pentru anumiți utilizatori 145
23.2. Bara de instrumente BitDefender din fereastra de chat 145
24. Modul pentru jocuri / laptop 146
24.1. Modul pentru jocuri 146
24.1.1. Configurarea modului pentru jocuri automat 147
24.1.2. Administrarea listei de jocuri 147
24.1.3. Adăugarea sau editarea jocurilor 148
24.1.4. Configurarea setărilor modului pentru jocuri 148
24.1.5. Schimbarea combinației de taste 148
24.2. Modul pentru laptop 149
24.2.1. Configurarea setărilor modului pentru laptop 149
24.3. Mod silențios 150
24.3.1. Configurarea acțiunii pe întreg ecranul 150
24.3.2. Configurarea setărilor modului silențios 151
25. Rețea personală 152
25.1. Activarea rețelei BitDefender 152
25.2. Adăugarea calculatoarelor la rețeaua BitDefender 153
25.3. Administrarea rețelei BitDefender 153
26. Actualizare 156
26.1. Efectuarea unei actualizări 156
26.2. Configurarea setărilor de actualizare 157
26.2.1. Configurarea locațiilor de actualizare 158
26.2.2. Configurarea actualizării automate 158
26.2.3. Configurarea actualizării manuale 158
26.2.4. Configurarea setărilor avansate 159

Ghid de instrucțiuni 160
27. Cum scanez fișiere și directoare? 161
27.1. Utilizând meniul contextual Windows 161
27.2. Utilizând sarcini de scanare 161
27.3. Utilizând bara de scanare 162
28. Cum creez o sarcină de scanare personalizată? 164
29. Cum programez o scanare a calculatorului? 166
30. Cum creez conturi de utilizator Windows? 168
31. Cum actualizez BitDefender printr-un server proxy? 169
32. Cum trec la un produs superior din gama BitDefender 2011? ... 170
Depanare probleme și asistență profesională 171
33. Depanarea problemelor 172
33.1. Probleme la instalare 172
33.1.1. Erori de validare a instalării 172
33.1.2. Instalare eșuată 173
33.2. Sistemul meu funcționează lent 174
33.3. Nu începe scanarea 175
33.4. Nu mai pot utiliza o aplicație 176
33.5. Nu mă pot conecta la internet 176
33.6. Nu pot utiliza imprimanta 177
33.7. Nu pot partaja fișiere cu un alt calculator 179
33.8. Conexiunea mea la internet este lentă 180
33.9. Cum să actualizați BitDefender în cazul unei conexiuni lente la internet ... 181
33.10. Calculatorul meu nu este conectat la internet. Cum actualizez BitDefender? 181
33.11. Serviciile BitDefender nu răspund 182
33.12. Filtrul Antispam nu funcționează corect 182
33.12.1. Mesaje legitime sunt marcate ca [spam] 183
33.12.2. Multe mesaje spam nu sunt detectate 186
33.12.3. Filtrul antispam nu detectează niciun mesaj spam 188
33.13. Nu s-a reușit dezinstalarea BitDefender 189
34. Eliminarea virușilor din sistem 191
34.1. BitDefender Rescue CD 191
34.2. Ce trebuie să fac atunci când BitDefender găsește viruși pe calculatorul meu? 192
34.3. Cum șterg un virus dintr-o arhivă? 193
34.4. Cum șterg un virus dintr-o arhivă de e-mail? 194
34.5. Cum scanez calculatorul în Safe Mode? 195
34.6. Ce este de făcut atunci când BitDefender a detectat un fișier curat ca fiind infectat? 196
34.7. Cum să curățați fișierele infectate din System Volume Information 196
34.8. Ce reprezintă fișierele protejate prin parolă din jurnalele de scanare? 197
34.9. Ce reprezintă elementele omise din jurnalul de scanare? 198

34.10. Ce reprezintă fișierele supracomprimate din jurnalul de scanare? 198
34.11. De ce BitDefender a șters în mod automat un fișier infectat? 198
35. Suport 199
35.1. Resurse online 199
35.1.1. BitDefender Knowledge Base 199
35.1.2. Forumul de suport al BitDefender 199
35.1.3. Portalul Malware City 200
35.1.4. Tutoriale video 200
35.2. Solicitarea ajutorului 201
36. Informații de contact 203
36.1. Adrese Web 203
36.2. Distribuitori locali 203
36.3. Filialele BitDefender 204
37. Informații utile 206
37.1. Cum dezinstalez alte soluții de securitate? 206
37.2. Cum pot reporni sistemul în Safe Mode? 207
37.3. Utilizez o versiune Windows pe 32 biți sau pe 64 biți? 207
37.4. Cum aflu care sunt setările mele proxy? 208
37.5. Cum dezinstalez complet BitDefender? 208
37.6. Cum activez/dezactivez protecția în timp real? 208
37.7. Cum pot afișa elementele ascunse din Windows? 209
Vocabular 210

Instalare și dezinstalare

1. Cerințe de sistem

Puteți instala BitDefender Internet Security 2011 doar pe calculatoare pe care rulează următoarele sisteme de operare:

- Windows XP cu Service Pack 3 (32 biți) / Windows XP cu Service Pack 2 (64 biți)
- Windows Vista cu Service Pack 1 sau o versiune superioară (32/64 bit)
- Windows 7 (32/64 biți)

Înainte de instalare, asigurați-vă că sistemul dumneavoastră îndeplinește cerințele hardware și software minime.

Notă

Pentru a afla sistemul de operare Windows care rulează pe calculatorul dumneavoastră, precum și informații hardware, faceți clic-dreapta pe iconița **My Computer** de pe desktop și apoi selectați **Properties** din meniu.

1.1. Cerințe de sistem minime

- 1 GB de spațiu liber disponibil pe hard-disc
- Procesor de 800 MHz
- Memorie RAM:
  - 512 MB pentru Windows XP
  - 1 GB pentru Windows Vista și Windows 7
- Internet Explorer 6.0
- .NET Framework 2 (disponibil de asemenea în kitul de instalare)
- Adobe Flash Player 10.0.45.2

1.2. Cerințe de sistem recomandate

- 1 GB de spațiu liber disponibil pe hard-disc
- Intel Core Duo (1.66 GHz) sau procesor echivalent
- Memorie RAM:
  - 1 GB pentru Windows XP și Windows 7
  - 1,5 GB pentru Windows Vista
- Internet Explorer 7
- .NET Framework 2 (disponibil de asemenea în kitul de instalare)
- Adobe Flash Player 10.0.45.2

1.3. Cerințe software

Protecția antiphishing este oferită doar pentru:

- Internet Explorer 6.0 sau mai recent
- Mozilla Firefox 3.x
- Yahoo! Messenger 8.1
- Microsoft Windows Live Messenger 8

Criptarea mesageriei instant (IM) este oferită doar pentru:

- Yahoo! Messenger 8.1
- Microsoft Windows Live Messenger 8

Protecția antispam este oferită pentru toți clienții de mail POP3/SMTP.Bara de comenzi antispam însă este integrată doar în:

- Microsoft Outlook 2003 / 2007 / 2010
- Microsoft Outlook Express
- Microsoft Windows Mail
- Mozilla Thunderbird 3.0.4

2. Pregătirea pentru instalare

Pentru a instala BitDefender Internet Security 2011 fără probleme, parcurgeți acești pași prealabili:

- Asigurați-vă că sistemul pe care doriți să instalați BitDefender întrunește cerințele minime.În cazul în care calculatorul nu întrunește toate cerințele minime de sistem, BitDefender nu va fi instalat sau nu va funcționa în mod corespunzător, determinând reducerea vitezei de funcționare și instabilitatea sistemului.Pentru o listă completă a cerințelor de sistem, consultați *„Cerințe de sistem”* (p. 2).
- Autentificați-vă pe calculator cu datele unui cont de administrator.
- Dezinstalați orice alt program de securitate de pe calculator.Rularea simultană a două programe de securitate poate afecta funcționarea lor și poate provoca probleme majore ale sistemului.Windows Defender va fi dezactivat implicit, înainte de inițierea instalării.
- Dezactivați sau dezinstalați orice alt program firewall de pe calculator.Rularea simultană a două programe firewall poate afecta funcționarea lor și poate provoca probleme majore ale sistemului.Windows Firewall va fi dezactivat implicit, înainte de inițierea instalării.

3. Instalarea BitDefender

Puteți instala BitDefender de pe CD-ul de instalare BitDefender sau folosind fișierul de instalare descărcat pe calculatorul dumneavoastră de pe site-ul BitDefender sau de pe alte site-uri autorizate (de exemplu, site-ul unui partener BitDefender sau un magazin online).Puteți descărca fișierul de instalare de pe site-ul BitDefender: http://www.bitdefender.com/site/Downloads/.

- Pentru a instala BitDefender de pe CD, introduceți CD-ul în unitate. În câteva momente se va afișa un ecran de întâmpinare. Urmați instrucțiunile pentru a începe instalarea.

  Notă

  Ecranul de bun venit oferă o opțiune pentru copierea pachetului de instalare de pe CD-ul de instalare pe un dispozitiv de stocare USB. Acest lucru este util atunci când doriți să instalați BitDefender pe un computer care nu are o unitate CD (de exemplu, pe un netbook).Introduceți dispozitivul de stocare în unitatea USB și apoi faceți clic pe **Copiere pe USB**.Apoi, mergeți la calculatorul fără unitate de CD, introduceți dispozitivul de stocare în USB și faceți dublu-clic pe `runsetup.exe` din directorul în care ați salvat pachetul de instalare.

  În cazul în care nu apare ecranul de întâmpinare, accesați directorul rădăcină al CD-ului și faceți dublu-clic pe `autorun.exe`.

- Pentru a instala BitDefender folosind fișierul de instalare descărcat pe calculator, localizați fișierul și faceți dublu-clic pe el.

Programul de instalare va verifica mai întâi sistemul dvs, pentru a valida instalarea.În cazul în care instalarea este validată, veți fi rugat să selectați limba înainte de apariția asistentului de configurare.

Asistentul vă va ajuta să instalați BitDefender pe calculator și în același timp vă va permite să configurați setările principale și interfața.

3.1. Pasul 1 - Introducere

Vă rugăm să citiți Acordul de licență și să selectați **Bifând această căsuță, sunt de acord cu acordul de licență BitDefender**.Faceți clic pe **Înainte** pentru a continua.

Dacă nu sunteți de acord cu prevederile acestui contract faceți clic pe **Anulare**. Procesul de instalare va fi abandonat și veți părăsi programul asistent.

3.2. Pasul 2 - Pregătirea instalării

BitDefender vă scanează sistemul și verifică dacă nu este instalat un alt software de securitate pe acesta.

Quick Scan

O scanare rapidă a zonelor critice din sistemul dumneavoastră este realizată pentru asigurarea faptului că niciun program malware nu se află în cadrul acestuia.

Scanarea nu va dura mai mult de câteva minute. Puteți anula oricând operațiunea prin utilizarea butonului aferent.

Important
Se recomandă să permiteți finalizarea scanării.
Programele malware active pot interveni în cadrul procesului de instalare și pot duce chiar la neefectuarea acestuia.

După finalizarea scanării, sunt afișate rezultatele. Dacă sunt identificate orice fel de amenințări, urmați instrucțiunile de îndepărtare a acestora înainte de a continua cu instalarea.

Faceți clic pe **Înainte** pentru a continua.

Dezinstalarea programelor de securitate existente

BitDefender Internet Security 2011 vă alertează dacă aveți alte produse de securitate instalate pe calculatorul dumneavoastră.Faceți clic pe butonul corespunzător pentru a începe procesul de dezinstalare și urmați instrucțiunile de eliminare a oricăror produse identificate.

Avertisment
Este recomandat să dezinstalați produsele antivirus detectate înainte de a instala BitDefender. Rularea a două sau mai multor produse antivirus în același timp, pe același calculator, provoacă în general instabilitatea sistemului de operare.

BitDefender recomandă de asemenea acțiuni ce trebuie efectuate în cazul funcțiilor de securitate Windows activate.

- **Dezactivează Firewallul Windows** - pentru a dezactiva aplicația Windows Firewall.

  Important
  Vă recomandăm să dezactivați Windows Firewall deoarece BitDefender Internet Security 2011 include un firewall avansat. Rularea simultană a două aplicații firewall pe un calculator poate provoca probleme.

- **Dezactivare Windows Defender** - pentru a dezactiva aplicația Windows Defender.

Faceți clic pe **Înainte** pentru a continua.

3.3. Pasul 3 - Înregistrare

Procesul de înregistrare a BitDefender constă în înregistrarea produsului cu cheia de licență și activarea funcțiilor online prin crearea unui cont BitDefender.

Înregistrați-vă produsul

Procedați în funcție de situația dumneavoastră:

- **Am achiziționat BitDefender Internet Security 2011 pe un CD sau online**

  În acest caz, trebuie să înregistrați produsul:

  1. Introduceți seria de înregistrare în câmpul editabil.

     Notă
     Puteți găsi seria dumneavoastră de înregistrare:
     - pe eticheta de pe CD.
     - pe certificatul de înregistrare al produsului.
     - în e-mailul de achiziționare online.

     Dacă nu aveți o serie de înregistrare BitDefender, faceți clic pe linkul furnizat pentru a merge la magazinul online BitDefender și a cumpăra una.

  2. Faceți clic pe **Înregistrare**.
  3. Faceți clic pe **Înainte**.

- **Am descărcat BitDefender Internet Security 2011 pentru evaluare**

  În acest caz, puteți utiliza toate opțiunile produsului pe o perioadă de 30 de zile.Pentru a începe perioada de încercare, selectați **Doresc să evaluez BitDefender Internet Security 2011 timp de 30 zile** și faceți clic pe **Înainte**.

Activarea funcțiilor online

ESTE NECESAR să vă creați un cont BitDefender pentru a primi actualizări BitDefender.Contul BitDefender vă oferă de asemenea acces la control parental online, suport tehnic gratuit, oferte speciale și promoții.Daca v-ați pierdut cheia de înregistrare BitDefender, puteți accesa contul dumneavoastră la http://myaccount.bitdefender.com pentru a o recupera.

Dacă nu doriți să creați un cont BitDefender în acest moment, selectați **Creează un cont mai târziu** și faceți clic pe **Înainte**.

Notă
Dacă instalați versiunea BitDefender Internet Security 2011 pentru evaluare, trebuie să creați un cont BitDefender în acest moment.
Dacă ați achiziționat produsul, trebuie să creați un cont în termen de 30 de zile de la instalare.

Altfel, continuați în funcție de situația dumneavoastră actuală:

- **Nu am cont BitDefender**

  Pentru a crea un cont BitDefender, urmați acești pași:

  1. Selectați **Creează un cont nou**.
  2. Introduceți informațiile solicitate în câmpurile corespunzătoare.Informațiile furnizate aici vor rămâne confidențiale.
     - **Nume de utilizator** - introduceți adresa dumneavoastră de e-mail.
     - **Parolă** - introduceți o parolă pentru contul dumneavoastră BitDefender.Parola trebuie să conțină între 6 și 16 caractere.
     - **Confirmați parola** - introduceți din nou parola specificată anterior.

       Nu trebuie să reintroduceți parola dacă ați ales ca aceasta să nu fie mascată în timpul tastării.

     Notă
     După activarea contului, puteți folosi adresa de e-mail și parola furnizate pentru a-l accesa, la adresa http://myaccount.bitdefender.com.

  3. Opțional, BitDefender vă poate informa despre oferte speciale și promoții folosind adresa de e-mail a contului dumneavoastră.Faceți clic pe **Vizualizare opțiuni contacte** și selectați una dintre opțiunile disponibile din fereastra care apare.
     - **Vreau sa primesc toate mesajele**
     - **Trimite-mi mesajele importante**
     - **Nu vreau sa primesc niciun mesaj**
  4. Faceți clic pe **Trimite**.
  5. Faceți clic pe **Înainte** pentru a continua.

     Notă
     Pentru a vă putea utiliza contul, trebuie mai întâi să îl activați.
     Verificați-vă adresa de e-mail și urmați instrucțiunile din mesajul trimis de către serviciul de înregistrare BitDefender.

- **Deja am un cont BitDefender**

  BitDefender va detecta automat dacă ați creat anterior un cont BitDefender pe calculatorul dumneavoastră.În acest caz, furnizați parola contului dumneavoastră și faceți clic pe **Trimite**.Faceți clic pe **Înainte** pentru a continua.

  Dacă aveți deja un cont activ, dar BitDefender nu-l detectează, urmați pașii de mai jos pentru a înregistra produsul cu contul respectiv:

  1. Selectați **Autentificare(cont anterior)**.

2. Introduceți adresa de e-mail și parola contului dvs în câmpurile corespunzătoare.

Notă
Dacă v-ați uitat parola, faceți clic pe **V-ați uitat parola?** și urmați instrucțiunile.

3. Opțional, BitDefender vă poate informa despre oferte speciale și promoții folosind adresa de e-mail a contului dumneavoastră.Faceți clic pe **Vizualizare opțiuni contacte** și selectați una dintre opțiunile disponibile din fereastra care apare.
   - **Vreau sa primesc toate mesajele**
   - **Trimite-mi mesajele importante**
   - **Nu vreau sa primesc niciun mesaj**
4. Faceți clic pe **Trimite**.
5. Faceți clic pe **Înainte** pentru a continua.

3.4. Pasul 4 - Selectarea modului de vizualizare

Aici puteți alege tipul de instalare care va fi efectuat și modul de vizualizare a interfeței ce va fi utilizat.

Alegeți tipul de configurare

Sunt disponibile următoarele opțiuni de configurare:

- **Configurare ușoară** - selectați această opțiune dacă preferați o instalare rapidă și nu intenționați să configurați setările BitDefender în detaliu.
- **Configurare personalizată** - selectați această opțiune dacă preferați să personalizați setările de instalare și ale BitDefender.

Pentru a vizualiza un tutorial video care vă va ajuta să efectuați instalarea, faceți clic pe **Ajutor**

Notă
Pentru instalarea BitDefender într-o configurare implicită și pentru a ajunge direct la ultimul pas din programul asistent de instalare, selectați **Omite configurarea**.

Faceți clic pe **Înainte** pentru a continua.

Alegeți locația pentru instalare

Notă
Acest pas apare numai dacă ați ales o **Configurare personalizată**.

În mod implicit, BitDefender Internet Security 2011 va fi instalat în `C:\Program Files\BitDefender\`.Dacă doriți să schimbați calea de instalare, faceți clic pe butonul **Caută** și selectați directorul în care doriți să fie instalat BitDefender.

Puteți partaja fișierele produsului și semnăturile cu alți utilizatori BitDefender.În acest mod, actualizările BitDefender pot fi realizate mai rapid.Dacă nu doriți să activați această funcție, bifați căsuța corespunzătoare.

Notă

Nicio informație personală identificabilă nu va fi partajată dacă această funcție este activată.

Faceți clic pe **Înainte** pentru a continua.

Alegeți interfața

Selectați modul de vizualizare a interfeței utilizatorului care se potrivește cel mai bine nevoilor dumneavoastră.BitDefender Internet Security 2011 vă pune la dispoziție trei interfețe la alegere, fiecare creată pentru a se potrivi dorințelor diferitelor tipuri de utilizatori.

Modul Novice

Potrivit pentru utilizatorii începători și pentru cei care doresc ca BitDefender să le protejeze calculatorul și datele fără a fi nevoiți să intervină. Interfața este foarte ușor de utilizat, iar interacțiunea dumneavoastră cu aceasta este minimă.

Tot ce trebuie să faceți este să remediați problemele existente, atunci când sunt semnalate de BitDefender. Un program asistent intuitiv vă ghidează, pas cu pas, în acest proces.În plus, puteți efectua sarcini obișnuite, cum ar fi actualizarea semnăturilor de viruși și a fișierelor de produs BitDefender sau scanarea calculatorului.

Modul Intermediar

Puteți configura principalele setări ale BitDefender, remedia problemele în mod separat, administra produsele BitDefender instalate pe produsele din căminul dumneavoastră și alege care aspecte necesită monitorizare.În plus, puteți controla modul în care copiii dumneavoastră utilizează calculatorul și internetul prin configurarea Controlului parental.

Modul Expert

Adecvat utilizatorilor mai experimentați, acest mod vă permite să configurați complet fiecare funcționalitate a BitDefender.De asemenea, puteți folosi toate sarcinile disponibile pentru a vă proteja calculatorul și datele.

Faceți selecția și faceți clic pe **Înainte** pentru a continua.

3.5. Pasul 5 - Configurare

Aici vă puteți personaliza produsul.

Configurarea setărilor

Notă
Acest pas apare numai dacă ați setat interfața BitDefender în **Modul expert**.

Aici puteți activa / dezactiva caracteristicile BitDefender organizate în două categorii.Pentru a modifica starea unei setări, faceți clic pe selectorul corespunzător.

- **Setări de securitate**

  În această zonă, puteți activa sau dezactiva setările de produs care acoperă diverse aspecte ale securității calculatorului și a datelor.

Setare	Descriere
Antivirus	Protecția în timp real asigură scanarea tuturor fișierelor accesate de dvs sau de o aplicație care rulează pe acest sistem.
Actualizarea Automată	Actualizarea automată asigură descărcarea și instalarea automată, în mod regulat, a celor mai recente fișiere de produs și semnături BitDefender.
Căutare vulnerabilități	Verificarea automată a vulnerabilităților asigură menținerea la zi a aplicațiilor critice de pe calculatorul dumneavoastră.
Antispam	Protecția Antispam filtrează mesajele e-mail pe care le primiți, marcându-le pe cele nedorite ca SPAM.
Antiphishing	Protecția antiphishing detectează și vă alertează în timp real dacă o pagină web este folosită pentru furt de informații personale.
Control identitate	Controlul identității vă permite să împiedicați trimiterea de date cu caracter personal pe Internet, fără consimțământul dumneavoastră. Această opțiune blochează orice mesaj instant, e-mail sau formular web prin care se transmit către destinatari neautorizați (adrese) date pe care le-ați identificat ca având caracter personal.
Criptare chat	Criptarea chatului asigură confidențialitatea conversațiilor dumneavoastră prin Yahoo! Messenger și Windows Live Messenger cu interlocutori care folosesc un produs BitDefender și o aplicație de mesagerie instant compatibile.

Setare	Descriere
Control parental	Controlul parental restricționează activitățile desfășurate pe calculator și online de către copii, pe baza regulilor definite de dumneavoastră. Restricțiile pot include blocarea accesului la site-uri web cu conținut inadecvat precum și limitarea accesului la jocuri și la Internet, conform programului indicat.
Firewall	Firewallul vă protejează calculatorul de atacurile din exterior ale hackerilor și aplicațiilor periculoase.

- **Setări generale**

  În această zonă, puteți activa sau dezactiva setările care afectează comportamentul produsului și interacțiunea cu utilizatorul.

Setare	Descriere
Modul pentru jocuri	Modul pentru jocuri modifică temporar setările de protecție pentru a minimiza impactul acestora asupra performanței sistemului atunci când vă jucați pe calculator.
Detecție Mod laptop	Modul pentru laptop modifică temporar setările de protecție pentru a minimiza impactul acestora asupra duratei de funcționare a laptopului pe baterie.
Parolă setări	Aceasta asigură că setările BitDefender pot fi modificate doar de către persoanele care cunosc această parolă. La activarea acestei opțiuni, vi se va solicita să configurați parola pentru setări. Introduceți parola dorită în ambele câmpuri și faceți clic pe **OK** pentru a o seta.
Știri BitDefender	Activând această opțiune, veți primi știri importante legate de companie, actualizări de produs sau noi amenințări de securitate de la BitDefender.
Alerte notificare produs	Activând această opțiune, veți primi alerte informative.
Bara de scanare	Bara de scanare este o fereastră mică, transparentă care indică progresul activității de scanare a BitDefender.Pentru mai multe informații, consultați *„Bara de scanare”* (p. 21).

Setare	Descriere
Trimite rapoarte virușI	Activând această opțiune, BitDefender va trimite rapoartele de scanare către Laboratorul BitDefender pentru analiză. Aceste rapoarte nu vor conține date confidențiale, cum ar fi numele dumneavoastră sau adresa IP și nu vor fi folosite în scop comercial.
Detecție epidemii virale	Activând această opțiune, BitDefender va trimite rapoarte privind potențiale epidemii virale către Laboratorul BitDefender pentru analiză. Aceste rapoarte nu vor conține date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, și nu vor fi folosite în scop comercial.

Faceți clic pe **Înainte** pentru a continua.

Configurarea Instrumentelor mele

Notă
Acest pas apare numai dacă ați setat interfața BitDefender în **Modul Novice** sau în **Modul Intermediar**.

Cu ajutorul opțiunii **Instrumentele mele**, puteți personaliza panoul prin adăugarea de comenzi rapide pentru acele instrumente care au cea mai mare importanță pentru dumneavoastră.În acest mod puteți asigura un acces facil la acestea.

Din acest ecran, puteți adăuga comenzi rapide pentru oricare dintre următoarele instrumente:

- Control parental - controlați și monitorizați activitățile de pe calculator ale copilului dumneavoastră.
- Mod jocuri - configurați BitDefender pentru a nu interfera cu jocurile rulate în sistemul dumneavoastră.
- Mod laptop - modifică temporar setările de protecție pentru a reduce impactul acestora asupra duratei de funcționare a acumulatorului laptopului.
- Administrare rețea personală - gestionați produsele BitDefender instalate pe calculatoare din rețeaua personală de pe un singur PC.

Selectați instrumentele pe care doriți să le adăugați și faceți clic pe **Înainte** pentru a continua.

Configurarea Controlului parental

Notă
Acest pas apare numai dacă ați adăugat funcția Control parental în Instrumentele mele.

Puteți selecta una dintre cele trei opțiuni:

- **Setați Controlul parental pentru conturile copiilor**

  Selectați această opțiune pentru a activa funcția de Control parental pentru conturile Windows create pentru copiii dumneavoastră și pentru a o gestiona din contul de administrator.

- **Setați Controlul parental pentru contul actual**

  Selectați această opțiune pentru a activa funcția de Control parental pentru contul Windows curent. Aceasta înseamnă că nu trebuie să creați conturi separate pentru copiii dumneavoastră, însă regulile privind Controlul parental vor afecta orice persoană care utilizează acest cont.

  În acest caz, este necesară o parolă pentru a proteja setările de Control parental.O puteți seta acum sau ulterior din fereastra BitDefender.

- **Omite deocamdată configurarea**

  Selectați această opțiune pentru a configura această caracteristică ulterior din fereastra BitDefender.

Faceți clic pe **Înainte** pentru a continua.

Administrare rețea personală

Notă
Acest pas apare numai dacă ați adăugat funcția Administrare rețea personală în Instrumentele mele.

Puteți selecta una dintre cele trei opțiuni:

- **Configurați acest calculator ca server**

  Selectați această opțiune dacă intenționați să gestionați produsele BitDefender instalate pe alte calculatoare din rețeaua personală de la acest calculator.

  Pentru a putea accesa rețeaua, este necesară o parolă.Introduceți parola în căsuțele de text puse la dispoziție și faceți clic pe **Trimite**.

- **Configurați acest calculator drept client**

  Selectați această opțiune dacă BitDefender va fi administrat de la un alt calculator din cadrul rețelei personale pe care rulează de asemenea BitDefender.

Pentru a putea accesa rețeaua, este necesară o parolă.Introduceți parola în căsuțele de text puse la dispoziție și faceți clic pe **Trimite**.

- **Omite deocamdată configurarea**

  Selectați această opțiune pentru a configura această caracteristică ulterior din fereastra BitDefender.

Faceți clic pe **Înainte** pentru a continua.

3.6. Pasul 6 - Opțiuni de asistență

Aici puteți personaliza opțiunile de asistență:

- Activați / dezactivați **Sfaturile inteligente**.Sfaturile utile sunt mesaje personalizate afișate în Tabloul de comandă BitDefender pentru a vă ajuta să vă îmbunătățiți performanțele calculatorului.
- Confirmați adresa de e-mail pe care o veți utiliza în cazul în care trebuie să contactați Serviciul clienți al BitDefender. Dacă nu intenționați să contactați Serviciul clienți prin e-mail, bifați căsuța corespunzătoare.

3.7. Pasul 7 - Confirmare

Aici puteți revedea configurația selectată.

În mod implicit, sunt programate de asemenea două sarcini:

- O scanare completă a sistemului este programată imediat după finalizarea procesului de instalare.

  Este recomandat să realizați această scanare completă care va detecta dacă există amenințări malware în sistemul dumneavoastră.

- O scanare a sistemului este programată în fiecare duminică la ora 2:00.

  Se recomandă să scanați sistemul cel puțin o dată pe săptămână.Selectați o dată și o oră diferită în cazul în care programul implicit nu este convenabil pentru dumneavoastră.Dacă aveți calculatorul închis atunci când sarcina trebuie să ruleze, aceasta va fi executată imediat ce deschideți calculatorul.

Faceți clic pe **Finalizare**.

3.8. Pasul 8 - Finalizare

Instalarea se apropie de final. Setările finale sunt aplicate și este realizată o actualizare.

Asistentul se va închide automat atunci când procedura de instalare s-a finalizat.Dacă această opțiune a fost selectată în timpul pasului anterior, este inițiată o scanare completă a sistemului.

Asistentul de configurare va detecta rețeaua la care sunteți conectat și vă va permite să o clasificați ca rețea personală/de birou sau publică.

Notă
Poate fi necesară o repornire a sistemului.

4. Actualizarea unei versiuni anterioare a BitDefender

Dacă folosiți deja BitDefender Internet Security 2011 beta sau una dintre versiunile 2008, 2009 sau 2010, o puteți actualiza la versiunea superioară BitDefender Internet Security 2011.

Există două moduri de trecere la o versiune superioară de produs:

- Instalați BitDefender Internet Security 2011 direct peste versiunea mai veche.Dacă instalați direct peste versiunea 2010, listele de prieteni și de spammeri, precum și Carantina vor fi importate în mod automat.
- Dezinstalați vechea versiune, apoi reporniți calculatorul și instalați noua versiune, conform instrucțiunilor de la capitolul „*Instalarea BitDefender*” (p. 5).Nicio setare de produs nu va fi salvată.Folosiți această metodă de trecere la o versiune superioară de produs dacă cealaltă nu funcționează.

5. Repararea sau dezinstalarea BitDefender

Dacă doriți să reparați sau să dezinstalați BitDefender Internet Security 2011, urmați calea din meniul Start al Windows: **Start → Toate programele → BitDefender 2011 → Reparare sau dezinstalare**.

Va fi afișat un program asistent care vă va ajuta să finalizați sarcina dorită.

1. **Reparare sau eliminare**

   Selectați acțiunea pe care doriți s-o efectuați:

   - **Reparare** - pentru a reinstala toate componentele programului.
   - **Dezinstalare** - pentru dezinstalarea tuturor componentelor instalate.

   Notă
   Vă recomandăm să alegeți **Dezinstalare** pentru a asigura o reinstalare corectă.

2. **Confirmarea acțiunii**

   Citiți cu grijă informațiile afișate înainte de a face clic pe **Înainte** pentru confirmarea acțiunii.

3. **Progres**

   Așteptați ca BitDefender să finalizeze acțiunea pe care ați selectat-o.Aceasta va dura câteva minute.

4. **Finalizare**

   Sunt afișate rezultatele.

   Trebuie să reporniți calculatorul pentru a finaliza procesul. Faceți clic pe **Repornire** pentru a reporni calculatorul imediat sau pe **Finalizare** pentru a închide fereastra și reporni ulterior.

Introducere

6. Descriere generală

Odată ce ați instalat BitDefender Internet Security 2011, calculatorul dumneavoastră este protejat împotriva tuturor tipurilor de programe periculoase (cum ar fi virușii, programele spion și troienii) și amenințărilor de pe internet (cum ar fi pirații informatici, atacurile de tip phishing și mesajele spam).

Nu trebuie să configurați alte setări ale BitDefender pe lângă cele configurate în timpul instalării.Cu toate acestea, puteți profita de setările oferite de BitDefender pentru a vă ajusta și îmbunătăți protecția.

Din când în când, trebuie să deschideți BitDefender și să remediați problemele existente.Este posibil să fie nevoie să configurați anumite componente ale BitDefender sau să luați măsuri preventive pentru a vă proteja calculatorul și datele dumneavoastră.Dacă doriți, puteți configura BitDefender să nu vă avertizeze în legătură cu anumite probleme.

Dacă nu ați înregistrat produsul (inclusiv prin crearea unui cont BitDefender), amintiți-vă să faceți acest lucru până la încheierea perioadei de evaluare.Este necesar să vă creați un cont în termen de 15 zile de la instalarea BitDefender (dacă înregistrați produsul cu o serie de înregistrare, termenul limită se extinde la 30 de zile).În caz contrar, BitDefender nu se va mai actualiza.Pentru mai multe informații despre procesul de înregistrare, consultați secțiunea *„Înregistrare și Contul meu”* (p. 52).

6.1. Deschiderea BitDefender

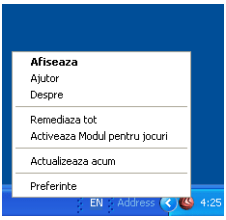
Pentru a accesa fereastra principală a BitDefender Internet Security 2011, folosiți meniul Start al Windows, urmând calea **Start → Toate programele → BitDefender 2011 → BitDefender Internet Security 2011** sau, mai rapid, faceți dublu-clic pe iconița BitDefender din bara de sistem.

Pentru mai multe informații cu privire la fereastra principală, consultați *„Fereastra principală a aplicației”* (p. 25).

6.2. Iconița din bara de sistem

Pentru a administra întregul produs mai rapid, puteți folosi iconița BitDefender din bara de sistem.Dacă faceți dublu-clic pe această iconiță, se va deschide fereastra BitDefender. De asemenea, făcând clic-dreapta pe iconiță, un meniu contextual vă va oferi posibilitatea unei administrări rapide a BitDefender.

- **Afișează** - deschide interfața principală a BitDefender.
- **Ajutor** - deschide documentația electronică, unde vi se explică în detaliu cum să configurați și să utilizați produsul BitDefender Internet Security 2011.
- **Despre** - deschide o fereastră în care puteți vedea informații despre BitDefender și unde puteți solicita asistență profesională în cazul unei probleme.
- **Remediază** - vă ajută să remediați problemele curente de securitate.Dacă opțiunea nu este disponibilă, nu există probleme care trebuie remediate.Pentru mai multe detalii, consultați *„Remedierea problemelor”* (p. 42).



Iconiță în bară

- **Activează/Dezactivează Modul pentru jocuri** - activează/dezactivează modul pentru jocuri.
- **Actualizează acum** - inițiază o actualizare imediată.Va apărea o nouă fereastră în care puteți vedea starea actualizării.
- **Preferințe** - deschide o fereastră în care puteți activa sau dezactiva setările principale ale produsului și reconfigura profilul de utilizare.Pentru mai multe informații, consultați *„Configurarea setărilor principale”* (p. 45).

Iconița BitDefender din bara de sistem vă informează despre problemele care vă afectează calculatorul sau despre funcționarea produsului, prin afișarea unui simbol special, după cum urmează:

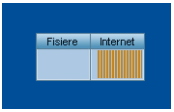
Triunghi roșu cu semnul exclamării: Probleme grave de securitate afectează calculatorul dumneavoastră. Acestea necesită atenția dumneavoastră imediat și trebuie remediate în cel mai scurt timp.
Litera G: Produsul funcționează în Modul pentru jocuri.

Dacă BitDefender nu funcționează, iconița din bara de sistem apare în gri .Acest lucru se întâmplă de obicei când expiră licența. O altă cauză poate fi faptul că serviciile BitDefender nu răspund sau că alte erori afectează funcționarea normală a produsului.

6.3. Bara de scanare

Bara de scanare este o reprezentare grafică a activității de scanare din sistemul dumneavoastră.Această fereastră mică este disponibilă, implicit, numai în Modul Expert.

Barele gri (zona **Fișiere**) reprezintă numărul de fișiere scanate pe secundă, pe o scară de la 0 la 50.Barele portocalii din zona **Internet** reprezintă numărul de kiloocteți transferați (trimiși și primiți de pe Internet) pe secundă, pe o scară de la 0 la 100.



Bara de scanare

Notă
Bara de scanare vă va avertiza când protecția în timp real sau protecția firewall este dezactivată prin afișarea unui X roșu deasupra zonei corespunzătoare (**Fișiere** sau **Internet**).

6.3.1. Scanare fișiere și directoare

Puteți utiliza bara de scanare pentru a scana rapid fișiere și directoare.Trageți fișierul sau directorul care doriți să fie scanat peste **Bara de scanare**, ca în imaginile de mai jos.

Trageți fișierul

Lăsați fișierul

Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

Opțiuni de scanare. Opțiunile de scanare sunt pre-configurate pentru a obține rata maximă de detecție.Dacă sunt detectate fișiere infectate, BitDefender va încerca să le dezinfecteze (va elimina codul malițios). Dacă dezinfectarea eșuează, programul asistent de scanare vă va permite să specificați alte acțiuni ce vor fi luate asupra fișierelor infectate.Opțiunile de scanare sunt standard și nu le puteți modifica.

6.3.2. Dezactivarea/Reactivarea barei de scanare

Când nu mai doriți să vedeți bara de scanare, faceți clic-dreapta pe ea și selectați **Închide**.Pentru a reactiva bara de scanare, urmați acești pași:

1. Deschideți BitDefender.

2. Faceți clic pe butonul **Opțiuni** din colțul dreapta sus al ferestrei și selectați **Preferințe**.
3. În categoria Setări generale, utilizați selectorul corespunzător opțiunii **Bara de scanare** pentru a o activa.
4. Faceți clic pe **OK** pentru a salva și aplica modificările.

6.4. Detecție automată unități

BitDefender detectează automat unitățile mobile de stocare pe care le conectați la calculator și propune scanarea lor înainte să accesați fișierele pe care le conțin acestea.Acest lucru este recomandat pentru a preveni pătrunderea virușilor și a altor aplicații periculoase pe calculatorul dumneavoastră.

Unitățile detectate fac parte din următoarele categorii:

- CD/DVD
- unități de stocare pe USB, cum ar fi memoriile flash sau hard discurile externe
- unități de rețea mapate (la distanță)

La detectarea unei astfel de unități se afișează o fereastră de alertă.

Pentru a scana unitatea de stocare, faceți clic pe **Da**.Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

Dacă nu doriți să scanați unitatea, faceți clic pe **Nu**. În acest caz, v-ar putea fi de folos una dintre aceste opțiuni:

- **Nu mă mai întreba despre acest tip de unitate** - BitDefender nu va mai propune scanarea unităților de stocare de acest tip atunci când acestea sunt conectate la calculator.
- **Dezactivează detecția automată a unităților** - Nu vi se va mai propune să scanați noile unități de stocare atunci când acestea sunt conectate la calculator.

Dacă ați dezactivat detecția automată a unităților în mod accidental și vreți s-o reactivați sau să-i configurați setările, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus>Scanare viruși**.
3. În lista de sarcini de scanare, localizați sarcina **Scanare dispozitive**.
4. Faceți clic pe sarcină și selectați **Proprietăți**.Va apărea o nouă fereastră.
5. Pe tabul **Generalități**, configurați opțiunile de scanare după cum este necesar.Pentru mai multe informații, consultați *„Configurarea setărilor de scanare”* (p. 76).
6. Pe tabul **Detecție**, alegeți tipurile de unități de stocare care să fie detectate.

7. Faceți clic pe **OK** pentru a salva și aplica modificările.

7. Fereastra principală a aplicației

BitDefender Internet Security 2011 îndeplinește deopotrivă cerințele persoanelor experimentate și pe cele ale începătorilor în utilizarea calculatorului. Interfața sa grafică este proiectată pentru a se potrivi fiecărei categorii de utilizatori.

Puteți opta pentru vizualizarea interfeței în oricare dintre cele trei moduri, în funcție de cunoștințele dumneavoastră de operare a calculatorului și de gradul de familiarizare cu BitDefender.

Modul Novice

Potrivit pentru utilizatorii începători și pentru cei care doresc ca BitDefender să le protejeze calculatorul și datele fără a fi solicitați să intervină. În acest mod, produsul este foarte ușor de utilizat, iar interacțiunea dumneavoastră cu el este minimă.

Tot ce trebuie să faceți este să remediați problemele existente, atunci când sunt semnalate de BitDefender. Un program asistent intuitiv vă ghidează, pas cu pas, în acest proces.În plus, puteți efectua sarcini obișnuite, cum ar fi actualizarea semnăturilor de viruși și a fișierelor de produs BitDefender sau scanarea calculatorului.

Modul Intermediar

Destinată utilizatorilor cu abilități medii de folosire a calculatorului, această interfață extinde capacitățile de acțiune oferite în Modul Novice.

Puteți remedia problemele separat și puteți alege care dintre acestea să fie monitorizate.În plus, puteți administra la distanță produsele BitDefender instalate pe calculatoarele din rețeaua personală.

Modul Expert

Adecvat utilizatorilor mai experimentați, acest mod vă permite să configurați complet fiecare funcționalitate a BitDefender.De asemenea, puteți folosi toate sarcinile disponibile pentru a vă proteja calculatorul și datele.

Modul de vizualizare este selectat în timpul instalării.

Pentru a schimba modul de vizualizare:

1. Deschideți BitDefender.
2. Faceți clic pe butonul **Opțiuni** din colțul din dreapta sus al ferestrei.
3. Selectați modul de vizualizare dorit din meniu.

7.1. Modul Novice

Dacă sunteți începător în operarea calculatorului, afișarea interfeței în Modul Novice ar putea fi cea mai bună alegere pentru dumneavoastră.În acest mod, produsul este simplu de folosit, iar interacțiunea cu utilizatorul este minimă.

Fereastra conține trei secțiuni principale:

Zona de stare
: Informațiile de stare sunt prezentate în partea stângă a ferestrei.

Zona Protejați-vă calculatorul!
: Aici puteți efectua acțiunile necesare pentru gestionarea protecției dumneavoastră.

Zona de ajutor
: Aici puteți afla cum să utilizați BitDefender Internet Security 2011 și cum să obțineți asistență.

Butonul **Opțiuni** din colțul dreapta sus al ferestrei vă permite să schimbați modul de vizualizare a interfeței și să configurați principalele setări ale programului.

În colțul din dreapta jos al ferestrei, puteți găsi mai multe linkuri utile.

Link	Descriere
Informații licență	Deschide o fereastră în care puteți vedea informații despre licența actuală și unde vă puteți înregistra produsul cu o nouă serie de înregistrare.
Jurnale	Vă permite să vedeți un istoric detaliat al tuturor sarcinilor efectuate de BitDefender pe sistemul dumneavoastră.
Asistență	Faceți clic pe acest link dacă aveți nevoie de ajutor cu BitDefender.
?	Deschide un fișier de ajutor care vă ajută să utilizați BitDefender.

7.1.1. Zona de stare

Informațiile de stare sunt prezentate în partea stângă a ferestrei.

- **Starea securității** vă informează dacă sunt probleme care afectează securitatea calculatorului dumneavoastră și vă ajută să le rezolvați.Dacă faceți clic pe **Remediază**, un program asistent vă va permite să eliminați cu ușurință orice pericol la adresa calculatorului și a datelor dumneavoastră.Pentru mai multe detalii, consultați *„Remedierea problemelor”* (p. 42).
- **Starea licenței** afișează câte zile mai sunt până la expirarea licenței.În cazul în care utilizați o versiune de evaluare sau dacă licența dumneavoastră se apropie de data expirării, puteți face clic pe **Cumpărați acum** pentru a achiziționa o serie de înregistrare.Pentru mai multe detalii, consultați *„Înregistrare și Contul meu”* (p. 52).

7.1.2. Zona Protejați-vă calculatorul

Aici puteți efectua acțiunile necesare pentru gestionarea protecției dumneavoastră.

Sunt disponibile trei butoane:

- **Securitate** vă asigură comenzi rapide către sarcinile și setările de securitate.
- **Actualizează acum** vă permite să actualizați semnăturile de viruși și fișierele de produs ale BitDefender.Va apărea o nouă fereastră în care puteți vedea starea actualizării.Dacă sunt detectate actualizări, acestea sunt descărcate automat și instalate pe calculatorul dumneavoastră.
- **Instrumentele mele** vă permite să creați comenzi rapide către sarcinile și setările dumneavoastră preferate.

Pentru a efectua o sarcină sau a configura setări, faceți clic pe butonul corespunzător și alegeți instrumentul dorit din meniu.Pentru a adăuga sau elimina comenzi rapide, faceți clic pe butonul corespunzător și alegeți **Opțiuni suplimentare**.Pentru mai multe detalii, consultați *„Instrumentele mele”* (p. 33).

7.1.3. Zona de ajutor

Aici puteți afla cum să utilizați BitDefender Internet Security 2011 și cum să obțineți asistență.

Sfaturile utile reprezintă o manieră distractivă și ușoară de a învăța despre cele mai bune practici de securitate legate de calculatoare și modul de utilizare a BitDefender Internet Security 2011.

Dacă aveți nevoie de ajutor, tastați un cuvânt cheie sau o întrebare în câmpul **Asistență** și faceți clic pe **Caută**.

7.2. Modul Intermediar

Destinat utilizatorilor cu aptitudini medii de operare a calculatorului, Modul Intermediar afișează o interfață simplă, care vă oferă acces la toate modulele, la nivel de bază. În acest mod, va trebui să urmăriți avertismentele și alertele importante și să remediați problemele nedorite.

În Modul Intermediar, fereastra principală este organizată în mai multe file.

Stare
: Pagina de stare vă ajută să monitorizați și să gestionați cu ușurință protecția sistemului dumneavoastră.

Securitate
: Afișează starea setărilor de securitate și vă ajută să remediați problemele detectate.Puteți rula sarcini de securitate sau configura setările de securitate.

Rețea
Afișează structura rețelei BitDefender.Aici puteți efectua diverse acțiuni pentru a configura și administra produsele BitDefender instalate în rețeaua dumneavoastră personală.În acest fel, puteți administra securitatea rețelei personale de la un singur calculator.

Butonul **Opțiuni** din colțul dreapta sus al ferestrei vă permite să schimbați modul de vizualizare a interfeței și să configurați principalele setări ale programului.

În colțul din dreapta jos al ferestrei, puteți găsi mai multe linkuri utile.

Link	Descriere
Informații licență	Deschide o fereastră în care puteți vedea informații despre licența actuală și unde vă puteți înregistra produsul cu o nouă serie de înregistrare.
Jurnale	Vă permite să vedeți un istoric detaliat al tuturor sarcinilor efectuate de BitDefender pe sistemul dumneavoastră.
Cumpără	Vă ajută să achiziționați o serie de înregistrare pentru produsul dumneavoastră BitDefender Internet Security 2011.
Asistență	Faceți clic pe acest link dacă aveți nevoie de ajutor cu BitDefender.
	Deschide un fișier de ajutor care vă ajută să utilizați BitDefender.

7.2.1. Stare

Pagina de stare vă ajută să monitorizați și să gestionați cu ușurință protecția sistemului dumneavoastră.

Pagina de stare conține următoarele secțiuni:

- **Detalii stare** indică starea fiecărui modul principal folosind propoziții explicite și una dintre următoarele iconițe:

  Cerc verde cu bifă: Nicio problemă de securitate.Calculatorul și datele dumneavoastră sunt protejate.

  Cerc roșu cu semnul exclamării: Mai multe probleme afectează securitatea sistemului dumneavoastră.Problemele majore necesită atenția dvs imediat. Problemele minore trebuie remediate cât mai curând.

  Cerc gri cu semnul exclamării: Activitatea componentelor acestui modul nu este monitorizată. Prin urmare, nu sunt disponibile informații legate de starea lor de securitate.Pot exista anumite probleme legate de acest modul.

Faceți clic pe numele unui modul pentru a vedea mai multe detalii despre starea sa și pentru a configura monitorizarea stării componentelor sale.

- **Starea licenței** afișează câte zile mai sunt până la expirarea licenței.În cazul în care utilizați o versiune de evaluare sau dacă licența dumneavoastră se apropie de data expirării, puteți face clic pe **Cumpărați acum** pentru a achiziționa o serie de înregistrare.Pentru mai multe detalii, consultați *„Înregistrare și Contul meu”* (p. 52).
- **Instrumentele mele** vă permite să creați comenzi rapide către sarcinile și setările dumneavoastră preferate.Pentru mai multe detalii, consultați *„Instrumentele mele”* (p. 33).
- **Sfaturile utile** reprezintă o manieră distractivă și ușoară de a învăța despre cele mai bune practici de securitate legate de calculatoare și modul de utilizare a BitDefender Internet Security 2011.

7.2.2. Securitate

Fila Securitate vă permite să gestionați securitatea calculatorului și a datelor dumneavoastră.

„Zona de stare” (p. 29)
„Sarcini rapide” (p. 30)

Zona de stare

În zona de stare puteți vedea lista completă a componentelor de securitate monitorizate și starea lor actuală.Ca urmare a monitorizării fiecărui modul de securitate, BitDefender vă va alerta nu numai când configurați setări care pot afecta securitatea calculatorului dumneavoastră, ci și atunci când uitați să executați sarcini importante.

Starea curentă a fiecărei componente este indicată prin propoziții explicite și una dintre următoarele iconițe:

Cerc verde cu bifă: Nicio problemă nu afectează componenta.

Cerc roșu cu semnul exclamării: Mai multe probleme afectează componenta.

Faceți clic pe butonul **Remediază** din dreptul unei descrieri pentru a remedia problema semnalată.Dacă o problemă nu este remediată pe loc, urmați pașii programului asistent.

Pentru a configura care componente trebuie monitorizate:

1. Faceți clic pe **Adăugare/Editare listă**.
2. Pentru a activa sau dezactiva monitorizarea unui anumit element, utilizați selectorul corespunzător.
3. Faceți clic pe **Închide** pentru a salva modificările și pentru a închide fereastra.

Important
Pentru a vă asigura că sistemul dumneavoastră este complet protejat, activați monitorizarea tuturor componentelor și remediați toate problemele raportate.

Sarcini rapide

Aici găsiți linkuri către cele mai importante sarcini de securitate:

- **Actualizează acum** - inițiază o actualizare imediată.
- **Scanare completă** - pornește o scanare standard a întregului calculator (fără arhive). Pentru sarcini de scanare suplimentare, faceți clic pe săgeata de pe acest buton și selectați o altă sarcină de scanare.
- **Scanare personalizată** - pornește un asistent care vă permite să creați și să rulați o sarcină de scanare personalizată.
- **Scanare vulnerabilități** - pornește un asistent care verifică sistemul de vulnerabilități și vă ajută să le rezolvați.
- **Configurare Firewall** - deschide o fereastră în care puteți vizualiza și configura setările firewall.Pentru mai multe informații, consultați *„Firewall”* (p. 128).

7.2.3. Rețea

Aici puteți efectua diverse acțiuni pentru a configura și administra produsele BitDefender instalate în rețeaua dumneavoastră personală.În acest fel, puteți administra securitatea rețelei personale de la un singur calculator.

Pentru mai multe detalii, consultați *„Rețea personală”* (p. 152).

7.3. Modul Expert

Modul Expert oferă acces la fiecare componentă a BitDefender. Aici puteți configura BitDefender în detaliu.

Notă
Modul Expert este potrivit pentru utilizatorii cu abilități de operare a calculatorului peste medie, care știu la ce fel de pericole este expus calculatorul și cum funcționează programele de securitate.

În partea stângă a ferestrei există un meniu care conține toate modulele de securitate.Fiecare modul are unul sau mai multe taburi în care puteți configura setările de securitate corespunzătoare sau puteți efectua sarcini de securitate sau administrative.Următoarea listă descrie pe scurt fiecare modul.Pentru mai multe detalii, consultați secțiunea „Configurare și administrare” (p. 56) a acestui manual.

General
Vă permite să accesați setările generale sau să vizualizați pagina de stare și informații detaliate despre sistem.

Antivirus
Vă permite să configurați protecția antivirus în timp real și operațiile de scanare, să setați excepții și să configurați modulul de carantină.Aici puteți configura de asemenea protecția antiphishing și Consilierul pentru căutare.

Antispam
Vă permite să țineți mesajele spam la distanță de căsuța dumneavoastră de mesaje și să configurați setările antispam în detaliu.

Control parental
Vă permite să vă protejați copiii împotriva conținutului inadecvat utilizând regulile dumneavoastră privind accesul la calculator.

Control date
Vă permite să preveniți furtul de date de pe calculatorul dumneavoastră și să vă protejați confidențialitatea în timp ce sunteți online.

Firewall
Vă protejează calculatorul de tentative de conexiune neautorizată la ieșire sau la intrare. Modulul este asemănător unui paznic – supraveghează conexiunea la Internet și monitorizează aplicațiile cărora le este permis accesul la Internet precum și pe cele care trebuie blocate.

Vulnerabilitate
Vă permite să mențineți actualizate cele mai importante aplicații de pe calculatorul dumneavoastră.

Criptare
Vă permite să criptați comunicațiile prin Yahoo și Windows Live (MSN) Messenger.

Mod jocuri/laptop
Vă permite să amânați executarea sarcinilor BitDefender programate cât timp laptopul dumneavoastră funcționează pe baterii și, de asemenea, să eliminați toate alertele și pop-upurile atunci când vă jucați pe calculator.

Rețea personală
Vă permite să configurați și să administrați mai multe calculatoare din locuința dumneavoastră.

Actualizare
Vă permite să obțineți informații despre cele mai recente actualizări, să actualizați produsul și să configurați procesul de actualizare în detaliu.

Înregistrare
Vă permite să înregistrați BitDefender Internet Security 2011, să schimbați seria de înregistrare sau să creați un cont BitDefender.

Butonul **Opțiuni** din colțul dreapta sus al ferestrei vă permite să schimbați modul de vizualizare a interfeței și să configurați principalele setări ale programului.

În colțul din dreapta jos al ferestrei, puteți găsi mai multe linkuri utile.

Link	Descriere
Informații licență	Deschide o fereastră în care puteți vedea informații despre licența actuală și unde vă puteți înregistra produsul cu o nouă serie de înregistrare.
Jurnale	Vă permite să vedeți un istoric detaliat al tuturor sarcinilor efectuate de BitDefender pe sistemul dumneavoastră.
Cumpără	Vă ajută să achiziționați o serie de înregistrare pentru produsul dumneavoastră BitDefender Internet Security 2011.
Asistență	Faceți clic pe acest link dacă aveți nevoie de ajutor cu BitDefender.
?	Deschide un fișier de ajutor care vă ajută să utilizați BitDefender.

8. Instrumentele mele

La utilizarea BitDefender în Modul Novice sau Modul Intermediar de vizualizare, puteți personaliza tabloul de comandă adăugând comenzi rapide la sarcini și setări care sunt importante pentru dumneavoastră.Astfel, puteți obține rapid acces la caracteristicile pe care le utilizați de obicei și la setările avansate, fără a fi necesar să comutați la un mod mai avansat de vizualizare a interfeței.

În funcție de modul de vizualizare a interfeței utilizat, comenzile rapide adăugate la instrumentele mele sunt disponibile după cum urmează:

Modul Novice
: În zona Protejați-vă calculatorul!, faceți clic pe Instrumentele mele.Va apărea un meniu.Faceți clic pe o comandă rapidă pentru a lansa instrumentul corespunzător.

Modul Intermediar
: Comenzile rapide apar în secțiunea Instrumentele mele.Faceți clic pe o comandă rapidă pentru a lansa instrumentul corespunzător.

Pentru a deschide fereastra din care puteți selecta comenzile rapide ce vor apărea în secțiunea Instrumentele mele, procedați după cum urmează:

Modul Novice
: În zona Protejați-vă calculatorul!, faceți clic pe Instrumentele mele și selectați **Opțiuni suplimentare**.

Modul Intermediar
: Faceți clic pe unul dintre butoanele din Instrumentele mele sau pe linkul **Configurează Instrumentele mele**.

Utilizați selectoarele pentru a alege instrumentele ce vor fi adăugate la Instrumentele mele.Puteți selecta oricare dintre următoarele categorii de instrumente.

- **Sarcini de scanare**

  Adăugați sarcinile pe care le utilizați de obicei pentru a scana sistemul în scopul identificării amenințărilor de securitate.

Sarcină de scanare	Descriere
Scanare profundă	Scanează întregul sistem.În configurația implicită, se scanează după toate tipurile de aplicații periculoase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spion, adware, obiecte ascunse (rootkituri) și altele.
Scanare completă sistem	Scanează întregul sistem, cu excepția arhivelor.În configurația implicită, se scanează după toate tipurile

Sarcină de scanare	Descriere
	de aplicații periculoase, cu excepția celor de tip rootkit.
Quick Scan	Scanarea rapidă utilizează o tehnologie de scanare "in-the-cloud" (online) pentru a detecta aplicațiile periculoase ce rulează pe sistemul dumneavoastră. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o fracțiune din resursele de sistem necesare pentru o scanare antivirus obișnuită.
Scanare personalizată	Pornește programul asistent care vă permite să creați o sarcină de scanare personalizată.
Scanare documente	Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` și `StartUp`. Astfel, veți asigura siguranța documentelor dumneavostră, un spațiu de lucru sigur și rularea la pornirea sistemului a unor aplicații necompromise.
Programează scanări	Deschide fereastra de setări antivirus, unde puteți personaliza sarcinile de scanare la cerere.

Pentru mai multe informații despre sarcinile de scanare, consultați *„Administrarea sarcinilor de scanare existente”* (p. 73).

- **Opțiuni**

Adăugați comenzi rapide la setările BitDefender pe care doriți să le configurați:

Opțiuni	Descriere
Setări antivirus	Configurați modulul antivirus. Pentru mai multe informații, consultați *„Protecție antivirus”* (p. 61).
Configurare Firewall	Configurați modulul firewall. Pentru mai multe informații, consultați *„Firewall”* (p. 128).
Control parental	Configurați modulul Control parental. Pentru mai multe informații, consultați *„Control parental”* (p. 102).
Modul pentru jocuri	Comutați în modul pentru jocuri. Pentru mai multe informații, consultați *„Modul pentru jocuri”* (p. 146).
Modul pentru laptop	Comutați în modul laptop. Pentru mai multe informații, consultați *„Modul pentru laptop”* (p. 149).

Opțiuni	Descriere
Actualizează	Realizați o actualizare a BitDefender. Pentru mai multe informații, consultați *„Actualizare”* (p. 156).
Afișează & remediază toate problemele	Deschideți programul asistent care vă va ajuta să soluționați toate problemele de securitate ce vă afectează sistemul. Pentru mai multe informații, consultați *„Remedierea problemelor”* (p. 42).

- **Ajutor & asistență**

  Accesați secțiunea de asistență. Pentru mai multe informații, consultați „Contactați-ne direct din cadrul produsului dumneavoastră BitDefender” (p. 201).

9. Alerte și ferestre pop-up

BitDefender utilizează ferestre pop-up și alerte pentru a vă informa despre funcționarea sa și despre evenimente speciale care v-ar putea interesa și pentru a vă solicita să alegeți o acțiune atunci când este nevoie.Acest capitol prezintă ferestrele pop-up ale BitDefender și alertele pe care le puteți întâlni.

Ferestrele pop-up sunt ferestre de mici dimensiuni care apar temporar pe ecran pentru a vă informa în legătură cu diversele evenimente BitDefender, cum ar fi scanarea mesajelor e-mail, un calculator nou care s-a conectat la rețeaua dumneavoastră fără fir (wireless), o regulă de firewall adăugată etc.Atunci când apare o fereastră pop-up, vi se va solicita să faceți clic pe un buton **OK** sau un link, cel mult.

Alertele sunt ferestre de dimensiuni mai mari care vă solicită să efectuați o acțiune sau vă informează în legătură cu un aspect foarte important (de exemplu depistarea unui virus.)Pe lângă ferestrele de alertă, puteți primi e-mailuri, mesaje instantant sau pagini web de alertă.

Printre ferestrele pop-up și alertele BitDefender se numără:

- Alerte antivirus
- Alerte Active Virus Control
- Alerte privind detectarea dispozitivelor
- Ferestre pop-up și alerte referitoare la firewall
- Pagini web de alertă antiphishing
- Mesaje de alertă privind Controlul parental
- Alerte privind controlul datelor personale

9.1. Alerte antivirus

BitDefender vă protejează împotriva a numeroase tipuri de aplicații periculoase (malware), cum ar fi virușii, aplicațiile spion sau de tip rootkit.Atunci când detectează un virus sau un alt cod periculos, BitDefender aplică o anumită acțiune fișierului infectat și vă informează în legătură cu acesta printr-o fereastră de alertă.

Puteți vedea numele virusului, calea către fișierul infectat și acțiunea luată de BitDefender.

Faceți clic pe **OK** pentru a închide fereastra.

Important

La identificarea unui virus, este recomandat să vă scanați tot calculatorul pentru a vă asigura că nu există și alți viruși.Pentru mai multe informații, consultați *„Cum scanez fișiere și directoare?”* (p. 161).
Dacă virusul nu a fost blocat, consultați *„Eliminarea virușilor din sistem”* (p. 191).

9.2. Alerte Active Virus Control

Modulul Active Virus Control poate fi configurat să vă alerteze și să vă solicite să acționați atunci când o aplicație încearcă să efectueze o acțiune cu potențial periculos.

Dacă utilizați Modul Novice sau Modul Intermediar de vizualizare a interfeței, o fereastră pop-up vă va informa de fiecare dată când Active Virus Control blochează o aplicație potențial periculoasă.În cazul în care utilizați Modul Expert de vizualizare, vi se va solicita să alegeți o anumită acțiune, prin intermediul unei ferestre de alertă, atunci când o aplicație are un comportament rău intenționat.

Dacă aplicația detectată este cunoscută, faceți clic pe **Permite**.

Dacă doriți să închideți imediat aplicația, faceți clic pe **OK**.

Selectați căsuța **Reține acțiunea pentru această aplicație** înainte de a face selecția și BitDefender va aplica aceeași acțiune la detectarea ulterioară a aplicației.Regula creată astfel va fi afișată în fereastra de configurare a Active Virus Control.

9.3. Alerte privind detectarea dispozitivelor

BitDefender detectează automat unitățile mobile de stocare pe care le conectați la calculator și propune scanarea lor înainte să accesați fișierele pe care le conțin acestea.Acest lucru este recomandat pentru a preveni pătrunderea virușilor și a altor aplicații periculoase pe calculatorul dumneavoastră.

Unitățile detectate fac parte din următoarele categorii:

- CD/DVD
- unități de stocare pe USB, cum ar fi memoriile flash sau hard discurile externe
- unități de rețea mapate (la distanță)

La detectarea unei astfel de unități se afișează o fereastră de alertă.

Pentru a scana unitatea de stocare, faceți clic pe **Da**.Va apărea programul asistent Scanare antivirus, care vă va ghida în procesul de scanare.

Dacă nu doriți să scanați unitatea, faceți clic pe **Nu**. În acest caz, v-ar putea fi de folos una dintre aceste opțiuni:

- **Nu mă mai întreba despre acest tip de unitate** - BitDefender nu va mai propune scanarea unităților de stocare de acest tip atunci când acestea sunt conectate la calculator.
- **Dezactivează detecția automată a unităților** - Nu vi se va mai propune să scanați noile unități de stocare atunci când acestea sunt conectate la calculator.

Dacă ați dezactivat detecția automată a unităților în mod accidental și vreți s-o reactivați sau să-i configurați setările, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus>Scanare viruși**.
3. În lista de sarcini de scanare, localizați sarcina **Scanare dispozitive**.
4. Faceți clic pe sarcină și selectați **Proprietăți**.Va apărea o nouă fereastră.
5. Pe tabul **Generalități**, configurați opțiunile de scanare după cum este necesar.Pentru mai multe informații, consultați *„Configurarea setărilor de scanare”* (p. 76).
6. Pe tabul **Detecție**, alegeți tipurile de unități de stocare care să fie detectate.
7. Faceți clic pe **OK** pentru a salva și aplica modificările.

9.4. Ferestre pop-up și alerte referitoare la firewall

Firewallul utilizează ferestre pop-up pentru a vă informa în legătură cu diverse evenimente legate de conexiunea dumneavoastră la rețea (de exemplu, atunci când un nou calculator se conectează la rețeaua Wi-Fi, atunci când unei noi aplicații îi este permis să aibă acces la internet sau când este blocată o scanare de porturi).Aceste ferestre pop-up pot fi foarte utile pentru detectarea încercărilor de pătrundere în sistem a programelor sau persoanele rău intenționate, protejându-vă astfel împotriva amenințărilor din rețea.

În cazul în care utilizați Modul Expert de vizualizare, vi se va solicita să alegeți o anumită acțiune, prin intermediul unei ferestre de alertă, ori de câte ori o aplicație necunoscută încearcă să se conecteze la internet.

Puteți vedea aplicația care încearcă să acceseze internetul, calea către aceasta, destinația, protocolul utilizat și portul prin care aplicația încearcă să se conecteze.

Faceți clic pe **Permite** pentru a permite tot traficul (la intrare și la ieșire) generat de această aplicație de pe calculatorul local către orice destinație, prin protocolul IP respectiv și pe toate porturile. Dacă faceți clic pe **Blochează**, va fi refuzat complet accesul aplicației la Internet prin protocolul IP respectiv.

Important
Permiteți tentative de conectare la intrare doar de la adrese IP sau domenii în care aveți încredere.

Pe baza răspunsului dumneavoastră, va fi creată o regulă, care va fi aplicată și listată în tabel. Data viitoare când aplicația va încerca să se conecteze, această regulă va fi aplicată implicit.

Dacă utilizați Modul Novice sau Modul Intermediar de vizualizare, încercarea de conectare va fi blocată în mod automat.

9.5. Alerte Antiphishing

Cu protecția antiphishing activată, BitDefender vă va avertiza în momentul în care veți încerca să accesați pagini care ar putea avea ca scop furtul de informații personale.Înainte să accesați o astfel de pagină web, BitDefender va bloca pagina respectivă și va afișa în schimb o alertă generică.

Verificați adresa paginii web în bara de adrese a browserului dumneavoastră.Căutați indicii care ar putea indica faptul că pagina web respectivă este folosită pentru phishing.Dacă adresa este suspectă, este recomandat să nu o deschideți.

Iată câteva indicii care ar putea fi utile:

- Dacă ați introdus manual adresa unui site web legitim, verificați dacă adresa este corectă. Dacă adresa nu este corectă, reintroduceți-o și mergeți din nou la acea adresă.
- Dacă ați dat clic pe un link dintr-un e-mail sau dintr-un mesaj instant, verificați cine vi l-a trimis. Dacă nu recunoașteți persoana care v-a trimis linkul, probabil ca mesajul reprezintă o tentativă de phishing. În cazul în care cunoașteți expeditorul, este recomandat să verificați dacă mesajul a fost trimis într-adevăr de către acea persoană.
- Dacă ați găsit pagina web întâmplător, navigând pe Internet, verificați pagina unde ați găsit acel link (faceți clic pe butonul Back al browserului dumneavoastră).

Dacă doriți să vizualizați pagina, faceți clic pe linkul corespunzător pentru a realiza una dintre aceste acțiuni:

- **Vizualizarea paginii numai de această dată.** Nu există niciun risc atâta timp cât nu introduceți date personale în acea pagină.Dacă pagina este una legitimă, o puteți adăuga pe lista albă (faceți clic pe bara de instrumente BitDefender Antiphishing și selectați **Adaugă pe lista albă**).
- **Adaugarea paginii pe lista albă.** Pagina va fi afișată imediat, iar BitDefender nu vă va mai alerta niciodată în legătură cu aceasta.

Important

Adăugați pe lista albă numai paginile web în care aveți deplină încredere (de exemplu pagina web a băncii dumneavoastră, magazine online cunoscute, etc).BitDefender nu verifică paginile web de pe Lista albă pentru a descoperi eventuale tentative de furt de informații personale.

Puteți administra protecția antiphishing si lista albă folosind bara de instrumente BitDefender din browserul dumneavoastră.Pentru mai multe informații, consultați *„Administrarea protecției antiphishing BitDefender din Internet Explorer și Firefox”* (p. 86).

9.6. Mesaje de alertă privind Controlul parental

Puteți configura Controlul parental să blocheze:

- pagini web inadecvate.
- accesul la Internet, pentru anumite intervale de timp (de exemplu, în timpul rezervat lecțiilor).
- paginile web, mesajele e-mail și mesajele instant care conțin anumite cuvinte cheie.
- jocuri, aplicații de chat, partajare de fișiere și altele.
- mesaje instant trimise de alte contacte de mesagerie instant decât cele permise.

Utilizatorul este informat de fiecare dată când o activitate este blocată prin intermediul unui anumit mesaj de alertă (de exemplu, o pagină web, un e-mail sau un mesaj instantaneu standard de alertă).Sunt oferite informații detaliate pentru ca utilizatorul să poată afla motivul pentru care activitatea a fost blocată.

9.7. Alerte privind controlul datelor personale

Controlul datelor personale oferă utilizatorilor avansați caracteristici adiționale pentru protejarea datelor personale.Dacă alegeți să activați oricare dintre aceste componente, vi se va solicita să efectuați o acțiune prin intermediul unor ferestre de alertă:

- Controlul regiștrilor - vă cere permisiunea de fiecare dată când un program încearcă să modifice informațiile din regiștri astfel încât să fie lansat la pornirea Windows.
- Controlul fișierelor cookie - vă cere permisiunea de fiecare dată când un site încearcă să seteze un cookie.
- Controlul scripturilor - vă cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ.

9.7.1. Alerte regiștri

În cazul în care activați Controlul regiștrilor, vi se va solicita permisiunea de fiecare dată când un nou program încearcă să modifice o cheie de regiștri pentru a putea fi rulat la pornirea sistemului Windows.

Puteți vedea programul care încearcă să modifice regiștrii Windows.

Notă

BitDefender vă va alerta atunci când instalați programe pentru care este necesară lansarea la pornirea Windows. În cele mai multe cazuri, aceste programe sunt legitime și sigure.

Dacă nu recunoașteți programul și acesta pare suspect, faceți clic pe **Blochează** pentru a-l împiedica să modifice regiștrii Windows.Altfel, faceți clic pe **Permite** pentru a permite modificarea.

Pe baza răspunsului dumneavoastră, o regulă este creată și listată în tabelul de reguli.Aceeași acțiune este aplicată de fiecare dată când acest program încearcă să modifice o cheie de regiștri.

Pentru mai multe informații, consultați *„Control regiștri”* (p. 124).

9.7.2. Alerte de scripturi

În cazul în care activați Controlul scripturilor, vi se va solicita permisiunea de fiecare dată când un nou website încearcă să ruleze un script sau alt conținut activ.

Puteți vedea numele resursei.

Faceți clic pe **Da** sau pe **Nu** pentru ca o nouă regulă să fie creată, aplicată și listată în tabelul de reguli.Aceeași acțiune va fi aplicată automat ori de câte ori respectivul site încearcă să ruleze conținut activ.

Notă
Este posibil ca unele pagini web să nu fie afișate corect dacă blocați conținutul activ.

Pentru mai multe informații, consultați *„Control scripturi”* (p. 126).

9.7.3. Alerte fișiere cookie

În cazul în care activați Controlul fișierelor cookie, vi se va solicita permisiunea de fiecare dată când un nou site web încearcă să seteze sau să solicite un cookie.

Puteți vedea numele aplicației care încearcă să trimită fișierul cookie.

Faceți clic pe **Da** sau pe **Nu** pentru ca o nouă regulă să fie creată, aplicată și listată în tabelul de reguli.Aceeași acțiune va fi aplicată automat ori de câte ori accesați respectivul site.

Pentru mai multe informații, consultați *„Controlul fișierelor cookie”* (p. 125).

10. Remedierea problemelor

BitDefender folosește un sistem de monitorizare pentru a detecta și a vă informa despre problemele care pot afecta securitatea calculatorului și a datelor dumneavoastră. În mod implicit, sunt monitorizate numai problemele considerate a fi foarte importante. Totuși, puteți configura sistemul după cum doriți, prin alegerea problemelor despre care doriți să primiți notificări.

Existența unor probleme este semnalată astfel:

- Un simbol special este afișat deasupra iconiței BitDefender din bara de sistem pentru a semnala existența unor probleme.De asemenea, dacă plasați cursorul mouse-ului peste iconiță, o fereastră pop-up va confirma existența unor probleme.
- Când deschideți BitDefender, zona de stare a securității va indica numărul de probleme care afectează sistemul dvs.
  - În Modul Novice, starea de securitate este afișată în partea stângă a ferestrei.
  - În Modul Expert, mergeți la **General>Stare** pentru a verifica starea de securitate.

10.1. Asistentul de remediere a problemelor

Cel mai ușor mod de a remedia problemele existente este să urmați pașii **asistentului de remediere a problemelor**.Pentru a porni asistentul, aveți următoarele alternative:

- Faceți clic-dreapta pe iconița BitDefender din bara de sistem și selectați **Remediază tot**.
- Deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:
  - În Modul Novice, faceți clic pe **Remediază tot**.
  - În Modul Expert, mergeți la **General > Stare** și faceți clic pe **Afișează toate problemele**.

> **Notă**
> De asemenea, puteți adăuga o comandă rapidă în Instrumentele mele.

Este afișată lista de amenințări curente la adresa securității calculatorului dumneavoastră.

Toate problemele curente sunt selectate pentru a fi remediate. Dacă nu doriți ca o anumită problemă să fie remediată, debifați căsuța corespunzătoare acesteia. Dacă faceți acest lucru, starea problemei în cauză va fi înlocuită cu **Omite**.

Notă

Dacă nu doriți să fiți informat despre anumite probleme, trebuie să configurați sistemul de alerte în consecință, conform instrucțiunilor din secțiunea următoare.

Pentru a rezolva problemele selectate, faceți clic pe **Start**. Unele probleme sunt remediate imediat. Pentru remedierea celorlalte, veți avea la dispoziție programe asistent separate.

Problemele pe care acest program asistent vă permite să le remediați pot fi grupate în următoarele categorii principale:

- **Setări de securitate dezactivate.** Aceste probleme sunt remediate pe loc, prin activarea setărilor de securitate în cauză.
- **Sarcini de securitate preventive pe care trebuie să le efectuați.** Un exemplu de astfel de sarcină este scanarea calculatorului. Este recomandat să vă scanați calculatorul cel puțin o dată pe săptămână. BitDefender va efectua această scanare automat, în majoritatea cazurilor. Dacă ați modificat programul de scanare sau dacă acest program nu este finalizat, veți fi informat despre această problemă.

  Când remediați astfel de probleme, un program asistent vă ajută să finalizați sarcina cu succes.
- **Vulnerabilități ale sistemului.** BitDefender verifică automat dacă există vulnerabilități în sistemul dumneavoastră și vă informează în legătură cu acestea.În categoria vulnerabilităților sistemului intră:
  - parolele simple ale conturilor de utilizator Windows.
  - programele neactualizate de pe calculatorul dumneavoastră.
  - actualizări Windows lipsă.
  - actualizarea automată a Windows este dezactivată.

  Atunci când remediați astfel de probleme, este lansat programul asistent de verificare a vulnerabilităților. Acesta vă permite să remediați vulnerabilitățile detectate în sistem.Pentru informații detaliate, consultați secțiunea *„Căutare după vulnerabilități”* (p. 141).

10.2. Configurarea alertelor de stare

Sistemul de alertare este preconfigurat pentru a monitoriza și pentru a vă alerta în legătură cu principalele probleme care pot afecta securitatea calculatorului și datelor dumneavoastră.În afară de problemele monitorizate în mod implicit, există o serie de alte probleme despre care puteți fi informat.

Puteți configura sistemul de alertare conform preferințelor dumneavoastră selectând problemele specifice despre care doriți să fiți informat.Puteți face aceasta fie în Modul Intermediar, fie în Modul Expert de vizualizare.

- În Modul Intermediar de vizualizare, sistemul de alertare poate fi configurat din locații diferite.Urmați acești pași:
  1. Accesați fila **Securitate**.
  2. Faceți clic pe linkul **Adăugare/Editare listă** din zona de stare.
  3. Utilizați selectorul corespunzător pentru a modifica starea de alertă a unui element.
- În Modul Expert, sistemul de alertare poate fi configurat dintr-o singură locație.Urmați acești pași:
  1. Mergeți la **General > Stare**.
  2. Faceți clic pe **Adăugare/Editare alerte**.
  3. Utilizați selectorul corespunzător pentru a modifica starea de alertă a unui element.

11. Configurarea setărilor principale

Puteți să configurați setările principale de produs (inclusiv să reconfigurați profilul de utilizare) din fereastra de preferințe. Pentru a o deschide, aveți următoarele opțiuni:

- Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul dreapta sus al ferestrei și alegeți **Preferințe**.
- Faceți clic-dreapta pe iconița BitDefender din bara de sistem și selectați **Preferințe**.

Notă

Pentru configurarea detaliată a setărilor de produs, folosiți interfața în Modul Expert de vizualizare.Pentru mai multe detalii, consultați secțiunea „Configurare și administrare” (p. 56) a acestui manual.

Setările sunt grupate în trei categorii:

- Setări de securitate
- Setări alerte
- Setări generale

Pentru a activa sau dezactiva o setare, utilizați selectorul corespunzător.

Pentru a aplica și a salva modificările de configurație pe care le faceți, faceți clic pe **OK**. Pentru a închide fereastra fără a salva modificările, faceți clic pe **Anulează**.

Linkul **Reconfigurează profil** din colțul dreapta sus a ferestrei vă permite să reconfigurați profilul de utilizare.Pentru mai multe informații, consultați *„Reconfigurarea profilului de utilizare”* (p. 49).

11.1. Setări de securitate

În această zonă, puteți activa sau dezactiva setările de produs care acoperă diverse aspecte ale securității calculatorului și a datelor.Pentru a activa sau dezactiva o setare, utilizați selectorul corespunzător.

Avertisment

Atenție când dezactivați protecția în timp real, firewallul sau actualizarea automată.Dezactivarea acestor funcționalități poate compromite securitatea calculatorului dumneavoastră. Dacă este necesar să le dezactivați, amintiți-vă să le activați din nou cât mai curând posibil.

Acestea sunt setările disponibile:

Antivirus
Protecția în timp real asigură scanarea tuturor fișierelor accesate de dvs sau de o aplicație care rulează pe acest sistem.

Actualizarea Automată
Actualizarea automată asigură descărcarea și instalarea automată, în mod regulat, a celor mai recente fișiere de produs și semnături BitDefender.Actualizările sunt efectuate în mod implicit la fiecare oră.

Scanare vulnerabilități
Funcția de verificare automată a vulnerabilităților vă alertează și vă ajută să remediați vulnerabilitățile din sistemul dumneavoastră care îi pot afecta securitatea. Astfel de vulnerabilități includ programe neactualizate, parole slabe pentru conturile de utilizator sau actualizări Windows absente.

Antispam
Protecția Antispam filtrează mesajele e-mail pe care le primiți, marcându-le pe cele nedorite ca SPAM.

Antiphishing
Protecția antiphishing detectează și vă alertează în timp real dacă o pagină web este folosită pentru furt de informații personale.

Consilier pentru căutare
Consilierul pentru căutare scanează linkurile din rezultatele dumneavostră de căutare și vă informează care dintre acestea sunt sigure și care nu.

Control identitate
Controlul identității vă permite să împiedicați trimiterea de date cu caracter personal pe Internet, fără consimțământul dumneavoastră. Această opțiune blochează orice mesaj instant, e-mail sau formular web prin care se transmit către destinatari neautorizați (adrese) date pe care le-ați identificat ca având caracter personal.

Criptare chat
Criptarea chatului asigură confidențialitatea conversațiilor dumneavoastră prin Yahoo! Messenger și Windows Live Messenger cu interlocutori care folosesc un produs BitDefender și o aplicație de mesagerie instant compatibile.

Control parental (utilizator curent)
Controlul parental restricționează activitățile desfășurate pe calculator și online de către copii, pe baza regulilor definite de dumneavoastră. Restricțiile pot include blocarea accesului la site-uri web cu conținut inadecvat precum și limitarea accesului la jocuri și la Internet, conform programului indicat.

Firewall
Firewallul vă protejează calculatorul de atacurile din exterior ale hackerilor și aplicațiilor periculoase.

Starea unora dintre aceste setări poate fi monitorizată de sistemul BitDefender de monitorizare a problemelor.Dacă dezactivați o setare monitorizată, BitDefender va semnala acest lucru ca pe o problemă pe care trebuie s-o remediați.

Dacă nu doriți ca o setare monitorizată pe care ați dezactivat-o să fie semnalată ca problemă, trebuie să configurați sistemul de monitorizare în consecință. Puteți face acest lucru fie în Modul Intermediar, fie în Modul Expert de vizualizare.Pentru mai multe detalii, consultați *„Configurarea alertelor de stare”* (p. 43).

11.2. Setări alerte

În această zonă, puteți dezactiva ferestrele pop-up și alertele BitDefender.BitDefender utilizează alerte pentru a vă solicita să efectuați o anumită acțiune și ferestre pop-up pentru a vă informa în legătură cu acțiunile pe care le-a efectuat în mod automat sau în legătură cu alte evenimente.Pentru a activa sau dezactiva o categorie de alerte, utilizați selectorul corespunzător.

Important
Majoritatea acestor alerte și ferestre pop-up trebuie menținute active pentru a evita posibilele probleme.

Acestea sunt setările disponibile:

Alerte antivirus
Alertele antivirus vă informează când BitDefender detectează și blochează un virus.La identificarea unui virus, este recomandat să vă scanați tot calculatorul pentru a vă asigura că nu există și alți viruși.

Ferestre pop-up Active Virus Control
Dacă utilizați Modul Novice sau Modul Intermediar de vizualizare a interfeței, o fereastră pop-up vă va informa de fiecare dată când Active Virus Control blochează o aplicație potențial periculoasă.În cazul în care utilizați Modul Expert de vizualizare, vi se va solicita să alegeți o anumită acțiune, prin intermediul unei ferestre de alertă, atunci când o aplicație are un comportament rău intenționat.

Ferestre pop-up pentru scanare e-mail
Aceste ferestre pop-up sunt afișate pentru a vă informa că BitDefender scanează e-mailurile pentru identificarea programelor malware.

Alerte de Administrare rețea personală
Aceste alerte informează utilizatorul în legătură cu acțiuni administrative ce sunt efectuate de la distanță.

Ferestre pop-up pentru firewall
Firewallul utilizează ferestre pop-up pentru a vă informa în legătură cu diverse evenimente legate de conexiunea dumneavoastră la rețea (de exemplu, atunci când un nou calculator se conectează la rețeaua Wi-Fi, atunci când unei noi

aplicații îi este permis să aibă acces la internet sau când este blocată o scanare de porturi).În cazul în care utilizați Modul Expert de vizualizare, vi se va solicita să alegeți o anumită acțiune, prin intermediul unei ferestre de alertă, ori de câte ori o aplicație necunoscută încearcă să se conecteze la internet.

Aceste ferestre pop-up pot fi foarte utile pentru detectarea încercărilor de pătrundere în sistem a programelor sau persoanele rău intenționate, protejându-vă astfel împotriva amenințărilor din rețea.

Alerte carantină
Alertele de carantină vă informează atunci când au fost șterse fișiere vechi din carantină.

Alerte Control parental
De fiecare dată când Controlul parental blochează o activitate, este afișată o alertă care va informa utilizatorul de ce activitatea este blocată (de exemplu, o pagină web de alertă este afișată în locul unei pagini web blocate).

Alerte pop-up pentru înregistrare
Alertele pop-up de înregistrare sunt utilizate pentru a vă reaminti că trebuie să vă înregistrați produsul BitDefender sau pentru a vă informa că se apropie termenul de expirare a seriei de înregistrare sau că aceasta a expirat deja.

11.3. Setări generale

În această zonă, puteți activa sau dezactiva setările care afectează comportamentul produsului și interacțiunea cu utilizatorul.Pentru a activa sau dezactiva o setare, utilizați selectorul corespunzător.

Acestea sunt setările disponibile:

Modul pentru jocuri
Modul pentru jocuri modifică temporar setările de protecție pentru a minimiza impactul acestora asupra performanței sistemului atunci când vă jucați pe calculator.

Detecție Mod laptop
Modul pentru laptop modifică temporar setările de protecție pentru a minimiza impactul acestora asupra duratei de funcționare a laptopului pe baterie.

Parolă setări
Pentru a împiedica alte persoane să modifice setările BitDefender, le puteți proteja cu o parolă.La activarea acestei opțiuni, vi se va solicita să configurați parola pentru setări. Introduceți parola dorită în ambele câmpuri și faceți clic pe **OK** pentru a o seta.

Știri BitDefender
Activând această opțiune, veți primi știri importante legate de companie, actualizări de produs sau noi amenințări de securitate de la BitDefender.

Alerte notificare produs

Activând această opțiune, veți primi alerte informative.

Bara de scanare

Bara de scanare este o fereastră mică, transparentă care indică progresul activității de scanare a BitDefender.

Trimite rapoarte virusi

Activând această opțiune, BitDefender va trimite rapoartele de scanare către Laboratorul BitDefender pentru analiză. Aceste rapoarte nu vor conține date confidențiale, cum ar fi numele dumneavoastră sau adresa IP și nu vor fi folosite în scop comercial.

Detecție epidemii virale

Activând această opțiune, BitDefender va trimite rapoarte privind potențiale epidemii virale către Laboratorul BitDefender pentru analiză. Aceste rapoarte nu vor conține date confidențiale, cum ar fi numele dumneavoastră sau adresa IP, și nu vor fi folosite în scop comercial.

11.4. Reconfigurarea profilului de utilizare

În timpul instalării, ați putut configura un profil de utilizare.Profilul de utilizare reflectă principalele activități desfășurate pe calculator. În funcție de profil, interfața produsului este organizată astfel încât să vă permită să accesați ușor sarcinile dumneavoastră favorite.

Pentru a reconfigura profilul de utilizare, faceți clic pe **Reconfigurează profil** și urmați pașii asistentului de configurare.Puteți naviga prin programul asistent cu ajutorul butoanelor **Înainte** și **Înapoi**.Pentru a părăsi asistentul, faceți clic pe **Anulează**.

1. **Alegeți modul de vizualizare**

   Selectați modul preferat de vizualizare a interfeței utilizatorului.

2. **Configurarea Instrumentelor mele**

   Dacă ați selectat Modul Novice sau Modul Intermediar de vizualizare, alegeți opțiunile pentru care ați dori să creați comenzi rapide pe tabloul de comandă.

3. **Configurarea setărilor**

   În cazul în care ați selectat Modul Expert de vizualizare, configurați setările BitDefender conform preferințelor dumneavoastră.Pentru a activa sau dezactiva o setare, utilizați selectorul corespunzător.

4. **Configurarea Controlului parental**

   Notă

   Acest pas apare numai dacă ați adăugat funcția Control parental în Instrumentele mele.

Puteți selecta una dintre cele trei opțiuni:

- **Setați Controlul parental pentru conturile copiilor**

  Selectați această opțiune pentru a activa funcția de Control parental pentru conturile Windows create pentru copiii dumneavoastră și pentru a o gestiona din contul de administrator.

- **Setați Controlul parental pentru contul actual**

  Selectați această opțiune pentru a activa funcția de Control parental pentru contul Windows curent. Aceasta înseamnă că nu trebuie să creați conturi separate pentru copiii dumneavoastră, însă regulile privind Controlul parental vor afecta orice persoană care utilizează acest cont.

  În acest caz, este necesară o parolă pentru a proteja setările de Control parental.O puteți seta acum sau ulterior din fereastra BitDefender.

- **Omite deocamdată configurarea**

  Selectați această opțiune pentru a configura această caracteristică ulterior din fereastra BitDefender.

5. **Administrare rețea personală**

   Notă
   Acest pas apare numai dacă ați adăugat funcția Administrare rețea personală în Instrumentele mele.

   Puteți selecta una dintre cele trei opțiuni:

   - **Configurați acest calculator ca server**

     Selectați această opțiune dacă intenționați să gestionați produsele BitDefender instalate pe alte calculatoare din rețeaua personală de la acest calculator.

     Pentru a putea accesa rețeaua, este necesară o parolă.Introduceți parola în căsuțele de text puse la dispoziție și faceți clic pe **Trimite**.

   - **Configurați acest calculator drept client**

     Selectați această opțiune dacă BitDefender va fi administrat de la un alt calculator din cadrul rețelei personale pe care rulează de asemenea BitDefender.

     Pentru a putea accesa rețeaua, este necesară o parolă.Introduceți parola în căsuțele de text puse la dispoziție și faceți clic pe **Trimite**.

   - **Omite deocamdată configurarea**

     Selectați această opțiune pentru a configura această caracteristică ulterior din fereastra BitDefender.

6. **Configurare finalizată**

   Faceți clic pe **Finalizare**.

12. Istoric și evenimente

Linkul **Jurnale**, situat în partea de jos a ferestrei BitDefender, deschide o nouă fereastră care conține istoricul și evenimentele BitDefender. Această fereastră vă furnizează un rezumat al evenimentelor legate de securitate.De exemplu, puteți verifica rapid dacă produsul a fost actualizat, dacă au fost detectate coduri sau aplicații periculoase pe calculatorul dumneavoastră etc.

Pentru a gestiona mai ușor istoricul și evenimentele BitDefender, următoarele categorii sunt oferite în partea stângă:

- **Stare**
- **Antivirus**
- **Antispam**
- **Control parental**
- **Control date**
- **Firewall**
- **Vulnerabilitate**
- **Criptare chat**
- **Mod jocuri/laptop**
- **Rețea personală**
- **Actualizare**
- **Înregistrare**

Pentru fiecare categorie este disponibilă o listă de evenimente. Următoarele informații sunt furnizate pentru fiecare eveniment: o scurtă descriere, acțiunea luată de BitDefender atunci când evenimentul a avut loc și data și timpul când a avut loc. Dacă doriți mai multe informații în legătură cu un anumit eveniment din listă, faceți dublu-clic pe evenimentul respectiv.

Aici puteți accesa de asemenea informații detaliate și statistici legate de evenimentele funcției de Control parental, cum ar fi site-urile web accesate sau aplicațiile utilizate de copiii dumneavoastră.

Faceți clic pe **Șterge jurnalele** dacă doriți să ștergeți înregistrările vechi sau pe **Actualizează** pentru a vă asigura că sunt afișate și cele mai recente înregistrări.

13. Înregistrare și Contul meu

Procedura de înregistrare cuprinde două etape:

1. **Activarea produsului (înregistrarea unui cont BitDefender).** Trebuie să creați un cont BitDefender pentru ca produsul să se actualizeze și pentru a avea acces la suport tehnic gratuit.Dacă aveți deja un cont BitDefender, trebuie să vă înregistrați produsul BitDefender pe acel cont.BitDefender vă va înștiința că trebuie să vă activați produsul și vă va ajuta să remediați această problemă.

   Important

   Trebuie să vă creați un cont în 15 zile de la instalarea BitDefender.În caz contrar, BitDefender nu se va mai actualiza.

2. **Înregistrarea cu o serie de înregistrare.** Seria de înregistrare precizează pentru cât timp aveți dreptul de a utiliza produsul.Imediat după expirarea seriei de înregistrare, BitDefender se va opri din funcționare și nu vă va mai proteja calculatorul.Este recomandat să achiziționați o serie de înregistrare sau să vă reînnoiți licența cu câteva zile înainte de expirarea seriei actuale de înregistrare.

Dacă ați achiziționat BitDefender Internet Security 2011 pe un CD/DVD sau online, vi s-a solicitat să vă înregistrați produsul cu o serie de înregistrare în timpul instalării.

Dacă descărcați BitDefender Internet Security 2011 pentru evaluare, trebuie să vă înregistrați produsul cu o serie de înregistrare pentru a-l putea utiliza în continuare după expirarea perioadei de evaluare de 30 de zile. În perioada de evaluare, produsul este complet funcțional și îl puteți testa pentru a vedea dacă este în conformitate cu așteptările dumneavoastră.

13.1. Înregistrarea BitDefender Internet Security 2011

Dacă doriți să înregistrați produsul cu o serie de înregistrare sau să schimbați seria de înregistrare actuală, faceți clic pe linkul **Informații licență**, situat în partea de jos a ferestrei BitDefender.Va apărea fereastra de înregistrare a produsului.

Puteți vedea starea înregistrării produsului dumneavoastră BitDefender, seria actuală de înregistrare și câte zile au mai rămas până la expirarea licenței.

Pentru a înregistra BitDefender Internet Security 2011:

1. Introduceți seria de înregistrare în câmpul editabil.

   Notă

   Puteți găsi seria dumneavoastră de înregistrare:
   - pe eticheta de pe CD.
   - pe certificatul de înregistrare al produsului.
   - în e-mailul de achiziționare online.

Dacă nu aveți o serie de înregistrare BitDefender, faceți clic pe linkul furnizat pentru a porni programul asistent care vă va ajuta să cumpărați una.

2. Faceți clic pe **Înregistrare**.
3. Faceți clic pe **Finalizare**.

13.2. Activarea BitDefender

Pentru a activa BitDefender, trebuie să creați sau să accesați un cont BitDefender.Dacă nu ați înregistrat un cont BitDefender în cursul programului asistent de instalare, aveți următoarele alternative:

Modul Novice
: Faceți clic pe **Afișează toate problemele**.Asistentul vă va ajuta să remediați toate problemele curente, inclusiv activarea produsului.

Modul Intermediar
: Mergeți la fila **Securitate** și faceți clic pe butonul **Remediază** corespunzător problemei referitoare la actualizarea produsului.Faceți clic pe **Start** în fereastra asistentului pentru a activa produsul.

Modul Expert
: Mergeți la **Înregistrare** și faceți clic pe butonul **Activare produs**.

Se va deschide fereastra de înregistrare a contului.Aici puteți crea sau vă puteți conecta la un cont BitDefender pentru a vă activa produsul.

Dacă nu doriți să creați un cont BitDefender în acest moment, selectați **Creează un cont mai târziu** și faceți clic pe **Finalizare**.Altfel, continuați în funcție de situația dumneavoastră actuală:

- „Nu am un cont BitDefender” (p. 53).
- „Deja am un cont BitDefender” (p. 54).

Important

Trebuie să vă creați un cont în 15 zile de la instalarea BitDefender.În caz contrar, BitDefender nu se va mai actualiza.

Nu am un cont BitDefender

Pentru a crea un cont BitDefender, urmați acești pași:

1. Selectați **Creează un cont nou**.
2. Introduceți informațiile solicitate în câmpurile corespunzătoare.Informațiile furnizate aici vor rămâne confidențiale.
   - **Nume de utilizator** - introduceți adresa dumneavoastră de e-mail.

- **Parolă** - introduceți o parolă pentru contul dumneavoastră BitDefender.Parola trebuie să conțină între 6 și 16 caractere.
- **Confirmați parola** - introduceți din nou parola specificată anterior.

  Nu trebuie să reintroduceți parola dacă ați ales ca aceasta să nu fie mascată în timpul tastării.
- **Indiciu privind parola** - introduceți un cuvânt sau o expresie care vă va ajuta să vă reamintiți parola în cazul în care ați uitat-o.

Notă
După activarea contului, puteți folosi adresa de e-mail și parola furnizate pentru a-l accesa, la adresa http://myaccount.bitdefender.com.

3. Opțional, BitDefender vă poate informa despre oferte speciale și promoții folosind adresa de e-mail a contului dumneavoastră.Faceți clic pe **Vizualizare opțiuni contacte** și selectați una dintre opțiunile disponibile din fereastra care apare.
   - **Vreau sa primesc toate mesajele**
   - **Trimite-mi mesajele importante**
   - **Nu vreau sa primesc niciun mesaj**
4. Faceți clic pe **Trimite**.
5. Faceți clic pe **Finalizare** pentru a închide fereastra.

Notă
Pentru a vă putea utiliza contul, trebuie mai întâi să îl activați.
Verificați-vă adresa de e-mail și urmați instrucțiunile din mesajul trimis de către serviciul de înregistrare BitDefender.

Deja am un cont BitDefender

BitDefender va detecta automat dacă ați creat anterior un cont BitDefender pe calculatorul dumneavoastră.În acest caz, furnizați parola contului dumneavoastră și faceți clic pe **Trimite**.Faceți clic pe **Finalizare** pentru a închide fereastra.

Dacă aveți deja un cont activ, dar BitDefender nu-l detectează, urmați pașii de mai jos pentru a înregistra produsul cu contul respectiv:

1. Selectați **Autentificare(cont anterior)**.
2. Introduceți adresa de e-mail și parola contului dvs în câmpurile corespunzătoare.

Notă
Dacă v-ați uitat parola, faceți clic pe **V-ați uitat parola?** și urmați instrucțiunile.

3. Opțional, BitDefender vă poate informa despre oferte speciale și promoții folosind adresa de e-mail a contului dumneavoastră.Faceți clic pe **Vizualizare opțiuni contacte** și selectați una dintre opțiunile disponibile din fereastra care apare.
   - **Vreau sa primesc toate mesajele**
   - **Trimite-mi mesajele importante**
   - **Nu vreau sa primesc niciun mesaj**
4. Faceți clic pe **Trimite**.
5. Faceți clic pe **Finalizare** pentru a închide fereastra.

13.3. Achiziționarea sau reînnoirea unei serii de înregistrare

Dacă perioada de evaluare se va încheia în curând, trebuie să achiziționați o serie de înregistrare și să vă înregistrați produsul.

În mod similar, dacă seria de înregistrare actuală va expira în curând, trebuie să vă reînnoiți licența.La reînnoirea licenței, clienții BitDefender beneficiază de o reducere. În plus, este posibilă actualizarea produsului BitDefender la versiunea curentă beneficiind de o altă reducere sau chiar gratuit.

Pentru a începe o procedură simplă și sigură în patru pași care vă va permite să achiziționați o nouă serie de înregistrare sau să o reînnoiți pe cea existentă, deschideți BitDefender în Modul Intermediar sau Modul Expert și faceți clic pe linkul **Achiziționare** / **Reînnoire** din partea inferioară a ferestrei.

Configurare și administrare

14. Setări generale

Modulul General furnizează informații despre activitatea BitDefender și despre sistem.De asemenea, aici puteți seta comportamentul general al BitDefender.

Pentru configurarea setărilor generale:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **General > Setări**.

- **Activează protecția prin parolă pentru setările produsului** - permite setarea unei parole pentru a proteja configurația BitDefender.

  Notă
  Dacă nu sunteți singura persoană cu drepturi administrative care folosește acest calculator, este recomandat să vă protejați setările BitDefender cu o parolă.

  Introduceți parola în câmpul **Parolă**, reintroduceți-o în câmpul **Confirmați parola** și faceți clic pe **OK**.

  După ce ați setat parola, vi se va cere să o introduceți ori de câte ori doriți să modificați setările BitDefender.De asemenea, ceilalți administratori de sistem (dacă există) vor trebui să furnizeze această parolă pentru a schimba setările BitDefender.

  Dacă doriți ca parola să fie solicitată doar la configurarea Controlului parental, trebuie să selectați de asemenea **Aplică protecția pe bază de parolă exclusiv setărilor de control parental**.Pe de altă parte, dacă parola a fost configurată doar pentru Controlul parental și debifați această opțiune, parola respectivă va fi cerută la configurarea oricărei opțiuni BitDefender.

  Important
  Dacă uitați parola va fi nevoie să reparați produsul pentru a schimba configurarea BitDefender.

- **Solicită configurarea parolei la activarea Controlului parental** - vă solicită să configurați parola atunci când doriți să activați Controlul parental, dacă aceasta nu este configurată.Setând parola, veți împiedica alți utilizatori cu drepturi administrative pe sistem să modifice setările de Control parental pe care le-ați configurat pentru un anumit utilizator.
- **Afișează știri BitDefender (avertizări de securitate)** - afișează din când în când notificări de securitate referitoare la noi viruși descoperiți, trimise de serverul BitDefender.
- **Afișează ferestre pop-up (note pe ecran)** - afișează ferestre de informare cu privire la starea produsului.Puteți configura BitDefender să afișeze ferestre pop-up

numai atunci când interfața este în Modul Novice / Intermediar sau în Modul Expert.

- **Afișează bara de scanare (graficul de pe ecran al activității produsului)** - afișează bara de scanare atunci când vă conectați la Windows.Debifați această căsuță dacă nu doriți ca bara de scanare să mai fie afișată.

Notă

Această opțiune poate fi configurată doar pentru contul de utilizator Windows curent.Bara de scanare este disponibilă numai atunci când interfața se află în Modul Expert de vizualizare.

Setări raportare viruși

- **Trimite rapoarte virusi** - trimite Laboratorului BitDefender rapoarte referitoare la virușii identificați în calculatorul dumneavoastră. Astfel ne ajutați să ținem evidența noilor viruși.

  Rapoartele nu conțin date confidențiale, precum numele dumneavoastră, adresa IP sau altele, și nu vor fi folosite în scopuri comerciale. Informațiile trimise vor conține doar numele virușilor și vor fi folosite doar pentru a crea rapoarte statistice.

- **Activează Detecția epidemiilor virale de către BitDefender** - trimite Laboratorului BitDefender rapoarte referitoare la potențiale epidemii virale.

  Rapoartele nu conțin date confidențiale, precum numele dumneavoastră, adresa IP sau altele, și nu vor fi folosite în scopuri comerciale. Informațiile trimise vor conține doar potențialul virus și vor fi folosite doar pentru a detecta noi viruși.

Setări conexiune

Mai multe componente BitDefender (modulele de firewall, actualizare, raportare viruși și spam în timp real) necesită acces la internet. BitDefender este prevăzut cu un proxy manager care asigură configurarea dintr-un anumit loc a setărilor proxy utilizate de componentele BitDefender pentru a obține acces la internet.

În cazul în care compania utilizează un server proxy pentru conectarea la Internet, trebuie să specificați setările proxy pentru ca BitDefender să se poată actualiza. Altfel, BitDefender va utiliza setările proxy ale administratorului care a instalat produsul sau ale browserului implicit al utilizatorului curent, dacă acestea există.Pentru mai multe informații, consultați *„Cum aflu care sunt setările mele proxy?”* (p. 208).

Notă

Setările proxy pot fi configurate doar de utilizatori cu drepturi administrative pe calculator sau de către utilizatori care cunosc parola produsului.

Pentru administrarea setărilor proxy, faceți clic pe **Setări proxy**.

Există trei seturi de setări proxy:

- **Proxy detectat la momentul instalării** - setări proxy detectate pe contul administratorului în timpul instalării și care pot fi configurate doar dacă sunteți conectat la acel cont. Dacă serverul proxy necesită un nume de utilizator și o parolă pentru autentificare, atunci va trebui să le specificați în câmpurile corespunzătoare.
- **Proxy browser implicit** - setări proxy ale utilizatorului curent, extrase din browserul implicit. Dacă serverul proxy solicită un nume de utilizator și o parolă pentru autentificare, specificați-le în câmpurile corespunzătoare.

  Notă

  Browserele web suportate sunt Internet Explorer, Mozilla Firefox și Opera. Dacă utilizați un alt browser în mod implicit, BitDefender nu va putea obține setările proxy ale utilizatorului curent.

- **Proxy personalizat** - setări proxy pe care le puteți configura dacă sunteți autentificat ca administrator.

  Următoarele setări trebuie specificate:
  - **Adresă** - introduceți adresa IP a serverului proxy.
  - **Port** - introduceți portul folosit BitDefender pentru a se conecta la serverul proxy.
  - **Utilizator** - introduceți un nume de utilizator recunoscut de proxy.
  - **Parolă** - introduceți o parolă validă pentru numele de utilizator introdus.

BitDefender va utiliza seturile de setări proxy în următoarea ordine până ce reușește să se conecteze la internet:

1. setările proxy specificate.
2. setările proxy detectate la momentul instalării.
3. setările proxy ale utilizatorului actual.

Atunci când BitDefender va încerca să se conecteze la Internet, va fi încercat pe rând fiecare set de setări proxy, până când se va reuși conexiunea.

Mai întâi, va fi utilizat setul conținând propriile dumneavoastre setări proxy pentru conectarea la Internet. Dacă acesta nu merge, vor fi încercate în continuare setările proxy detectate la instalare. În sfârșit, dacă nici acestea nu sunt bune, vor fi extrase setările proxy ale utilizatorului curent din browserul implicit și vor fi folosite pentru conectarea la Internet.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Faceți clic pe **Aplică** pentru a salva schimbările sau pe **Implicit** pentru a încărca setările standard.

Informații sistem

BitDefender vă permite să vedeți, dintr-un singur loc, toate setările de sistem și aplicațiile înregistrate să ruleze la pornirea sistemului. Astfel, puteți monitoriza activitatea sistemului și a aplicațiilor instalate pe acesta și identifica posibile infectări ale sistemului.

Pentru a obține informații despre sistem:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **General > Informații sistem**.

Lista conține toate obiectele încărcate la pornirea sistemului precum și obiectele încărcate de diverse aplicații.

Sunt disponibile trei butoane:

- **Restaurează** - modifică o asociere de fișiere curentă cu asocierea de fișiere implicită.Disponibil doar pentru setările **Asocieri de fișiere**!
- **Mergi la** - deschide o fereastră unde obiectul selectat este plasat (de exemplu, **Regiștrii**).

  Notă
  În funcție de elementul selectat, este posibil ca butonul **Mergi la** să nu apară.

- **Actualizează** - redeschide secțiunea **Informații sistem**.

15. Protecție antivirus

BitDefender vă protejează calculatorul împotriva oricăror amenințări malware (viruși, troieni, aplicații spyware, rootkituri și altele).Protecția oferită de BitDefender se împarte în două categorii:

- Protecția în timp real - previne pătrunderea noilor amenințări malware în sistemul dumneavoastră.BitDefender va scana, de exemplu, un document Word atunci când îl deschideți și un mesaj e-mail atunci când îl primiți.

  Protecția în timp real mai este denumită și scanare la acces - fișierele sunt scanate în timp ce utilizatorii le accesează.

  Important
  Pentru a preveni infectarea calculatorului personal cu viruși, păstrați **Protecția în timp real** activată.

- Scanarea la cerere - permite detectarea și eliminarea virușilor și a altor coduri periculoase care există deja în sistemul dumneavoastră.Acesta este modul clasic de scanare, inițiată de utilizator – dumneavoastră alegeți partițiile, directoarele sau fișierele pe care trebuie să le scaneze BitDefender, iar BitDefender le scanează – la cerere.Sarcinile de scanare permit crearea unor rutine de scanare personalizate și pot fi programate să ruleze periodic.

Atunci când detectează un virus sau un alt cod periculos, BitDefender va încerca în mod automat să elimine codul periculos din fișierul infectat și să reconstruiască fișierul original.Această operațiune este denumită dezinfectare.Fișierele care nu pot fi dezinfectate sunt mutate în carantină pentru a preveni infectarea altor fișiere.Pentru mai multe informații, consultați *„Zona de carantină”* (p. 83).

În cazul în care calculatorul dumneavoastră a fost infectat cu malware, consultați *„Eliminarea virușilor din sistem”* (p. 191).

Utilizatorii avansați pot configura excepțiile de la scanare în cazul în care nu doresc ca anumite fișiere să fie scanate.Pentru mai multe informații, consultați *„Configurarea excepțiilor de scanare”* (p. 80).

15.1. Protecție în timp real

BitDefender oferă protecție continuă în timp real împotriva unui număr mare de amenințări malware scanând toate fișierele accesate, mesajele e-mail și comunicațiile prin programe de mesagerie instant (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

Setările implicite de protecție în timp real asigură o bună protecție împotriva malware cu un impact minor asupra performanțelor sistemului.Puteți modifica ușor setările de protecție în timp real în funcție de dorințele dumneavoastră prin comutarea la

unul dintre nivelurile de protecție predefinite.Sau, dacă sunteți un utilizator experimentat, puteți configura setările de scanare în detaliu prin crearea unui nivel de protecție personalizat.

Pentru a afla mai multe, consultați aceste subiecte:

- *„Reglarea nivelului de protecție în timp real”* (p. 62)
- *„Crearea unui nivel de protecție personalizat”* (p. 63)
- *„Modificarea acțiunilor aplicate fișierelor detectate”* (p. 64)
- *„Restaurarea setărilor implicite”* (p. 65)

Pentru a vă proteja împotriva unor aplicații rău intenționate necunoscute, BitDefender utilizează o tehnologie avansată euristică (Active Virus Control) și un sistem de detectare a intruziunilor, care monitorizează în permanență sistemul dumneavoastră.Pentru a afla mai multe, consultați aceste subiecte:

- *„Configurarea setărilor Active Virus Control”* (p. 66)
- *„Configurarea sistemului de detectare a intruziunilor”* (p. 68)

15.1.1. Reglarea nivelului de protecție în timp real

Nivelul de protecție în timp real definește setările de scanare pentru acest tip de protecție.Puteți modifica ușor setările de protecție în timp real în funcție de dorințele dumneavoastră prin comutarea la unul dintre nivelurile de protecție predefinite.

Pentru a regla nivelul de protecție în timp real:

1. Deschideți BitDefender.
2. În funcție de modul de vizualizare a interfeței, procedați după cum urmează:

   Modul Intermediar
   Mergeți la fila **Securitate** și faceți clic pe **Configurare antivirus** în zona de Sarcini rapide din partea stângă a ferestrei.

   Mergeți la fila **Scut**.

   Modul Expert
   Mergeți la **Antivirus > Scut**.

   Notă
   În Modul Novice și Modul Intermediar de vizualizare, puteți configura o comandă rapidă pentru a putea accesa aceste setări din pagina de stare.Pentru mai multe informații, consultați *„Instrumentele mele”* (p. 33).

3. Trageți de cursor de-a lungul scalei pentru a seta nivelul de protecție dorit.Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul de protecție care se potrivește mai bine nevoilor dumneavoastră de securitate.

15.1.2. Crearea unui nivel de protecție personalizat

Utilizatorii avansați pot folosi și modifica opțiunile de scanare oferite de BitDefender în beneficiul lor. Motorul de scanare poate fi setat să scaneze doar anumite extensii de fișiere, să caute anumite tipuri de amenințări malware sau să nu scaneze arhivele. Aceasta poate reduce cu mult timpul de scanare, precum și viteza de reacție a sistemului pe durata scanării.

Puteți configura setările protecției în timp real în detaliu prin crearea unui nivel de protecție personalizat.Pentru a crea un nivel de protecție personalizat:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus > Scut**.
3. Faceți clic pe **Nivel personalizat**.
4. Configurați setările de scanare după cum este nevoie.Pentru a afla ce face o opțiune, țineți cursorul mouse-ului deasupra ei și citiți descrierea afișată în partea de jos a ferestrei.
5. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Aceste informații vă pot fi de folos:

- Dacă nu sunteți familiarizat cu anumiți termeni, verificați-i în glosar.De asemenea, puteți găsi informații utile pe Internet.
- **Scanează fișiere accesate.** Puteți seta BitDefender să scaneze toate tipurile de fișiere accesate, numai aplicații (fișiere de programe) sau tipuri specifice de fișiere pe care le considerați periculoase.Scanarea tuturor fișierelor accesate asigură cea mai bună protecție, în timp ce scanarea exclusivă a aplicațiilor poate fi utilizată pentru asigurarea unei performanțe ridicate a sistemului.

  Aplicațiile (sau fișierele de program) sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere.Această categorie include următoarele extensii de fișiere:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Dacă optați pentru **Scanarea extensiilor definite de utilizator**, se recomandă să includeți toate extensiile aplicațiilor pe lângă celelalte extensii ale fișierelor pe care le considerați periculoase.
- **Scanează numai fișiere noi sau modificate.** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.

- **Scanează în arhive.** Scanarea în interiorul arhivelor este un proces lent și care necesită multe resurse, nefiind recomandată, prin urmare, pentru protecția în timp real.Arhivele ce conțin fișiere infectate nu reprezintă o amenințare imediată la adresa securității sistemului dumneavoastră.Codurile periculoase (malware) vă pot afecta sistemul numai dacă fișierul infectat este extras din arhivă și este executat fără a avea activată protecția în timp real.

- **Optiuni de acțiune.** Dacă doriți să modificați acțiunile aplicate fișierelor detectate, verificați recomandările din *„Modificarea acțiunilor aplicate fișierelor detectate”* (p. 64).

- **Opțiuni de scanare pentru traficul e-mail, web și de mesagerie instant.** Pentru a împiedica descărcarea fișierelor infectate pe calculatorul dumneavoastră, BitDefender scanează automat următoarele puncte de intrare:
  - e-mailuri recepționate
  - trafic web
  - fișiere primite prin Yahoo! Messenger și Windows Live Messenger

  Scanarea traficului web poate încetini puțin navigarea pe internet, însă aceasta va bloca programele malware provenite de pe internet, inclusiv descărcările ascunse.

  Deși nu se recomandă, puteți dezactiva funcția de scanare antivirus a e-mailurilor, paginilor web sau a mesageriei instantant pentru a spori performanțele sistemului.Dacă dezactivați opțiunile de scanare corespunzătoare, e-mailurile și fișierele primite sau descărcate de pe internet nu vor fi scanate, permițând astfel fișierelor infectate să fie salvate pe calculatorul dumneavoastră.Aceasta nu reprezintă o amenințare majoră deoarece protecția în timp real va bloca programul malware atunci când fișierele infectate sunt accesate (deschise, mutate, copiate sau executate).

15.1.3. Modificarea acțiunilor aplicate fișierelor detectate

Fișierele detectate cu ajutorul protecției în timp real sunt grupate în două categorii:

- **Fișiere infectate.** Fișierele detectate ca fiind infectate se potrivesc unei semnături malware din baza de date cu semnături malware a BitDefender.În mod normal, BitDefender poate să elimine codul malware dintr-un fișier infectat și să reconstruiască fișierul original. Această operațiune este cunoscută sub denumirea de dezinfectare.

Notă

Semnăturile malware sunt fragmente de coduri extrase din mostre reale de malware. Acestea sunt utilizate de către programele antivirus pentru a realiza identificarea după model și detectarea programelor malware.
Baza de date cu semnături malware a BitDefender reprezintă o colecție de semnături malware actualizate în fiecare oră de către cercetătorii malware ai BitDefender.

- **Fișiere suspecte.** Fișierele sunt identificate ca fiind suspecte în urma analizei euristice.Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

În funcție de tipul de fișier detectat, următoarele acțiuni sunt aplicate în mod automat:

- În cazul în care este detectat un fișier infectat, BitDefender va încerca în mod automat să-l dezinfecteze.Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția.

Important
Pentru anumite tipuri de malware, dezinfectarea nu este posibilă deoarece fișierul detectat este în întregime periculos. În astfel de situații, fișierul infectat este șters de pe disc.

- Dacă este detectat un fișier suspect, accesul la respectivul fișier va fi respins în scopul prevenirii unei potențiale infecții.

Cu excepția cazului în care aveți un motiv temeinic, nu ar trebui să modificați acțiunile aplicate implicit fișierelor detectate.

Pentru a modifica acțiunile aplicate implicit fișierelor infectate sau suspecte detectate:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus > Scut**.
3. Faceți clic pe **Nivel personalizat**.
4. Configurați acțiunile care vor fi aplicate fiecărei categorii de fișiere detectate, după cum este cazul.Cea de-a doua acțiune este aplicată în cazul în care prima nu reușește (de exemplu dacă dezinfectarea nu este posibilă, fișierul infectat este mutat în carantină).

15.1.4. Restaurarea setărilor implicite

Setările implicite de protecție în timp real asigură o bună protecție împotriva malware cu un impact minor asupra performanțelor sistemului.

Pentru a restaura setările implicite pentru protecția în timp real:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus > Scut**.
3. Faceți clic pe **Nivel implicit**.

15.1.5. Configurarea setărilor Active Virus Control

Active Virus Control BitDefender detectează aplicațiile posibil rău intenționate pe baza comportamentului acestora.

Active Virus Control monitorizează încontinuu aplicațiile care rulează pe calculator, verificând dacă nu există acțiuni similare programelor malware. Fiecare dintre aceste acțiuni are un anumit punctaj, iar punctajul global este calculat pentru fiecare proces.Atunci când punctajul general al unui proces atinge un anumit prag stabilit, procesul este considerat a fi periculos. În funcție de setările programului, procesul este blocat în mod automat sau este posibil să vi se solicite să specificați acțiunea ce va fi realizată.

Modulul Active Virus Control poate fi configurat să vă alerteze și să vă solicite să acționați atunci când o aplicație încearcă să efectueze o acțiune cu potențial periculos.

Dacă aplicația detectată este cunoscută, faceți clic pe **Permite**.

Dacă doriți să închideți imediat aplicația, faceți clic pe **OK**.

Selectați căsuța **Reține acțiunea pentru această aplicație** înainte de a face selecția și BitDefender va aplica aceeași acțiune la detectarea ulterioară a aplicației.Regula creată astfel va fi afișată în fereastra de configurare a Active Virus Control.

Pentru a configura Active Virus Control:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus > Scut**.
3. Faceți clic pe **Setări avansate**.
4. Mergeți la fila **AVC**.
5. Selectați căsuța corespunzătoare pentru a activa Active Virus Control.
6. Trageți de cursor de-a lungul scalei pentru a seta nivelul de protecție dorit.Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul de protecție care se potrivește mai bine nevoilor dumneavoastră de securitate.

Reglarea nivelului de agresivitate

Pentru a configura nivelul de protecție al Active Virus Control:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus > Scut**.
3. Faceți clic pe **Setări avansate**.

4. Mergeți la fila **AVC**.
5. Trageți de cursor de-a lungul scalei pentru a seta nivelul de protecție dorit.Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul de protecție care se potrivește mai bine nevoilor dumneavoastră de securitate.

Configurarea răspunsului la programele rău intenționate

În cazul în care o aplicație are un comportament rău intenționat, vi se va solicita să alegeți acceptarea sau blocarea acesteia.

Pentru a configura răspunsul la programele rău intenționate:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus > Scut**.
3. Faceți clic pe **Setări avansate**.
4. Mergeți la fila **AVC**.
5. Dacă doriți să vi se solicite o acțiune atunci când Active Virus Control detectează o aplicație posibil rău intenționată, bifați căsuța **Alertează înainte de aplicarea unei acțiuni**.Pentru a bloca în mod automat o aplicație care are un comportament rău intenționat (fără afișarea unei ferestre de alertă), debifați această căsuță.

Administrarea aplicațiilor sigure/nesigure

Puteți adăuga aplicații cunoscute și în care aveți încredere pe lista de aplicații sigure. Aceste aplicații nu vor mai fi verificate de BitDefender Active Virus Control și li se va permite accesul în mod automat.

Pentru a gestiona aplicațiile care nu sunt monitorizate de către Active Virus Control:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus > Scut**.
3. Faceți clic pe **Setări avansate**.
4. Mergeți la fila **AVC**.
5. Faceți clic pe fila **Excluderi**.

Aplicațiile pentru care ați creat reguli apar în tabelul **Excluderi**.Pentru fiecare regulă, sunt afișate calea către aplicație și acțiunea pe care ați stabilit-o pentru aceasta (Permite sau Blochează).

Pentru a schimba acțiunea corespunzătoare unei aplicații, faceți clic pe acțiunea curentă și selectați acțiunea dorită din meniu.

Pentru administrarea listei, folosiți butoanele de deasupra tabelului:

- **Adăugare** - adăugați o nouă aplicație pe listă.
- **Eliminare** - eliminați o aplicație din listă.
- **Editează** - editați o regulă aferentă unei aplicații.

15.1.6. Configurarea sistemului de detectare a intruziunilor

Sistemul BitDefender de detectare a intruziunilor monitorizează activitățile din rețea și din sistem pentru detectarea operațiunilor rău intenționate și a încălcărilor politici.

Pentru a configura sistemul de detectare a intruziunilor:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus > Scut**.
3. Faceți clic pe **Setări avansate**.
4. Mergeți la fila **IDS**.
5. Bifați căsuța corespunzătoare pentru a activa Sistemul de detectare a intruziunilor.
6. Trageți de cursor de-a lungul scalei pentru a seta nivelul de agresivitate dorit.Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul de agresivitate care se potrivește mai bine nevoilor dumneavoastră de securitate.

15.2. Scanarea la cerere

Principalul obiectiv BitDefender este protejarea calculatorului dumneavoastră de viruși. Aceasta se face în primul rând nepermițând virușilor noi să pătrundă în sistem, prin scanarea mesajele e-mail și a fișierelor descărcate sau copiate pe calculator.

Există însă riscul ca un virus să fi fost în sistem înainte de instalarea BitDefender. Din acest motiv, este indicat să vă scanați calculatorul de viruși după instalarea BitDefender. Și este, de asemenea, recomandat să vă scanați sistemul periodic.

Scanarea la cerere se bazează pe sarcini de scanare. Sarcinile de scanare sunt cele care specifică opțiunile de scanare și obiectele care să fie scanate.Puteți scana calculatorul oricând doriți rulând sarcinile de scanare predefinite sau propriile dumneavoastră sarcini de scanare (sarcini definite de utilizator). De asemenea, puteți programa sarcinile să ruleze periodic sau când sistemul nu este utilizat, pentru a nu interfera cu munca dumneavoastră.Pentru instrucțiuni rapide, consultați aceste subiecte:

- *„Cum scanez fișiere și directoare?”* (p. 161)
- *„Cum creez o sarcină de scanare personalizată?”* (p. 164)
- *„Cum programez o scanare a calculatorului?”* (p. 166)

15.2.1. Scanarea fișierelor și directoarelor

Trebuie să scanați fișierele și directoarele ori de câte ori considerați că acestea pot fi infectate.Faceți clic-dreapta pe fișierul sau directorul care doriți să fie scanat și selectați opțiunea **Scanează cu BitDefender**.Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

Dacă doriți să scanați anumite locații de pe calculator, puteți configura și rula o sarcină de scanare personalizată.Pentru mai multe informații, consultați *„Cum creez o sarcină de scanare personalizată?”* (p. 164).

Pentru a vă scana sistemul sau o parte din el puteți rula sarcinile de scanare predefinite sau propriile sarcini de scanare.Pentru a rula o sarcină de scanare, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Novice
: Faceți clic pe butonul **Securitate** și alegeți una dintre sarcinile de scanare disponibile.

Modul Intermediar
: Accesați fila **Securitate**.Faceți clic pe **Scanare completă** în zona de Sarcini rapide din partea stângă și selectați una dintre sarcinile de scanare disponibile.

Modul Expert
: Mergeți la **Antivirus > Scanare viruși**.Pentru a rula o sarcină de scanare a sistemului sau una definită de utilizator, faceți clic pe butonul **Rulează sarcina** corespunzător.

Acestea sunt sarcinile implicite pe care le puteți utiliza pentru a vă scana calculatorul:

Scanare completă sistem
: Scanează întregul sistem, cu excepția arhivelor.În configurația implicită, se scanează după toate tipurile de aplicații periculoase, cu excepția celor de tip rootkit.

Quick Scan
: Scanarea rapidă utilizează o tehnologie de scanare "in-the-cloud" (online) pentru a detecta aplicațiile periculoase ce rulează pe sistemul dumneavoastră. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o fracțiune din resursele de sistem necesare pentru o scanare antivirus obișnuită.

Scanare profundă
: Scanează întregul sistem.În configurația implicită, se scanează după toate tipurile de aplicații periculoase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spion, adware, obiecte ascunse (rootkituri) și altele.

Înainte de a începe scanarea, este necesar să vă asigurați că BitDefender este la zi cu semnăturile malware. Scanarea calculatorului folosind semnături vechi poate

împiedica BitDefender să detecteze programele periculoase mai recente, descoperite după ultima actualizare efectuată.

Pentru ca BitDefender să facă o scanare completă, este necesar să închideți toate programele. Este important să închideți în primul rând clientul de e-mail (i.e. Outlook, Outlook Express sau Eudora).

Sugestii pentru scanare

Iată alte câteva sugestii pentru scanare pe care le-ați putea găsi utile:

- În funcție de dimensiunea hard-discului, scanarea completă a calculatorului (Scanare profundă de sistem sau Scanare de sistem) poate dura (până la o oră sau chiar mai mult).Prin urmare, este recomandat să efectuați astfel de scanări când nu aveți nevoie de calculator pentru mai mult timp (de exemplu, în timpul nopții).

  Puteți programa scanarea pentru a începe atunci când este convenabil.Nu uitați să lăsați calculatorul pornit.Pentru Windows Vista, asigurați-vă să nu fie calculatorul în modul de veghe (sleep mode) atunci când sarcina este programată să înceapă.

- Dacă descărcați în mod frecvent fișiere de pe internet într-un anumit director, creați o sarcină nouă de scanare și setați directorul respectiv ca locație de scanare.Programați sarcina să ruleze în fiecare zi sau mai des.

- Un anumit tip de programe periculoase modifică setările Windows pentru a fi lansate automat la pornirea sistemului.Pentru a vă proteja calculatorul împotriva unor astfel de programe periculoase, puteți programa sarcina **Scanare Auto-logon** să ruleze automat la pornirea sistemului.Vă rugăm să țineți cont că scanarea autologon poate afecta funcționarea sistemului pentru o scurtă perioadă de timp după pornire.

15.2.2. Programul asistent de scanare

Atunci când inițiați o scanare la cerere (de exemplu, faceți clic-dreapta pe un director și selectați **Scanează cu BitDefender**), va apărea programul asistent de scanare.Urmați programul asistent în trei pași pentru a realiza procesul de scanare.

Notă

Dacă asistentul de scanare nu apare, este posibil ca scanarea să fie configurată să ruleze discret, în fundal.Căutați iconița de scanare în curs în bara de sistem.Puteți face dublu-clic pe această iconiță pentru a deschide fereastra de scanare și a vedea evoluția scanării.

Pasul 1/3 - Scanare

BitDefender va începe scanarea obiectelor selectate.

Puteți vedea stadiul și statisticile scanării (viteza de scanare, timpul scurs de la începutul scanării, numărul obiectelor scanate / infectate / suspecte / ascunse și altele).

Așteptați ca BitDefender să finalizeze scanarea.

Notă
Procesul de scanare poate dura destul de mult, în funcție de complexitatea scanării.

Arhive protejate prin parolă. Atunci când este identificată o arhivă protejată prin parolă, în funcție de setările de scanare, este posibil să fiți rugat să introduceți parola.Arhivele protejate prin parolă nu pot fi scanate decât dacă furnizați parola.Următoarele opțiuni sunt disponibile:

- **Doresc să introduc parola pentru acest obiect.** Dacă doriți ca BitDefender să scaneze arhiva, selectați această opțiune și introduceți parola.Dacă nu cunoașteți parola, selectați una dintre celelalte opțiuni.
- **Nu vreau să introduc parola pentru acest obiect (nu scana acest obiect).** Selectând această opțiune, arhiva nu fi scanată.
- **Nu vreau să introduc parolă pentru niciun obiect (nu scana niciun obiect protejat prin parolă).** Selectați această opțiune dacă doriți să nu vi se mai solicite introducerea parolei pentru arhivele protejate prin parolă.BitDefender nu le va putea scana, dar va păstra o înregistrare în raportul de scanare.

Faceți clic pe **OK** pentru a continua scanarea.

Oprirea sau întreruperea temporară a scanării. Puteți opri scanarea oricând doriți făcând clic pe **Stop&Da**. Veți sări direct la ultimul pas al programului asistent.Pentru a opri temporar procesul de scanare, faceți clic pe **Întrerupe**. Va trebui să faceți clic pe **Reia** pentru a relua scanarea.

Pasul 2/3 - Selectați acțiunile

După ce scanarea a fost finalizată, va apărea o nouă fereastră, unde puteți vedea rezultatele scanării.

Dacă nu există amenințări nesoluționate, faceți clic pe **Continuă**.În caz contrar, trebuie să configurați noi acțiuni pentru a vă proteja sistemul de amenințările nesoluționate.

Obiectele infectate sunt afișate în grupuri, în funcție de codul malware cu care sunt infectate.Faceți clic pe linkul corespunzător unei amenințări pentru a afla mai multe informații despre obiectele infectate.

Puteți alege o acțiune globală care să fie luată asupra tuturor problemelor sau puteți alege acțiuni separate pentru fiecare grup de probleme.Una sau mai multe dintre opțiunile următoare pot apărea în meniu:

Nicio acțiune
Nu se va lua nicio acțiune asupra fișierelor detectate.După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.

Dezinfectează
Elimină codul periculos din fișierele infectate.

Șterge
Îndepărtează fișierele identificate de pe disc.

Mută în carantină
Mută fișierele detectate în carantină.Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.Pentru mai multe informații, consultați *„Zona de carantină”* (p. 83).

Redenumește
Redenumește fișierele ascunse adăugând extensia `.bd.ren` la numele acestora.Ca urmare, veți putea căuta și găsi astfel de fișiere pe calculatorul dumneavoastră, dacă există.

Aceste fișiere ascunse nu sunt fișierele pe care le ascundeți deliberat din Windows. Ele sunt fișiere ascunse cu ajutorul unor programe speciale, cunoscute sub numele de rootkituri.Rootkiturile nu sunt în sine programe periculoase. Totuși, ele sunt utilizate frecvent pentru a împiedica detectarea virușilor sau aplicațiilor spion de către programele antivirus obișnuite.

Faceți clic pe **Continuă** pentru a aplica acțiunile specificate.

Pasul 3/3 - Examinați rezultatele

Atunci când BitDefender a remediat toate problemele apărute, rezultatele scanării vor fi afișate într-o nouă fereastră.Dacă doriți informații complete cu privire la procesul de scanare, faceți clic pe **Afișează jurnal** pentru a vizualiza jurnalul de scanare.

Important
Dacă este necesar, reporniți sistemul pentru a finaliza procesul de curățare.

Faceți clic pe **Închide** pentru a închide fereastra.

BitDefender nu a putut remedia anumite probleme

În majoritatea cazurilor, BitDefender va dezinfecta fișierele infectate detectate sau le va izola.Cu toate acestea, există anumite probleme care nu pot fi rezolvate automat.Pentru mai multe informații și instrucțiuni privind modul de eliminare a programelor malware în mod manual, consultați *„Eliminarea virușilor din sistem”* (p. 191).

BitDefender a detectat fișiere suspecte

Fișierele suspecte sunt fișiere detectate în cadrul analizei euristice ca fiind posibil infectate cu malware a cărui semnătură nu a fost încă lansată.

Dacă au fost detectate fișiere suspecte în timpul scanării, vi se va cere să le trimiteți Laboratorului BitDefender.Faceți clic pe **OK** pentru a trimite aceste fișiere Laboratorului BitDefender spre a fi analizate.

15.2.3. Examinarea rapoartelor de scanare

De fiecare dată când realizați o scanare, se creează un raport de scanare.Raportul de scanare conține informații detaliate despre procesul de scanare înregistrat, cum ar fi opțiunile de scanare, locațiile scanate, amenințările găsite și acțiunile luate asupra acestor amenințări.

Puteți deschide raportul de scanare direct din programul asistent de scanare, după ce scanarea a luat sfârșit, apăsând **Afișează jurnal**.

Pentru a verifica rapoartele de scanare mai târziu:

1. Deschideți BitDefender.
2. Faceți clic pe linkul **Jurnale** din colțul dreapta jos al ferestrei.
3. Faceți clic pe **Antivirus** în meniul din stânga.
4. În secțiunea **Sarcini la cerere**, puteți verifica ce operațiuni de scanare au fost realizate recent.Faceți dublu-clic pe evenimentele din listă pentru a vedea mai multe detalii.Pentru a deschide raportul de scanare, faceți clic pe **Afișează raport scanare**.Raportul de scanare va fi deschis în browserul dumneavoastră implicit.

Pentru a șterge un jurnal, faceți clic-dreapta pe acesta și selectați **Șterge**.

15.2.4. Administrarea sarcinilor de scanare existente

BitDefender este dotat cu o serie de sarcini predefinite, care acoperă nevoile comune de securitate. Pe lângă acestea, puteți crea propriile dumneavoastră sarcini de scanare.Pentru mai multe informații, consultați *„Cum creez o sarcină de scanare personalizată?”* (p. 164).

Pentru a administra sarcinile de scanare existente:

1. Deschideți BitDefender.
2. În funcție de modul de vizualizare a interfeței, procedați după cum urmează:

   Modul Intermediar

   Mergeți la fila **Securitate** și faceți clic pe **Configurare antivirus** în zona de Sarcini rapide din partea stângă a ferestrei.

   Mergeți la fila **Scanare viruși**.

Modul Expert

Mergeți la **Antivirus > Scanare viruși**.

Notă

În Modul Novice și Modul Intermediar de vizualizare, puteți configura o comandă rapidă pentru a putea accesa aceste setări din pagina de stare.Pentru mai multe informații, consultați *„Instrumentele mele”* (p. 33).

Există trei categorii de sarcini de scanare:

- **Sarcini sistem** - conține lista sarcinilor implicite de sistem. Următoarele sarcini sunt disponibile:

  Scanare completă sistem

  Scanează întregul sistem, cu excepția arhivelor.În configurația implicită, se scanează după toate tipurile de aplicații periculoase, cu excepția celor de tip rootkit.

  Quick Scan

  Scanarea rapidă utilizează o tehnologie de scanare "in-the-cloud" (online) pentru a detecta aplicațiile periculoase ce rulează pe sistemul dumneavoastră. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o fracțiune din resursele de sistem necesare pentru o scanare antivirus obișnuită.

  Scanare automată la conectare

  Scanează obiectele executate atunci când un utilizator se conectează la Windows.În mod implicit, scanarea autologon este dezactivată.

  Dacă doriți să folosiți această sarcină, faceți clic-dreapta pe ea, selectați **Program** și stabiliți ca sarcina să fie rulată **la pornirea sistemului**.Puteți indica după cât timp de la pornirea sistemului să fie rulată sarcina (în minute).

  Scanare profundă

  Scanează întregul sistem.În configurația implicită, se scanează după toate tipurile de aplicații periculoase care amenință securitatea sistemului dumneavoastră, cum ar fi virușii, aplicațiile spion, adware, obiecte ascunse (rootkituri) și altele.

Notă

Deoarece sarcinile **Scanare profundă sistem** și **Scanare completă sistem** analizează întregul sistem, scanarea poate lua ceva timp. De aceea, vă recomandăm să rulați aceste sarcini cu prioritate scăzută sau, și mai bine, atunci când nu utilizați calculatorul.

- **Sarcini definite de utilizator** - conține sarcinile definite de utilizator.

O sarcină denumită `Documentele mele` este furnizată.Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` și `StartUp`. Astfel, veți asigura siguranța documentelor dumneavoastră, un spațiu de lucru sigur și rularea la pornirea sistemului a unor aplicații necompromise.

- **Sarcini diverse** - conține o listă de sarcini de scanare diverse. Aceste sarcini de scanare se referă la tipuri alternative de scanare ce nu pot fi rulate din această fereastră. Puteți doar să modificați setările acestora și să examinați rapoartele de scanare.Sunt disponibile urmatoarele sarcini:

  Scanare dispozitiv

  BitDefender poate detecta în mod automat conectarea la calculator a unui dispozitiv de stocare și-l poate scana.Utilizați această sarcină pentru a configura opțiunile funcției automate de detectare și scanare a dispozitivelor de stocare (CD-uri/DVD-uri, dispozitive de stocare USB sau unități de rețea mapate).

  Scanare contextuală

  Această sarcină este utilizată la scanarea prin intermediul meniului contextual al Windows sau folosind bara de scanare.Puteți modifica opțiunile de scanare pentru a răspunde mai bine nevoilor dumneavoastră.

Puteți administra sarcinile de scanare cu ajutorul butoanelor sau al meniului cu comenzi rapide.

Pentru a rula o sarcină de scanare a sistemului sau una definită de utilizator, faceți clic pe butonul **Rulează sarcina** corespunzător. Va apărea programul asistent de scanare care vă va ghida de-a lungul procesului de scanare.

Pentru a configura o anumită sarcină de scanare să ruleze automat, la un moment ulterior sau în mod regulat, faceți clic pe butonul **Program** corespunzător și configurați planificarea după cum este necesar.

Dacă nu mai aveți nevoie de una dintre sarcinile de scanare pe care le-ați creat (o sarcină definită de utilizator), o puteți șterge făcând clic pe butonul **Șterge** din dreapta acesteia.Nu puteți elimina sarcinile de sistem sau sarcinile diverse.

Fiecare sarcină de scanare are o fereastră de proprietăți în care puteți configura setările acesteia și vizualiza jurnalele de scanare.Pentru a accesa această fereastră, faceți clic pe butonul **Proprietăți** din stânga sarcinii (sau faceți clic-dreapta pe sarcină și apoi clic pe **Proprietăți**).

Pentru a afla mai multe, consultați aceste subiecte:

- *„Configurarea setărilor de scanare”* (p. 76)
- *„Setarea locației de scanare”* (p. 79)
- *„Planificarea sarcinilor de scanare”* (p. 79)

Utilizarea meniului contextual

Un meniu contextual este disponibil pentru fiecare sarcină. Faceți clic-dreapta pe o sarcină selectată pentru a-l deschide.

Pentru sarcinile de sistem și definite de utilizator, sunt disponibile următoarele comenzi în meniul de scurtături:

- **Scanează acum** - execută sarcina selectată, lansând o scanare imediată.
- **Căi** - deschide fereastra de **Proprietăți** la tabul Căi, unde puteți modifica ținta de scanare a sarcinii selectate.În cazul sarcinilor de sistem, această opțiune este înlocuită cu **Afișare căi scanare** deoarece puteți vedea numai locațiile scanate.
- **Program** - deschide fereastra de **Proprietăți** la tabul Programare, unde puteți programa sarcina selectată.
- **Jurnale** - deschide fereastra de **Proprietăți** la tabul Jurnale, unde puteți examina rapoartele generate la fiecare rulare a sarcinii selectate.
- **Clonează sarcina** - creează o copie a sarcinii selectate.Acest lucru este util atunci când creați noi sarcini, deoarece puteți modifica setările duplicatului unei sarcini.
- **Șterge** - șterge sarcina selectată.

  Notă

  Disponibil numai pentru sarcini create de utilizator. Nu puteți șterge o sarcină implicită.

- **Proprietăți** - deschide fereastra de **Proprietăți** la tabul Generalități, unde puteți modifica setările sarcinii selectate.

Datorită caracterului special al sarcinilor din categoria **Sarcini diverse**, numai opțiunile **Jurnale** și **Proprietăți** sunt disponibile în acest caz.

Configurarea setărilor de scanare

Pentru a configura opțiunile de scanare ale unei anumite sarcini de scanare, faceți clic-dreapta pe aceasta și selectați **Proprietăți**.

Puteți configura ușor opțiunile de scanare reglând nivelul de scanare. Mutați cursorul de-a lungul scalei pentru a seta nivelul de scanare dorit.Utilizați descrierea din partea dreaptă a scalei pentru a identifica nivelul de scanare care se potrivește mai bine nevoilor dumneavoastră.

De asemenea, puteți configura aceste opțiuni generale:

- **Rulează sarcina cu prioritate scăzută.** Reduce prioritatea procesului de scanare. Veți permite altor programe să ruleze cu o viteză superioară, dar timpul necesar pentru finalizarea scanării va crește.

- **Minimizează asistentul de scanare în bara de sistem.** Minimizează fereastra de scanare în bara de sistem. Faceți dublu-clic pe iconița BitDefender pentru a o deschide.
- Specificați acțiunea care trebuie luată în cazul în care nu sunt identificate niciun fel de amenințări.

Utilizatorii avansați pot folosi și modifica opțiunile de scanare oferite de BitDefender în beneficiul lor. Motorul de scanare poate fi setat să scaneze doar anumite extensii de fișiere, să caute anumite tipuri de amenințări malware sau să nu scaneze arhivele. Aceasta poate reduce cu mult timpul de scanare, precum și viteza de reacție a sistemului pe durata scanării.

Pentru a configura setările de scanare în detaliu:

1. Faceți clic pe **Personalizare**.
2. Configurați setările de scanare după cum este nevoie.Pentru a afla ce face o opțiune, țineți cursorul mouse-ului deasupra ei și citiți descrierea afișată în partea de jos a ferestrei.
3. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Aceste informații vă pot fi de folos:

- Dacă nu sunteți familiarizat cu anumiți termeni, verificați-i în glosar.De asemenea, puteți găsi informații utile pe Internet.
- **Nivel scanare.** Precizați tipurile de programe periculoase care doriți să fie căutate de BitDefender prin selectarea opțiunilor corespunzătoare.
- **Scanează fișiere.** Puteți seta BitDefender să scaneze toate tipurile de fișiere, numai aplicații (fișiere de programe) sau tipuri specifice de fișiere pe care le considerați periculoase.Scanarea tuturor fișierelor asigură cea mai bună protecție în timp ce scanarea aplicațiilor poate fi utilizată pentru efectuarea unei scanări mai rapide.

  Aplicațiile (sau fișierele de program) sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere.Această categorie include următoarele extensii de fișiere:`.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`; `.lnk`; `.pif`; `.prc`; `.url`; `.smm`; `.pdf`; `.msi`; `.ini`; `.csc`; `.cmd`; `.bas`; `.eml`; `.nws`.

  Dacă optați pentru **Scanarea extensiilor definite de utilizator**, se recomandă să includeți toate extensiile aplicațiilor pe lângă celelalte extensii ale fișierelor pe care le considerați periculoase.
- **Scanează numai fișiere noi sau modificate.** Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.

- **Scanează în arhive.** Arhivele ce conțin fișiere infectate nu reprezintă o amenințare imediată la adresa securității sistemului dumneavoastră.Codurile periculoase (malware) vă pot afecta sistemul numai dacă fișierul infectat este extras din arhivă și este executat fără a avea activată protecția în timp real.Cu toate acestea, se recomandă să utilizați această opțiune pentru a detecta și elimina orice amenințare potențială chiar dacă nu este o amenințare imediată.

  Notă
  Scanarea fișierelor arhivate crește timpul total necesar pentru scanare și necesită mai multe resurse de sistem.

- **Optiuni de acțiune.** Specificați acțiunile care vor fi aplicate fiecărei categorii de fișiere detectate, folosind opțiunile din această categorie.Există trei categorii de fișiere detectate:

  - **Fișiere infectate.** Fișierele detectate ca fiind infectate se potrivesc unei semnături malware din baza de date cu semnături malware a BitDefender.În mod normal, BitDefender poate să elimine codul malware dintr-un fișier infectat și să reconstruiască fișierul original. Această operațiune este cunoscută sub denumirea de dezinfectare.

    Notă
    Semnăturile malware sunt fragmente de coduri extrase din mostre reale de malware. Acestea sunt utilizate de către programele antivirus pentru a realiza identificarea după model și detectarea programelor malware.
    Baza de date cu semnături malware a BitDefender reprezintă o colecție de semnături malware actualizate în fiecare oră de către cercetătorii malware ai BitDefender.

  - **Fișiere suspecte.** Fișierele sunt identificate ca fiind suspecte în urma analizei euristice.Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

  - **Fișiere ascunse (rootkituri).** Aceste fișiere ascunse nu sunt fișierele pe care le ascundeți deliberat din Windows. Ele sunt fișiere ascunse cu ajutorul unor programe speciale, cunoscute sub numele de rootkituri.Rootkiturile nu sunt în sine programe periculoase. Totuși, ele sunt utilizate frecvent pentru a împiedica detectarea virușilor sau aplicațiilor spion de către programele antivirus obișnuite.

  Cu excepția cazului în care aveți un motiv temeinic, nu ar trebui să modificați acțiunile aplicate implicit fișierelor detectate.

  Pentru a stabili o nouă acțiune, faceți clic pe **Prima acțiune** curentă și selectați opțiunea dorită din meniu.Specificați o **A doua acțiune** care va fi aplicată dacă prima eșuează.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

Setarea locației de scanare

Nu puteți modifica ținta de scanare pentru sarcinile din categoria **Sarcini sistem**.Puteți doar să vedeți obiectele care vor fi scanate.Pentru a vedea ținta unei sarcini de scanare de sistem, faceți clic-dreapta pe sarcină și selectați **Afișare căi scanare**.

Pentru a stabili ținta unei anumite sarcini de scanare, faceți clic-dreapta pe sarcină și selectați **Căi**. Dacă sunteți deja în fereastra Proprietăți a sarcinii, selectați tabul **Căi**.

Puteți vedea lista partițiilor locale, de rețea și amovibile (unitatea floppy, CD/DVD), precum și fișierele și directoarele adăugate anterior, dacă există. Toate obiectele bifate vor fi scanate atunci când este rulată sarcina.

Următoarele butoane sunt disponibile:

- **Adaugă obiect(e)** - deschide o fereastră de explorare din care puteți selecta fișierele sau directoarele care doriți să fie scanate.

  Notă
  Puteți folosi drag & drop pentru a adăuga fișiere/directoare la listă.

- **Șterge obiect(e)** - șterge fișierele / directoarele care au fost selectate anterior din lista de obiecte de scanat.

În afară de aceste butoane, există o serie de opțiuni care vă permit să selectați rapid locațiile de scanare.

- **Discuri locale** - pentru scanarea partițiilor locale.
- **Partiții din rețea** - pentru scanarea tuturor partițiilor din rețea.
- **Unități detașabile** - pentru scanarea unităților mobile de disc (unitățile de CD-ROM și discheta).
- **Toate obiectele** - pentru scanarea tuturor partițiilor, indiferent dacă sunt locale sau de rețea, precum și a unităților detașabile.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

Planificarea sarcinilor de scanare

În cazul sarcinilor complexe, scanarea durează mai mult și este mai eficientă dacă închideți toate programele. Din acest motiv este bine să programați astfel de sarcini să ruleze atunci când nu utilizați sistemul.

Pentru a vizualiza sau modifica programul unei sarcini, faceți clic-drepata pe sarcină și selectați **Program**. Dacă sunteți deja în fereastra de Proprietăți a sarcinii, selectați tabul **Programare**.

Puteți vedea programul de rulare al sarcinii, dacă acesta există.

Când planificați o sarcină trebuie să alegeți una dintre următoarele opțiuni:

- **Nu** - lansează sarcina numai la cererea utilizatorului.
- **O singură dată** - sarcina este executată o singură dată, la un anumit moment. Specificați data și timpul lansării în execuție în câmpurile **Data începerii/Ora începerii**.
- **Periodic** - lansează scanarea periodic, la anumite intervale de timp (minute, ore, zile, săptămâni, luni), începând de la o dată și o oră precizate.
- **La pornirea sistemului** - sarcina este executată la numărul de minute specificat după ce un utilizator s-a conectat la Windows.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra. Pentru a executa sarcina faceți clic pe **Scanează**.

15.3. Configurarea excepțiilor de scanare

Este posibil ca uneori să fie nevoie să excludeți unele fișiere de la scanare. De exemplu, puteți exclude un fișier de test EICAR de la scanarea la acces sau fișiere `.avi` de la scanarea la cerere.

BitDefender permite excluderea obiectelor atât de la scanarea la acces, cât și de la scanarea la cerere. Această caracteristică este menită să reducă timpul de scanare și să evite orice fel de interferență cu munca dumneavostră.

Pot fi excluse de la scanare două tipuri de obiecte:

- **Căi** - fișierul sau directorul (incluzând toate obiectele conținute) indicat de o cale specificată va fi exclus de la scanare.
- **Extensii** - toate fișierele care au o anumită extensie vor fi excluse de la scanare, indiferent de localizarea acestora pe hard-disc.

Obiectele excluse de la scanarea la acces nu vor fi scanate, indiferent dacă acestea sunt accesate de către dumneavoastră sau de către o aplicație.

Notă

Excepțiile NU se vor aplica în cazul scanării contextuale.Scanarea contextuală este o metodă de scanare la cerere: faceți clic-dreapta pe fișierul sau directorul pe care doriți să-l scanați și selectați **Scanează cu BitDefender** .

15.3.1. Excluderea fișierelor sau directoarelor de la scanare

Pentru a exclude căi (locații) de la scanare:

1. Deschideți BitDefender.
2. În funcție de modul de vizualizare a interfeței, procedați după cum urmează:

   Modul Intermediar

   Mergeți la fila **Securitate** și faceți clic pe **Configurare antivirus** în zona de Sarcini rapide din partea stângă a ferestrei.

   Mergeți la tabul **Excluderi**.

   Modul Expert

   Mergeți la **Antivirus > Excluderi**.

   Notă

   În Modul Novice și Modul Intermediar de vizualizare, puteți configura o comandă rapidă pentru a putea accesa aceste setări din pagina de stare.Pentru mai multe informații, consultați *„Instrumentele mele”* (p. 33).

3. Bifați căsuța corespunzătoare pentru a activa excluderile.
4. Porniți asistentul de configurare după cum urmează:
   - Faceți clic-dreapta în tabelul Fișiere și directoare și selectați **Adaugă cale nouă**.
   - Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
5. Urmați programul asistent de configurare.Puteți naviga prin programul asistent cu ajutorul butoanelor **Înainte** și **Înapoi**.Pentru a părăsi asistentul, faceți clic pe **Anulează**.
   a. Selectați opțiunea de excludere a unei căi de la scanare.Acest pas apare numai atunci când porniți asistentul făcând clic pe butonul **Adaugă**.
   b. Pentru a preciza căile ce vor fi excluse de la scanare, utilizați una dintre următoarele metode:
      - Faceți clic pe **Caută**, selectați fișierul sau directorul care doriți să fie exclus de la scanare și faceți clic pe **Adaugă**.
      - Introduceți calea care doriți să fie exclusă de la scanare și faceți clic pe **Adaugă**.

      Căile vor apărea în tabel pe măsură ce le adăugați. Puteți adăuga oricâte căi doriți.
   c. Implicit, căile selectate sunt excluse atât de la scanarea la acces cât și de la scanarea la cerere. Pentru a alege când să fie aplicată excepția, faceți clic pe coloana din dreapta și selectați opțiunea dorită din listă.

d. Este recomandat să scanați fișierele din locațiile specificate pentru a vă asigura că acestea nu sunt infectate.Selectați căsuța pentru a scana aceste fișiere înainte de a le exclude de la scanare.

Faceți clic pe **Finalizează** pentru a adăuga excepțiile.

6. Faceți clic pe **Salvează** pentru a salva modificările.

15.3.2. Excluderea extensiilor de fișiere de la scanare

Pentru a exclude extensii de fișiere de la scanare:

1. Deschideți BitDefender.
2. În funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar

Mergeți la fila **Securitate** și faceți clic pe **Configurare antivirus** în zona de Sarcini rapide din partea stângă a ferestrei.

Mergeți la tabul **Excluderi**.

Modul Expert

Mergeți la **Antivirus > Excluderi**.

Notă

În Modul Novice și Modul Intermediar de vizualizare, puteți configura o comandă rapidă pentru a putea accesa aceste setări din pagina de stare.Pentru mai multe informații, consultați *„Instrumentele mele”* (p. 33).

3. Bifați căsuța corespunzătoare pentru a activa excluderile.
4. Porniți asistentul de configurare după cum urmează:
   - Faceți clic-dreapta în tabelul Extensii și selectați **Adaugă extensie nouă**.
   - Faceți clic pe butonul **Adaugă**, aflat în partea superioară a tabelului cu excepții.
5. Urmați programul asistent de configurare.Puteți naviga prin programul asistent cu ajutorul butoanelor **Înainte** și **Înapoi**.Pentru a părăsi asistentul, faceți clic pe **Anulează**.
   a. Selectați opțiunea de excludere a extensiilor de la scanare.Acest pas apare numai atunci când porniți asistentul făcând clic pe butonul **Adaugă**.
   b. Pentru a specifica extensiile ce vor fi excluse de la scanare, utilizați una dintre următoarele metode:
      - Selectați din meniu extensia care doriți să fie exclusă de la scanare și faceți clic pe **Adaugă**.

Notă
Meniul conține lista tuturor extensiilor înregistrate pe sistemul dumneavoastră. Atunci când selectați o extensie, îi puteți vedea descrierea, dacă aceasta există.

- Introduceți extensia care doriți să fie exclusă de la scanare și faceți clic pe **Adaugă**.

Extensiile vor apărea în tabel pe măsură ce le adăugați. Puteți adăuga oricâte extensii doriți.

c. Implicit, extensiile selectate sunt excluse atât de la scanarea la acces cât și de la scanarea la cerere. Pentru a schimba când să fie aplicată excepția, faceți clic pe coloana din dreapta și selectați opțiunea dorită din listă.

d. Este recomandat să scanați fișierele care au extensiile specificate pentru a vă asigura că acestea nu sunt infectate.

Faceți clic pe **Finalizează** pentru a adăuga excepțiile.

6. Faceți clic pe **Salvează** pentru a salva modificările.

15.3.3. Administrarea excepțiilor de scanare

Dacă excluderile de la scanare configurate nu mai sunt necesare, se recomandă să le ștergeți sau să dezactivați utilizarea lor.

Pentru a administra excepțiile de la scanare:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus > Excluderi**.

Pentru a șterge un obiect din listă, selectați-l și faceți clic pe butonul **Șterge**.

Pentru a edita un obiect din listă, selectați-l și faceți clic pe butonul **Editează**.Va apărea o nouă fereastră unde puteți schimba extensia sau calea care va fi exclusă, precum și tipul de scanare de la care acestea să fie excluse. Faceți modificările necesare și apoi faceți clic pe **OK**.

Notă
De asemenea, puteți face clic-dreapta pe un obiect și utiliza opțiunile meniului contextual pentru a-l edita sau șterge.

Pentru a dezactiva excluderile, debifați căsuța corespunzătoare.

15.4. Zona de carantină

BitDefender permite izolarea fișierelor infectate sau suspecte într-o zonă sigură, numită carantină. Izolând aceste fișiere în carantină, riscul răspândirii infectării

dispare, iar în plus, aveți posibilitatea să trimiteți aceste fișiere Laboratorului BitDefender pentru analiză aprofundată.

Notă
Atunci când sunt în carantină virușii sunt inofensivi, pentru că nu pot fi executați sau citiți.

În plus, BitDefender scanează fișierele din carantină după fiecare actualizare a semnăturilor malware.Fișierele curățate sunt mutate automat în locația lor originală.

Pentru vizualizarea și administrarea fișierelor aflate în carantină și configurarea setărilor carantinei:

1. Deschideți BitDefender.
2. În funcție de modul de vizualizare a interfeței, procedați după cum urmează:

   Modul Intermediar
   Mergeți la fila **Securitate** și faceți clic pe **Configurare antivirus** în zona de Sarcini rapide din partea stângă a ferestrei.

   Mergeți la fila **Carantină**.

   Modul Expert
   Mergeți la **Antivirus > Carantină**.

Notă
În Modul Novice și Modul Intermediar de vizualizare, puteți configura o comandă rapidă pentru a putea accesa aceste setări din pagina de stare.Pentru mai multe informații, consultați *„Instrumentele mele”* (p. 33).

Gestionarea fișierelor din carantină

Puteți trimite fișierele selectate la Laboratorul BitDefender pentru o analiză detaliată făcând clic pe **Trimite**.Implicit, BitDefender va trimite automat fișierele din carantină la fiecare 60 minute.

Pentru a șterge un fișier aflat în carantină, selectați-l și faceți clic pe butonul **Șterge**.

Dacă doriți să restaurați un fișier aflat în carantină în locația sa originală, selectați-l și faceți clic pe **Restaurează**.

Configurarea setărilor carantinei

Pentru a configura setările carantinei, faceți clic pe **Setări**.Utilizând setările carantinei, puteți seta BitDefender să execute automat următoarele acțiuni:

Șterge fișierele vechi. Pentru a șterge automat fișierele vechi din carantină, bifați opțiunea corespunzătoare.Trebuie să specificați numărul de zile după care fișierele din carantină ar trebui șterse și frecvența cu care BitDefender să caute fișiere vechi.

Trimite automat fișierele. Pentru a trimite automat fișierele din carantină, bifați opțiunea corespunzătoare.Trebuie să specificați frecvența cu care să fie trimise fișierele.

Scanează fișierele din carantină după actualizare. Pentru a scana automat fișierele aflate în carantină după fiecare actualizare, bifați opțiunea corespunzătoare.Puteți muta automat fișierele curățate în locația originală selectând **Restaurează fișiere curățate**.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

16. Protecție antiphishing

BitDefender Antiphishing împiedică dezvăluirea informațiilor personale în timp ce navigați pe Internet alertându-vă despre paginile web cu conținut potențial phishing.

BitDefender furnizează protecție antiphishing în timp real pentru:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

16.1. Configurarea listei albe antiphishing

Puteți configura și administra o listă albă de site-uri web care nu vor fi scanate de către motoarele antiphishing BitDefender.Este recomandat ca lista albă să conțină numai site-uri web în care aveți deplină încredere.De exemplu, adăugați site-urile web de unde cumpărați produse online.

Notă

Puteți adăuga ușor site-uri web pe lista albă utilizând bara de comenzi BitDefender Antiphishing integrată în browserul dumneavoastră.Pentru mai multe informații, consultați *„Administrarea protecției antiphishing BitDefender din Internet Explorer și Firefox”* (p. 86).

Pentru a configura și administra lista albă antiphishing:

- Dacă utilizați un browser compatibil, faceți clic pe bara de instrumente BitDefender și alegeți **Lista albă** din meniu.
- Alternativ, urmați acești pași:
  1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
  2. Mergeți la **Antivirus > Scut**.
  3. Faceți clic pe **Lista albă**.

Pentru a adăuga o pagină web pe lista albă, introduceți adresa acesteia în câmpul corespunzător și faceți clic pe **Adaugă**.

Pentru a șterge un site din lista albă, faceți clic pe butonul **Șterge** corespunzător.

Faceți clic pe **Salvează** pentru a salva modificările și închide fereastra.

16.2. Administrarea protecției antiphishing BitDefender din Internet Explorer și Firefox

BitDefender se integrează direct, printr-o bară de comenzi intuitivă și ușor de folosit, cu următoarele browsere web:

- Internet Explorer
- Mozilla Firefox

Puteți administra ușor și eficient protecția antiphishing și lista albă utilizând bara de comenzi BitDefender Antiphishing integrată în browserele web de mai sus.

Bara de comenzi antiphishing, reprezentată prin iconița BitDefender, se află în partea superioară a browserului.Faceți clic pe ea pentru a deschide meniul barei de instrumente.

Notă
Dacă nu puteți vedea bara de instrumente, deschideți meniul **View**, duceți cursorul pe **Toolbars** și bifați **BitDefender Toolbar**.

Următoarele comenzi sunt disponibile pe meniul barei de instrumente:

- **Activează / Dezactivează** - activează / dezactivează protecția antiphishing BitDefender în browserul web curent.
- **Setări** - deschide o fereastră în care puteți specifica setările barei de comenzi antiphishing.Următoarele opțiuni sunt disponibile:
  - **Protecția antiphishing pentru web în timp real** - detectează și vă avertizează în timp real dacă un site web este folosit pentru a fura informații personale.Această opțiune controlează protecția antiphishing oferită de BitDefender doar pentru browserul web curent.
  - **Întreabă înainte de a adăuga pe lista albă** - vă avertizează înainte de a adăuga o pagină web pe lista albă.
- **Adaugă pe lista albă** - adaugă pagina web curentă pe lista albă.

Important
Adăugarea unei pagini web pe lista albă înseamnă că BitDefender nu o va mai scana după amenințări phishing. Vă recomandăm să adăugați pe lista albă doar paginile web în care aveți deplină încredere.

- **Lista albă** - deschide lista albă.Pentru mai multe informații, consultați *„Configurarea listei albe antiphishing”* (p. 86).
- **Raportează ca tentativă de fraudare** - informează laboratorul BitDefender că site-ul web respectiv este folosit pentru furt de informații personale.Raportând site-urile web folosite pentru fraudă, ajutați la protejarea altor persoane împotriva furtului de identitate.
- **Ajutor** - deschide documentația electronică.
- **Despre** - deschide o fereastră în care puteți vedea informații despre BitDefender și unde puteți solicita asistență profesională în cazul unei probleme.

17. Consilier pentru căutare

Consilierul pentru căutare îmbunătățește protecția împotriva amenințărilor online, atenționându-vă în legătură cu paginile web cu conținut phishing sau nesigure direct din pagina cu rezultatele căutării.

Consilierul pentru căutare funcționează cu orice browser și verifică rezultatele căutării afișate de cele mai populare motoare de căutare:

- Google
- Yahoo!
- Bing

Consilierul pentru căutare indică dacă un anumit rezultat al căutării este sigur sau nu prin plasarea unei mici iconițe de stare în fața linkului.

Cerc verde cu bifă: Puteți accesa acest link în siguranță.

Cerc roșu cu semnul exclamării: Aceasta este o pagină web cu conținut phishing sau nesigură.Este recomandat să nu deschideți linkul.Dacă utilizați Internet Explorer sau Firefox și încercați să deschideți linkul, BitDefender va bloca în mod automat pagina web și va afișa în schimb o pagină de alertă.Dacă doriți să ignorați alerta și să accesați pagina web, urmați instrucțiunile de pe pagina de alertă.

17.1. Dezactivarea Consilierului pentru căutare

Pentru a dezactiva Consilierul pentru căutare:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul dreapta sus al ferestrei și alegeți **Preferințe**.
2. Mergeți la **Setări de securitate**.
3. Utilizați selectorul pentru a dezactiva Consilierul pentru căutare.

18. Antispam

Spam este un termen utilizat pentru a descrie un e-mail nesolicitat.Spamul este o problemă în creștere, atât pentru individ cât și pentru organizații. Nu este interesant, nu ați dori să fie văzut de către copii, puteți fi concediat din cauza lui (pentru pierdere de timp prin primirea de mesaje cu conținut sexual pe adresa de serviciu) și nu puteți împiedica trimiterea sa. Cel mai bun lucru pe care îl puteți face este, evident, să nu îl mai primiți. Din păcate, acesta există în cantități mari, într-o gamă largă de forme și mărimi.

BitDefender Antispam utlizează remarcabile inovații tehnologice și filtre antispam standard pentru a ține la distanță spamul de căsuțele de mesaje ale utilizatorilor.Pentru mai multe informații, consultați *„Detalii privind modulul Antispam”* (p. 89).

Protecția antispam BitDefender este disponibilă numai pentru clienții de e-mail configurați să primească mesaje e-mail prin protocolul POP3.POP3 este unul dintre cele mai des folosite protocoale de descărcare a mesajelor e-mail de pe un server de mail.

Notă
BitDefender nu asigură protecție antispam pentru conturile de e-mail pe care le accesați prin intermediul serviciilor de e-mail oferite pe internet.

Mesajele spam detectate de BitDefender sunt marcate cu prefixul `[spam]` în subiect.BitDefender mută în mod automat mesajele spam într-un anumit director, după cum urmează:

- În Microsoft Outlook, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Deleted Items**.Directorul **Spam** este creat în timpul instalării BitDefender.
- În Outlook Express și Windows Mail, mesajele spam sunt mutate direct în **Deleted Items**.
- În Mozilla Thunderbird, mesajele spam sunt mutate într-un director **Spam**, situat în directorul **Trash**.Directorul **Spam** este creat în timpul instalării BitDefender.

În cazul în care utilizați alți clienți de e-mail, trebuie să creați o regulă pentru a muta mesajele de e-mail marcate ca`[spam]`de către BitDefender într-un director de carantină personalizat.

18.1. Detalii privind modulul Antispam

18.1.1. Filtrele Antispam

Motorul BitDefender Antispam incorporează șapte filtre diferite care vă protejează directorul Inbox de Spam:Lista de prieteni, Lista de spammeri, Filtrul de caractere, Filtrul de imagini, Filtrul URL, Filtrul NeuNet(euristic) și Filtrul Bayesian.

Lista de prieteni / spammeri

Majoritatea oamenilor comunică în mod regulat cu un grup de cunoștințe sau chiar primesc mesaje de la companii sau organizații cu același domeniu de activitate. Folosind **listele de prieteni și spammeri** îi puteți clasifica ușor pe cei de la care doriți să primiți mesaje (prieteni), indiferent de conținut, sau cei de la care nu doriți să primiți nimic (spammeri).

Notă

Vă recomandăm să adăugați numele și adresele prietenilor la **lista de prieteni**.BitDefender nu va bloca mesajele de la cei de pe listă; deci adăugând prietenii vă veți asigura că mesajele legitime vor ajunge în Inbox.

Filtrul de caractere

Multe mesaje Spam sunt scrise cu caractere chirilice și / sau asiatice. Filtrul de caractere detectează acest tip de mesaje și le marchează ca SPAM.

Filtrul de imagini

Pentru că evitarea filtrului euristic a devenit o provocare, în ultima vreme, directoarele de mesaje recepționate sunt invadate de mesaje spam care includ numai o imagine atașată. Pentru rezolvarea acestei probleme crescânde, BitDefender a introdus **Filtrul de imagini**, care compară semnăturile imaginilor din mesaje cu cele dintr-o bază de date a BitDefender. Dacă se descoperă o imagine cu conținut spam mesajul va fi marcat ca SPAM.

Filtrul URL

Aproape toate mesajele spam conțin referințe (linkuri) la diverse pagini web. Aceste pagini conțin, de obicei, reclame și oferă posibilitatea de a cumpăra obiecte și, uneori, sunt folosite pentru tentative de phishing.

BitDefender menține o bază de date cu astfel de linkuri.Filtrul URL caută fiecare link URL dintr-un mesaj în baza sa de date. Dacă linkul este găsit, mesajul este marcat ca SPAM.

Filtrul Euristic

Filtrul NeuNet (euristic) verifică toate componentele unui mesaj, (nu doar antetul, ci și corpul mesajului în format HTML sau text), căutând cuvinte, fraze, linkuri sau alte caracteristici ale spamului.Pe baza rezultatelor analizei, filtrul adaugă un punctaj spam mesajului.

Filtrul detectează, de asemenea, mesajele marcate `SEXUALLY-EXPLICIT:` în subiect și le marchează ca SPAM.

Notă
Începând din 19 Mai 2004, mesajele Spam care conțin material cu specific sexual trebuie să includă avertismentul SEXUALLY-EXPLICIT: în subiect. În caz contrar expeditorii vor fi acuzați de încălcarea legii și ulterior amendați.

Filtrul Bayesian

Filtrul Bayesian verifică mesajele ținând cont de informații statistice despre frecvența cu care anumite cuvinte apar în mesaje clasificate ca Spam comparativ cu mesajele non-Spam (vor fi folosite mesajele etichetate de dumneavoastră sau de către Filtrul Euristic).

Aceasta înseamnă că dacă, de exemplu, un anumit cuvânt format din patru litere apare mai des în mesajele Spam, atunci se poate presupune logic că există o probabilitate ridicată ca următorul mesaj ce conține respectivul cuvânt să fie Spam. Toate cuvintele semnificative din mesaje sunt verificate. Sintetizând informațiile statistice, se calculează probabilitatea ca un anumit mesaj să fie Spam.

Acest modul prezintă o altă caracteristică interesantă: este educabil. Se adaptează rapid la tipul de mesaje primite de un anumit utilizator și stochează informații cu privire la toate mesajele. Pentru a funcționa eficient, filtrul trebuie educat, adică trebuie să i se dea exemple de SPAM precum și de mesaje legitime, la fel cum unui câine i se indică mirosul pe care trebuie să îl găsească. Uneori filtrul trebuie să fie și corectat / atenționat atunci când clasifică greșit unele mesaje.

Important
Puteți corecta filtrul Bayesian folosind butoanele **Este Spam** și **Nu este Spam** din bara de comenzi Antispam.

18.1.2. Funcționarea modulului Antispam

Motorul antispam al BitDefender utilizează concomitent toate filtrele antispam pentru a determina dacă un anumit mesaj e-mail ar trebui să ajungă în directorul **Inbox (Mesaje primite)** sau nu.

Fiecare mesaj e-mail pe care îl primiți este întâi verificat de filtrul Lista de prieteni/Lista de spammeri. Dacă adresa expeditorului se regăsește în Lista de prieteni mesajul este trimis direct în **Inbox**.

În caz contrar, filtrul Lista de spammeri va verifica dacă adresa expeditorului se află pe această listă. Dacă adresa este găsită, e-mailul este etichetat ca SPAM și este mutat în directorul **Spam**.

Altfel, Filtrul de caractere va verifica dacă mesajul este scris cu caractere chirilice sau asiatice. Dacă mesajul este scris astfel, el va fi etichetat ca SPAM și mutat în directorul **Spam**.

Dacă mesajul nu este scris cu caractere asiatice sau chirilice, acesta va fi transmis Filtrului de imagini. **Filtrul de imagini** va detecta toate mesajele e-mail care au atașate imagini cu conținut spam.

Filtrul URL va compara linkurile găsite în e-mail cu linkurile din baza de date BitDefender de linkuri spam cunoscute. În cazul unei potriviri, e-mailul va fi considerat SPAM.

Filtrul NeuNet (euristic) va prelua mesajul și va verifica toate componentele acestuia, căutând cuvinte, fraze, linkuri sau alte caracteristici SPAM. Pe baza rezultatelor analizei, e-mailul va primi un punctaj spam.

Notă
Dacă mesajul este etichetat ca SEXUALLY EXPLICIT în subiect, BitDefender îl va considera SPAM.

Filtrul Bayesian va analiza mesajul în continuare, ținând cont de informații statistice despre frecvența cu care anumite cuvinte apar în mesaje clasificate ca Spam comparativ cu mesajele non-Spam (vor fi folosite mesajele etichetate de dumneavoastră sau de către Filtrul Euristic). Mesajul va primi un alt punctaj spam.

În cazul în care punctajul spam total (punctajul euristic + punctajul bayesian) depășește nivelul limită, e-mailul este considerat a fi SPAM.Nivelul limită este definit prin intermediul nivelului de protecție antispam.Pentru mai multe informații, consultați *„Reglarea nivelului de protecție”* (p. 97).

18.1.3. Actualizări Antispam

La fiecare actualizare:

- noi semnături de imagini vor fi adăugate **Filtrului de imagini**.
- noi linkuri vor fi adăugate **Filtrului URL**.
- noi reguli vor fi adăugate **Filtrului NeuNet (euristic)**.

Aceasta permite sporirea eficienței motorului Antispam.

Pentru a vă proteja de spammeri, BitDefender poate realiza actualizări automate. Păstrați opțiunea **Actualizare automatică** activată.

18.2. Asistentul de optimizare Antispam

Prima dată când deschideți clientul dumneavoastră de mail după instalarea BitDefender, va apărea un program asistent care vă va ajuta să configurați lista de prieteni și lista de spammeri și să educați motorul de învățare (bayesian) pentru a crește eficiența filtrelor Antispam.

Notă
Programul asistent poate fi lansat, oricând doriți, făcând clic pe butonul **Asistent** din bara de comenzi Antispam.

Puteți naviga prin programul asistent cu ajutorul butoanelor **Înainte** și **Înapoi**.Dacă doriți să săriți peste un pas al configurării, selectați **Omite**.Pentru a părăsi asistentul, faceți clic pe **Anulează**.

1. **Fereastra de întâmpinare**
2. **Adăugați contactele pe Lista de prieteni**

   Aici puteți vedea toate adresele din **Address Book**. Selectați-le pe cele pe care doriți să le adăugați pe **lista de prieteni** (vă recomandăm să le selectați pe toate). Veți primi toate mesajele de la aceste adrese, indiferent de conținut.

   Pentru a vă adăuga toate contactele pe lista de prieteni, bifați **Selectează tot**.
3. **Ștergeți baza de date bayesiană**

   Notă
   Prima dată când rulați asistentul, mergeți direct la pasul următor.

   Există posibilitatea să descoperiți că filtrul Antispam a început să-și piardă eficiența. Aceasta se poate întâmpla din cauza educării incorecte (ați etichetat din greșeală unele mesaje legitime ca Spam, sau invers). Dacă filtrul Antispam este ineficient, trebuie să-i ștergeți baza de date și să-l reeducați urmând pașii acestui program asistent.

   Selectați **Șterge baza de date a filtrului antispam** dacă doriți să ștergeți baza de date a Filtrului Bayesian.

   Puteți salva baza de date a filtrului Bayesian într-un fișier pentru a o putea folosi cu un alt produs BitDefender sau după reinstalarea BitDefender.Pentru a salva baza de date Bayesiană, faceți clic pe butonul **Salvează date** și salvați-o în locația dorită.Fișierul va avea o extensie `. dat`.

   Pentru a încărca o bază de date Bayesiană salvată anterior, faceți clic pe butonul **Încărcă date** și deschideți fișierul corespunzător.
4. **Educați filtrul bayesian cu e-mailuri legitime (non-spam)**

   Selectați un director care conține mesaje e-mail legitime. Aceste mesaje vor fi folosite pentru a educa filtrul Antispam.

   Sub lista de directoare se găsesc două opțiuni avansate:
   - **Include toate subdirectoarele** - pentru a include subdirectoarele în selecție.
   - **Adaugă automat pe lista de prieteni** - pentru a adăuga expeditorii pe lista de prieteni.
5. **Educați filtrul bayesian cu e-mailuri spam**

   Selectați un director care conține mesaje Spam. Aceste mesaje vor fi folosite pentru a educa filtrul Antispam.

Important
Directorul nu trebuie să conțină niciun mesaj legitim, altfel performanțele filtrului Antispam vor fi considerabil reduse.

Sub lista de directoare se găsesc două opțiuni avansate:

- **Include toate subdirectoarele** - pentru a include subdirectoarele în selecție.
- **Adaugă automat pe lista de spammeri** - pentru a adăuga expeditorii pe lista de spammeri.Mesajele e-mail de la acești expeditori vor fi marcate ca spam întotdeauna și prelucrate în consecință.

6. **Rezumat**

   În această fereastră puteți vedea toate setările făcute în programul asistent. Puteți face orice schimbări, revenind la pașii anteriori (faceți clic pe **Înapoi**).

   Dacă nu doriți să faceți nicio modificare, faceți clic pe **Finalizare** pentru a închide programul asistent.

18.3. Utilizarea barei de instrumente antispam din fereastra clientului de e-mail

În partea de sus a ferestrei clientului dumneavoastră de mail, puteți vedea bara de comenzi antispam.Bara de comenzi antispam vă ajută să administrați protecția antispam direct din clientul dumneavoastră de mail.Puteți corecta BitDefender cu ușurință dacă acesta a marcat un mesaj legitim ca SPAM.

Important
BitDefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat.Pentru o listă completă a clienților de mail admiși, consultați *„Cerințe software”* (p. 2).

Fiecare buton al barei de comenzi este explicat mai jos:

- **Este Spam** - trimite un mesaj modulului Bayesian indicând că mesajul selectat este Spam. Mesajul va primi eticheta SPAM și va fi mutat în directorul**Spam**.

  Mesajele viitoare care seamănă cu acest mesaj vor fi considerate SPAM.

- **Nu este Spam** - trimite un mesaj modulului Bayesian indicând că mesajul selectat nu este spam, iar BitDefender nu ar fi trebuit să-l marcheze.E-mailul va fi mutat din directorul **Spam** în directorul **Inbox** (Mesaje primite).

  Mesajele viitoare care seamănă cu acesta nu vor mai fi considerate SPAM.

Important
Butonul **Nu este Spam** este activ doar când selectați un mesaj etichetat ca SPAM de către BitDefender (în mod normal aceste mesaje se găsesc în directorul **Spam**).

- **Adaugă Spammer** - adaugă expeditorul e-mailului selectat pe Lista de spammeri.Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare.Mesajele e-mail primite de la adrese de pe Lista de spammeri sunt marcate automat ca `[spam]`.
- **Adaugă prieten** - adaugă expeditorul e-mailului selectat pe Lista de prieteni.Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare.Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.
- **Spammeri** - deschide **lista de spammeri** care conține adrese de e-mail de la care nu doriți să primiți mesaje, indiferent de conținutul acestora.Pentru mai multe informații, consultați *„Configurarea listei de spammeri”* (p. 99).
- **Prieteni** - deschide **lista de prieteni** care conține adrese de e-mail de la care doriți întotdeauna să primiți mesaje, indiferent de conținutul acestora.Pentru mai multe informații, consultați *„Configurați lista de prieteni”* (p. 98).
- **Setări** - deschide fereastra de **Setări** unde puteți specifica unele opțiuni pentru modulul **Antispam**.
- **Program asistent** - deschide programul asistent de optimizare antispam.Acest asistent vă va ajuta să vă educați filtrul bayesian pentru a crește eficiența protecției dumneavoastră antispam.De asemenea, puteți adăuga adresele din Agenda dumneavoastră pe Lista de prieteni / spammeri.
- **BitDefender Antispam** - deschide o fereastră în care puteți configura nivelul de protecție antispam și filtrele antispam.

18.3.1. Indicarea erorilor de detecție

Dacă folosiți un client de mail admis, puteți corecta cu ușurință filtrul antispam (indicând care mesaje e-mail nu ar trebui marcate ca `[spam]`). Astfel, veți îmbunătăți considerabil eficiența filtrului antispam.Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele legitime pe care BitDefender le-a marcat incorect ca `[spam]`.
4. Faceți clic pe butonul **Adaugă prieten** din bara de instrumente antispam BitDefender, pentru a adăuga expeditorul pe Lista de prieteni.Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare.Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.
5. Faceți clic pe butonul **Nu este Spam** din bara de instrumente antispam BitDefender (localizată, de obicei, în zona de sus a ferestrei clientului de mail). Aceasta îi indică Motorului de învățare faptul că mesajul selectat nu este spam. Mesajul e-mail va fi mutat în directorul Inbox.Următoarele mesaje e-mail care corespund acelor tipare nu vor mai fi marcate ca `[spam]`.

18.3.2. Indicarea mesajelor spam nedetectate

Dacă folosiți un client de mail admis, puteți indica cu ușurință care mesaje e-mail ar fi trebuit să fie detectate ca spam. Astfel, veți îmbunătăți considerabil eficiența filtrului antispam.Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți la directorul Inbox.
3. Selectați mesajele spam nedetectate.
4. Faceți clic pe butonul **Este Spam** din bara de instrumente antispam BitDefender (localizată, de obicei, în zona de sus a ferestrei clientului de mail). Aceasta îi indică Motorului de învățare faptul că mesajele selectate sunt spam. Acestea sunt marcate imediat ca `[spam]` și mutate în directorul de mesaje nesolicitate (junk).Următoarele mesaje e-mail care corespund acelor tipare vor fi marcate ca `[spam]`.

18.3.3. Resetarea Motorului de învățare (bayesian)

Dacă filtrul dumneavoastră antispam nu este foarte precis, trebuie să curățați baza de date și să resetați filtrul bayesian.

Înainte de a educa Motorul de învățare (Bayesian), pregătiți un director care să conțină numai mesaje SPAM și un altul doar cu mesaje legitime. Motorul de învățare le va analiza și va învăța caracteristicile definitorii pentru mesajele spam sau legitime pe care le primiți de obicei. Pentru ca educarea să fie eficientă, trebuie să existe cel puțin 50 de mesaje din fiecare categorie.

Pentru a reseta baza de date Bayesiană și pentru a re-educa Motorul de învățare, urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Pe bara de instrumente antispam BitDefender, faceți clic pe butonul **Asistent** pentru a porni programul asistent de configurare antispam.
3. Faceți clic pe **Înainte**.
4. Selectați **Omite** și faceți clic pe **Înainte**.
5. Selectați **Șterge baza de date a filtrului antispam** și faceți clic pe **Înainte**.
6. Selectați directorul care conține mesaje legitime și faceți clic pe **Înainte**.
7. Selectați directorul care conține mesaje SPAM și faceți clic pe **Înainte**.
8. Faceți clic pe **Finalizează** pentru a începe procesul de educare.
9. Când educarea a luat sfârșit, faceți clic pe **Închide**.

18.3.4. Salvarea și încărcarea bazei de date bayesiane

Puteți salva baza de date a filtrului Bayesian într-un fișier pentru a o putea folosi cu un alt produs BitDefender sau după reinstalarea BitDefender.

Faceți clic pe butonul **Setări** de pe bara de instrumente antispam BitDefender.

Pentru a salva baza de date Bayesiană, faceți clic pe butonul **Salvează date** și salvați-o în locația dorită.Fișierul va avea o extensie `. dat`.

Pentru a încărca o bază de date Bayesiană salvată anterior, faceți clic pe butonul **Încărcă date** și deschideți fișierul corespunzător.

18.3.5. Configurarea setărilor generale

Pentru a configura setările generale antispam pentru clientul dumneavoastră de e-mail, faceți clic pe butonul **Setări** din bara de instrumente antispam BitDefender.

Următoarele opțiuni sunt disponibile:

- **Mută mesajul in directorul Deleted Items** - mută mesajele Spam în directorul **Deleted Items** (doar pentru Microsoft Outlook Express / Windows Mail);
- **Marchează mesajul ca 'citit'** - marchează toate mesajele spam ca fiind citite pentru a nu fi deranjat când sosesc noi mesaje spam.

Faceți clic pe tabul **Alerte** dacă doriți să accesați secțiunea în care puteți dezactiva apariția ferestrelor de confirmare pentru butoanele **Adaugă spammer** și **Adaugă prieten**.

În fereastra **Alerte** puteți de asemenea să activați / dezactivați apariția alertei **Selectați un mesaj e-mail**. Această alertă apare atunci când selectați un grup în loc de un mesaj e-mail.

18.4. Reglarea nivelului de protecție

Anumite filtre antispam pot identifica e-mailurile spam în mod direct, în timp ce altele adaugă un punctaj spam e-mailului, pe baza caracteristicilor spam identificate.

Nivelul de protecție antispam este utilizat pentru a determina dacă un e-mail poate fi considerat ca fiind spam pe baza punctajului spam total (primit după ce a fost verificat de toate filtrele antispam).

Nu trebuie să modificați nivelul de protecție antispam decât dacă protecția antispam nu funcționează corespunzător.Cu toate acestea, mai degrabă decât să modificați nivelul de protecție în mod independent, se recomandă să citiți mai întâi *„Filtrul Antispam nu funcționează corect”* (p. 182) și să urmați instrucțiunile de remediere a problemei.

Pentru a regla nivelul de protecție antispam:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antispam > Stare**.
3. Trageți de cursor de-a lungul scalei pentru a seta nivelul de protecție corespunzător.Pentru a seta nivelul implicit de protecție (**Moderat către agresiv**) faceți clic pe **Nivel implicit**.

Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul de protecție care se potrivește mai bine nevoilor dumneavoastră de securitate.Descrierea vă informează, de asemenea, despre orice acțiuni suplimentare pe care ar trebui să le luați pentru a evita potențialele probleme sau pentru a spori eficiența detecției antispam.

18.5. Configurați lista de prieteni

Lista de prieteni este o listă care conține toate adresele de e-mail de la care doriți să primiți mesaje, indiferent de conținutul acestora. Mesajele de la prieteni nu vor fi etichetate Spam, chiar dacă au conținut asemănător mesajelor Spam.

Notă
Orice mesaj venit de la o adresă inclusă pe **lista de prieteni** va fi trimis automat în directorul Inbox, fără a mai fi procesat.

Pentru a configura și administra lista de prieteni:

- Dacă utilizați Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, faceți clic pe butonul **Prieteni** de pe bara de instrumente antispam BitDefender integrată în clientul dumneavoastră de e-mail.
- Alternativ, urmați acești pași:
  1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
  2. Mergeți la **Antispam > Stare**.
  3. Faceți clic pe **Administrează prieteni**.

Pentru a adăuga o adresă de e-mail, selectați opțiunea **Adresă de e-mail**, introduceți adresa și faceți clic pe butonul de lângă câmpul de editare. Sintaxă: nume@domeniu.com.

Pentru a adăuga toate adresele de e-mail dintr-un anumit domeniu, selectați opțiunea **Nume domeniu**, introduceți numele domeniului și faceți clic pe butonul de lângă câmpul de editare.Sintaxă:

- @domeniu.com, *domeniu.com și domeniu.com - toate mesajele primite de la domeniu.com vor ajunge în directorul **Inbox** indiferent de conținut;
- *domain* - toate mesajele primite de la domain (indiferent de sufixul domeniului) vor ajunge în directorul **Inbox** indiferent de conținut;

- *com - toate mesajele primite având sufixul domeniului com vor ajunge în directorul **Inbox** indiferent de conținut;

Se recomandă să evitați adăugarea de domenii, însă acest lucru poate fi util în anumite situații.De exemplu, puteți adăuga domeniul de e-mail al companiei pentru care lucrați sau pe cele ale partenerilor dumneavoastră de încredere.

Pentru a șterge un obiect de pe listă, selectați-l și faceți clic pe butonul **Șterge**.Pentru a șterge toate înregistrările de pe listă faceți clic pe butonul **Șterge lista** și apoi pe **Da**, pentru confirmare.

Puteți salva Lista de prieteni într-un fișier, astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului.Pentru a salva Lista de prieteni, faceți clic pe butonul **Salvează** și salvați-o în locația dorită.Fișierul va avea o extensie `.bwl`.

Pentru a încărca o Listă de prieteni salvată anterior, faceți clic pe butonul **Încarcă** și deschideți fișierul `.bwl` corespunzător.Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior selectați **Suprascrie lista curentă**.

Faceți clic pe **Salvează** și **OK** pentru a salva modificările și a închide **Lista de prieteni**.

18.6. Configurarea listei de spammeri

Lista de spammeri este o listă care conține toate adresele de e-mail de la care nu doriți să primiți mesaje, indiferent de conținutul acestora.Orice mesaj primit de la o adresă din **lista de spammeri** va fi automat etichetat ca Spam, fără altă procesare.

Pentru a configura și administra lista de spammeri:

- Dacă utilizați Microsoft Outlook / Outlook Express / Windows Mail / Thunderbird, faceți clic pe butonul **Spammeri** de pe bara de instrumente antispam BitDefender integrată în clientul dumneavoastră de e-mail.
- Alternativ, urmați acești pași:
  1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
  2. Mergeți la **Antispam > Stare**.
  3. Faceți clic pe **Administrează spammeri**.

Pentru a adăuga o adresă de e-mail, selectați opțiunea **Adresă de e-mail**, introduceți adresa și faceți clic pe butonul de lângă câmpul de editare. Sintaxă: nume@domeniu.com.

Pentru a adăuga toate adresele de e-mail dintr-un anumit domeniu, selectați opțiunea **Nume domeniu**, introduceți numele domeniului și faceți clic pe butonul de lângă câmpul de editare.Sintaxă:

- @domeniu.com, *domeniu.com și domeniu.com - toate mesajele primite de la domeniu.com vor fi etichetate ca SPAM;
- *domain* - toate mesajele primite de la domain(indiferent de sufixul domeniului) vor fi etichetate ca SPAM;
- *com - a- toate mesajele primite având sufixul domeniului com vor fi etichetate ca SPAM.

Se recomandă să evitați adăugarea de domenii, însă acest lucru poate fi util în anumite situații.

Avertisment

Nu adăugați pe Lista de spammeri numele de domeniu ale serviciilor legitime de e-mail oferite online (Yahoo, Gmail, Hotmail sau altele asemenea). În caz contrar, mesajele e-mail primite de la orice utilizator înregistrat al unui astfel de serviciu vor fi detectate ca spam. Dacă, de exemplu, adăugați `yahoo.com` pe Lista de spammeri, toate mesajele e-mail care provin de la adrese `yahoo.com` vor fi marcate ca `[spam]`.

Pentru a șterge un obiect de pe listă, selectați-l și faceți clic pe butonul **Șterge**.Pentru a șterge toate înregistrările de pe listă faceți clic pe butonul **Șterge lista** și apoi pe **Da**, pentru confirmare.

Puteți salva Lista de spammeri într-un fișier astfel încât s-o puteți folosi pe un alt calculator sau după reinstalarea produsului.Pentru a salva Lista de spammeri, faceți clic pe butonul **Salvează** și salvați-o în locația dorită.Fișierul va avea o extensie `.bwl`.

Pentru a încărca o Listă de spammeri salvată anterior, faceți clic pe butonul **Încarcă** și deschideți fișierul `.bwl` corespunzător.Pentru a reseta conținutul listei curente atunci când încărcați o listă salvată anterior selectați **Suprascrie lista curentă**.

Faceți clic pe **Salvează** și **OK** pentru a salva modificările și a închide **Lista de spammeri**.

18.7. Configurarea filtrelor și setărilor antispam

Conform descrierii de la *„Detalii privind modulul Antispam”* (p. 89), BitDefender utilizează o combinație de diferite filtre antispam pentru a identifica spamul.Filtrele antispam sunt preconfigurate pentru asigurarea unei protecții eficiente.

Puteți dezactiva fiecare dintre aceste filtre sau modifica setările acestora, însă acest lucru nu este recomandat.Acestea sunt câteva schimbări pe care este posibil să doriți să le faceți:

- Dacă primiți e-mailuri legitime scrise cu caractere asiatice sau chirilice, dezactivați sau activați setarea care blochează în mod automat aceste e-mailuri.

Notă

Setarea corespunzătoare este dezactivată pentru versiunile localizate ale programului care utilizează astfel de seturi de caractere (de exemplu, în cazul versiunii în limba rusă sau chineză).

- Dacă nu doriți să adăugați în mod automat destinatarii e-mailurilor trimise de dumneavoastră în lista de prieteni, puteți dezactiva setarea corespunzătoare.În acest caz, adăugați contactele dumneavoastră în lista de prieteni, conform descrierii din *„Configurați lista de prieteni”* (p. 98).
- Utilizatorii avansați pot încerca să regleze dimensiunea dicționarului bayesian în scopul obținerii unor performanțe antispam îmbunătățite.Un număr mai mic de cuvinte va conduce la o procesare antispam mai rapidă, însă mai puțin precisă.Un număr mai mare de cuvinte va spori precizia identificării antispam, însă va dura mai mult până veți putea accesa e-mailurile.

Notă

Pentru a atinge nivelul dorit de performanță, pot fi necesare câteva reglaje ale dimensiunii dicționarului bayesian.Dacă rezultatul nu este cel așteptat, restabiliți setarea implicită și dimensiunea recomandată de 200,000 cuvinte.

Pentru configurarea setărilor și filtrelor antispam:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antispam > Setări**.
3. Configurați setările după cum este nevoie.Pentru a afla ce face o opțiune, țineți cursorul mouse-ului deasupra ei și citiți descrierea afișată în partea de jos a ferestrei.
4. Faceți clic pe **Salvează** pentru a salva modificările.

Pentru a aplica setările implicite, faceți clic pe **Nivel implicit**.

19. Control parental

Controlul parental BitDefender vă permite să controlați accesul la Internet și la anumite aplicații pentru fiecare utilizator care deține un cont de utilizator pe sistem.

Puteți configura Controlul parental să blocheze:

- pagini web inadecvate.
- accesul la Internet, pentru anumite intervale de timp (de exemplu, în timpul rezervat lecțiilor).
- paginile web, mesajele e-mail și mesajele instant care conțin anumite cuvinte cheie.
- jocuri, aplicații de chat, partajare de fișiere și altele.
- mesaje instant trimise de alte contacte de mesagerie instant decât cele permise.

Important

Doar utilizatorii cu drepturi administrative pe sistem (administratorii de sistem) pot accesa și configura Controlul parental.Pentru a vă asigura că doar dumneavoastră puteți modifica setările de Control parental pentru oricare utilizator, puteți proteja aceste setări cu o parolă.Vi se va cere să configurați parola atunci când activați Controlul parental pentru un anumit utilizator.

După ce ați configurat Controlul parental, puteți afla cu ușurință activitățile copiilor dumneavoastră la calculator.

Chiar și atunci când nu vă aflați acasă, puteți să verificați activitățile copiilor dumneavoastră și să modificați setările de Control parental prin intermediul funcției de Control parental la distanță.

19.1. Configurarea Controlului parental

Înainte de a configura funcția de Control parental, creați conturi de utilizator Windows separate pentru copiii dumneavoastră. Acestea vă vor permite să știți exact ce face fiecare la calculator. Trebuie să creați conturi de utilizator limitate (standard) pentru ca aceștia să nu poată modifica setările de Control parental. Pentru mai multe informații, consultați *„Cum creez conturi de utilizator Windows?”* (p. 168).

În cazul în care copiii dumneavoastră pot accesa un cont de administrator pe calculatorul lor, trebuie să configurați o parolă pentru a proteja setările de Control parental.Pentru mai multe informații, consultați *„Protejarea setărilor de Control parental”* (p. 104).

Pentru a configura Controlul parental:

1. Asigurați-vă că sunteți conectat la calculator pe contul de administrator.Doar utilizatorii cu drepturi administrative pe sistem (administratorii de sistem) pot accesa și configura Controlul parental.
2. Deschideți BitDefender.
3. În funcție de modul de vizualizare a interfeței, accesați setările Controlului parental după cum urmează:

   Modul Intermediar
   Mergeți la fila **Securitate** și faceți clic pe **Control parental** în zona de Sarcini rapide din partea stângă a ferestrei.

   Modul Expert
   Faceți clic pe **Control parental** în meniul din stânga.

Notă

În Modul Novice și Modul Intermediar de vizualizare, puteți configura o comandă rapidă pentru a putea accesa aceste setări din pagina de stare.Pentru mai multe informații, consultați *„Instrumentele mele”* (p. 33).

Puteți vedea informații despre starea Controlului parental, pentru fiecare cont de utilizator Windows.Categoria de vârstă este afișată sub fiecare nume de utilizator dacă este activat Controlul parental.Când Controlul parental este dezactivat, starea sa apare ca **neconfigurat**.

Pentru a configura Controlul parental pentru un anumit cont de utilizator:

1. Utilizați selectorul pentru a activa funcția de Control parental pentru respectivul cont de utilizator.
2. Vi se va solicita să setați parola pentru Controlul parental.Setați o parolă pentru a proteja setările dumneavoastră de Control parental.Pentru mai multe informații, consultați *„Protejarea setărilor de Control parental”* (p. 104).
3. Setați categoria de vârstă pentru a permite copilului dumneavoastră să acceseze numai site-uri web potrivite pentru vârstă lui.Setarea vârstei copilului va încărca automat setările considerate adecvate pentru respectiva categorie de vârstă, pe baza standardelor de dezvoltare a copilului.
4. Dacă doriți să configurați setările de Control parental în detaliu, faceți clic pe **Setări**.Faceți clic pe o filă pentru a configura funcția corespunzătoare de Control parental:

   - **Web** - pentru a filtra navigarea pe internet conform regulilor stabilite de dumneavoastră în secțiunea Web.
   - **Aplicații** - pentru a bloca accesul la aplicațiile pe care le precizați în secțiunea Aplicații.

- **Cuvinte cheie** - pentru a filtra accesul la web, mail și mesageria instant conform regulilor stabilite de dumneavoastră în secțiunea Cuvinte cheie.
- **Mesagerie** - pentru a bloca sau permite conversațiile cu utilizatori de mesagerie instant conform regulilor stabilite de dumneavoastră în secțiunea Mesagerie.

Notă
Pentru a afla cum să le configurați, consultați următoarele secțiuni din acest capitol.

Configurați opțiunile de monitorizare după cum este cazul:

- **Vreau să primesc un raport de activitate prin e-mail.** O notificare prin e-mail este trimisă de fiecare dată când funcția de Control parental a BitDefender blochează o activitate.Trebuie mai întâi să configurați setările privind notificările.
- **Salvează un jurnal de trafic internet.** Înregistrează în jurnal site-urile web vizitate de utilizatorii pentru care este activat Controlul Parental.

Pentru mai multe informații, consultați *„Monitorizarea activității copiilor”* (p. 111).

Dacă doriți să monitorizați și să controlați la distanță activitățile de la calculator și de pe internet ale copilului dumneavoastră, activați funcția de Control parental la distanță prin utilizarea selectorului.Pentru mai multe informații, consultați *„Control parental la distanță”* (p. 114).

19.1.1. Protejarea setărilor de Control parental

Dacă nu sunteți singura persoană cu drepturi administrative care utilizează acest calculator, este recomandat să vă protejați setările de Control parental cu o parolă.Setând parola, veți împiedica alți utilizatori cu drepturi administrative pe sistem să modifice setările de Control parental pe care le-ați configurat pentru un anumit utilizator.

BitDefender vă va solicita în mod implicit să setați o parolă atunci când activați Controlul parental.Pentru a seta protecția prin parolă, procedați astfel:

1. Introduceți parola în câmpul **Parolă**.
2. Introduceți parola din nou în câmpul **Confirmați parola**.
3. Faceți clic pe **OK** pentru a salva parola și închide fereastra.

Din acest moment, dacă doriți să schimbați setările de Control parental, vi se va solicita să introduceți parola.Ceilalți administratori de sistem, dacă există, vor trebui, de asemenea, să furnizeze parola pentru a putea schimba setările de Control parental.

Notă
Această parolă nu va proteja alte setări BitDefender.

Dacă nu setați parola și nu doriți să mai apară această fereastră din nou, bifați **Nu solicita parolă la activarea Controlului parental**.

Important
Dacă ați uitat parola, trebuie să reinstalați programul sau să contactați BitDefender pentru asistență.

Pentru a elimina protecția asigurată prin parolă:

1. Deschideți BitDefender și faceți clic pe butonul **Opțiuni** din colțul din dreapta sus al ferestrei.
2. Mergeți la **Setări generale**.
3. Utilizați selectorul pentru a dezactiva opțiunea **Parolă setări**.
4. Introduceți parola.
5. Faceți clic pe **OK**.

19.1.2. Control Web

Controlul Web vă ajută să blocați accesul la paginile web cu conținut inadecvat. O listă cu pagini web propuse spre a fi blocate este oferită de către BitDefender și actualizată permanent, ca parte a procesului obișnuit de actualizare.

Notă
Atunci când activați funcția de Control parental și setați vârsta copilului dumneavoastră, funcția de Control web este activată în mod automat și configurată pentru a bloca accesul la site-uri web considerate a fi nepotrivite pentru vârsta copilului dumneavoastră.

Pentru a configura Controlul web pentru un anumit cont de utilizator:

1. Accesați fereastra cu setările de Control parental BitDefender pentru respectivul cont de utilizator.
2. Faceți clic pe fila **Web**.
3. Utilizați selectorul pentru a activa controlul web.
4. Puteți verifica care categorii web sunt blocate/restricționate în mod automat pentru grupul de vârstă selectat în prezent.Dacă setările implicite nu sunt satisfăcătoare, le puteți configura după cum doriți.

   Pentru a modifica acțiunea configurată pentru o anumită categorie de conținut web, faceți clic pe starea actuală și selectați acțiunea dorită din meniu.
5. Dacă doriți, creați propriile dumneavoastră reguli pentru a permite sau bloca accesul la anumite site-uri web.Dacă funcția de Control parental blochează în mod automat accesul la un site, puteți crea o regulă pentru a permite în mod explicit accesul la respectivul site.

6. Puteți stabili limite în ceea ce privește timpul petrecut de copilul dumneavoastră pe internet.Pentru mai multe informații, consultați „Restricționarea accesului la internet în funcție de oră” (p. 106).

Crearea regulilor de Control web

Pentru a permite sau bloca accesul la un site web, urmați acești pași:

1. Faceți clic pe **Permite acces site web** sau **Blochează site web**.
2. Introduceți adresa site-ului web în câmpul **Pagina web**.
3. Selectați acțiunea dorită pentru această regulă - **Permite** sau **Blochează**.
4. Faceți clic pe **Finalizează** pentru a adăuga regula.

Administrarea regulilor de Control web

Regulile de Control web sunt afișate în tabelul din partea de jos a ferestrei. Sunt furnizate adresa site-ului web și starea curentă corespunzătoare fiecărei reguli de Control web.

Pentru a șterge o regulă, selectați-o și faceți clic pe **Șterge**.

Pentru a edita o regulă, selectați-o și faceți clic pe **Modifică** sau faceți dublu-clic pe aceasta.Efectuați modificările necesare în fereastra de configurare.

Restricționarea accesului la internet în funcție de oră

În secțiunea de Programare a accesului la internet, puteți seta limite privind timpul pe care-l petrece copilul dumneavoastră pe internet.

Pentru a bloca în totalitate accesul la internet, selectați **Blochează accesul la internet**.

Pentru a restricționa accesul la internet la anumite ore din zi:

1. Selectați **Durată restricție internet**.
2. Faceți clic pe **Modificare program**.
3. Selectați din grilă intervalele temporale în care accesul la internet este blocat.Puteți face clic pe celule individuale sau puteți face clic și trage pentru a acoperi perioade mai lungi de timp.
4. Faceți clic pe **Salvează**.

Notă

BitDefender va efectua actualizări în fiecare oră indiferent dacă accesul la internet este blocat.

19.1.3. Controlul aplicațiilor

Controlul aplicațiilor vă ajută să împiedicați orice aplicație să ruleze. Jocurile, programele media și de mesagerie, precum și alte categorii de programe și aplicații malițioase pot fi împiedicate să ruleze. Aplicațiile blocate în acest fel sunt de asemenea protejate de modificări, și nu pot fi copiate sau mutate.Puteți bloca aplicații permanent sau numai în anumite intervale, cum ar fi cele în care copiii dumneavoastră trebuie să-și facă temele.

Pentru a configura Controlul aplicațiilor pentru un anumit cont de utilizator:

1. Accesați fereastra cu setările de Control parental BitDefender pentru respectivul cont de utilizator.
2. Faceți clic pe fila **Aplicații**.
3. Utilizați selectorul pentru a activa Controlul aplicațiilor.
4. Creați reguli pentru aplicațiile către care doriți să blocați sau să restricționați accesul.

Crearea regulilor de Control al aplicațiilor

Pentru a bloca sau a restricționa accesul la o aplicație, urmați pașii de mai jos:

1. Faceți clic pe **Blochează** sau **Restricționează**.
2. Faceți clic pe **Caută** pentru a localiza aplicația la care doriți să blocați sau să restricționați accesul.Aplicațiile instalate sunt de obicei localizate în directorul `C:\Program Files`.
3. Selectați acțiunea regulii:
   - **Blochează permanent** pentru a bloca complet accesul la aplicație.
   - **Blochează conform acestui program** pentru a restricționa accesul în anumite intervale de timp.

   Dacă alegeți să restricționați accesul la aplicație în loc să-l blocați complet, trebuie să și selectați în grilă zilele și intervale de timp în care accesul este blocat.
4. Faceți clic pe **Salvează** pentru a adăuga regula.

Administrarea regulilor de Control al aplicațiilor

Regulile de Control al aplicațiilor sunt afișate în tabelul din partea de jos a ferestrei. Sunt furnizate numele, calea și starea actuală a fiecărei reguli de Control al aplicațiilor.

Pentru a șterge o regulă, selectați-o și faceți clic pe **Șterge**.

Pentru a edita o regulă, selectați-o și faceți clic pe **Modifică** sau faceți dublu-clic pe aceasta.Efectuați modificările necesare în fereastra de configurare.

19.1.4. Control cuvinte cheie

Opțiunea Control cuvinte cheie vă permite să blocați accesul utilizatorilor la mesaje e-mail, pagini web și mesaje instant care conțin anumite cuvinte.Folosind opțiunea Control cuvinte cheie, puteți împiedica vizualizarea de cuvinte sau expresii nepotrivite de către copiii dumneavoastră, atunci când aceștia sunt online.

Notă
Controlul după cuvinte cheie pentru mesageria instant este disponibil numai pentru Yahoo Messenger și Windows Live (MSN) Messenger.

Pentru a configura Controlul cuvintelor cheie pentru un anumit cont de utilizator:

1. Accesați fereastra cu setările de Control parental BitDefender pentru respectivul cont de utilizator.
2. Faceți clic pe fila **Cuvinte cheie**.
3. Utilizați selectorul pentru a activa controlul cuvintelor cheie.
4. Creați reguli de control cu cuvinte cheie pentru a bloca cuvintele cheie necorespunzătoare.
5. Pentru a vă împiedica copiii să dezvăluie informații personale (cum ar fi adresa de acasă sau numărul de telefon) persoanelor pe care le-ați întâlnit pe internet, trebuie să creați reguli de control al identității.Pentru mai multe informații, consultați „Crearea regulilor Controlului de identitate” (p. 109).

Crearea regulilor de Control cuvinte cheie

Pentru ca blocarea să se facă după un cuvânt sau o sintagmă, urmați acești pași:

1. Faceți clic pe **Blocare cuvânt cheie**.
2. Introduceți cuvântul sau sintagma cheie în câmpul editabil. Dacă doriți să fie detectate numai cuvintele întregi, selectați căsuța **Caută cuvinte întregi**
3. Selectați tipul de trafic pe care BitDefender trebuie să-l scaneze după cuvântul precizat.

Opțiune	Descriere
HTTP	Paginile web care conțin argumentul sunt blocate.
POP3	Mesajele e-mail care conțin argumentul sunt blocate.
Mesagerie instant	Mesajele instant care conțin argumentul sunt blocate.

4. Faceți clic pe **Finalizează** pentru a adăuga regula.

Administrarea regulilor de Control cuvinte cheie

Regulile Controlului pe bază de cuvinte cheie sunt afișate în tabel. Pentru fiecare regulă sunt oferite informații detaliate.

Pentru a șterge o regulă, selectați-o și faceți clic pe **Șterge**.

Pentru a edita o regulă, selectați-o și faceți clic pe **Modifică** sau faceți dublu-clic pe aceasta.Efectuați modificările necesare în fereastra de configurare.

Crearea regulilor Controlului de identitate

Pentru a crea o regulă de control al identității, faceți clic pe butonul corespunzător de **Blocare cuvânt cheie** și urmați pașii programului asistent.Puteți naviga prin programul asistent cu ajutorul butoanelor **Înainte** și **Înapoi**.Pentru a părăsi asistentul, faceți clic pe **Anulează**.

1. **Fereastra de întâmpinare**
2. **Furnizați tipul și argumentul regulei**

   Trebuie setați parametrii următori:

   - **Nume regulă** - introduceți numele regulii în acest câmp editabil.
   - **Tip regulă** - alegeți tipul regulei (adresă, nume, card de credit, PIN, etc.).
   - **Argument regulă** - introduceți datele pe care doriți să le protejați în acest câmp editabil.De exemplu, pentru a vă proteja numărul cardului dumneavoastră de credit, introduceți tot numărul sau doar o parte din el aici.

     Important
     Dacă introduceți mai puțin de trei caractere, vi se va solicita confirmarea acțiunii. Vă recomandăm să introduceți cel puțin trei caractere pentru a evita blocarea greșită a mesajelor și a paginilor web.

   Tot ceea ce introduceți este criptat. Pentru mai multă siguranță, nu introduceți întreaga dată pe care vreți să o protejați ci doar o parte a acesteia.
3. **Selectarea opțiunilor de scanare**

   Selectați tipul de trafic care doriți să fie scanat de BitDefender.

   - **Scanează web (trafic HTTP)** - scanează traficul HTTP (web) și blochează la ieșire toate datele ce corespund unei reguli.
   - **Scanează e-mail (trafic SMTP)** - scanează traficul SMTP (mail) și blochează trimiterea mesajelor e-mail care corespund unei reguli.
   - **Scanează MI (mesageria instant)** - scanează traficul de mesagerie instant și blochează trimiterea mesajelor instant care corespund unei reguli.

Puteți alege să aplicați regula doar dacă datele protejate apar ca șir independent sau ținând cont de majuscule și minuscule.

4. **Descrieți regula**

   Introduceți o scurtă descriere a regulei în câmpul editabil.Deoarece informația blocată (șirul respectiv de caractere) nu este afișată atunci când este accesată regula, descrierea trebuie să ajute la identificarea acesteia.

   Faceți clic pe **Finalizare**.Regula va apărea în tabel.

De acum înainte, orice încercare de a trimite datele specificate (prin e-mail, mesagerie instant sau prin intermediul unei pagini web) va eșua. Un mesaj de alertă va fi afișat indicând faptul că BitDefender a blocat transmiterea unor date personale.

19.1.5. Controlul mesageriei instant

Controlul mesageriei instant vă permite să specificați contactele de mesagerie instant cu care copiii dumneavoastră au voie să converseze.

Notă

Controlul mesageriei instant este disponibil doar pentru Yahoo Messenger și Windows Live (MSN) Messenger.

Pentru a configura Controlul mesageriei instant pentru un anumit cont de utilizator:

1. Accesați fereastra cu setările de Control parental BitDefender pentru respectivul cont de utilizator.
2. Faceți clic pe fila **Mesagerie**.
3. Utilizați selectorul pentru a activa Controlul mesageriei instant.
4. Selectați metoda preferată de filtrare și, în funcție de alegerea dumneavoastră, creați reguli corespunzătoare.

   - **Permite comunicarea prin mesageria instant cu excepția contactelor**

     În acest caz, trebuie să specificați utilizatorii de mesagerie instant care trebuie blocați (persoane cu care copilul dumneavoastră nu ar trebui să vorbească).

   - **Blochează comunicarea prin mesageria instant cu excepția contactelor**

     În acest caz, trebuie să specificați utilizatorii de mesagerie instant cu care copilul dumneavoastră are permisiunea directă de a vorbi folosind astfel de programe.De exemplu, puteți permite comunicarea prin mesageria instant cu membrii familiei, prietenii de la școală sau vecinii.

     Această a doua opțiune este recomandată pentru copiii cu vârsta sub 14 ani.

Crearea regulilor de Control al mesageriei instant

Pentru a permite sau bloca schimbul de mesaje instant cu un contact, urmați acești pași:

1. Faceți clic pe **Blochează ID IM** sau **Permite ID IM**.
2. Introduceți adresa de e-mail sau numele de utilizator folosit de contactul de mesagerie instant în câmpul **E-mail sau ID**.
3. Selectați programul de mesagerie instant asociat contactului.
4. Selectați acțiunea dorită pentru această regulă - **Permite** sau **Blochează**.
5. Faceți clic pe **Finalizează** pentru a adăuga regula.

Administrarea regulilor de Control al mesageriei instant

Regulile de Control al mesageriei instant sunt afișate în tabelul din partea inferioară a ferestrei.

Pentru a șterge o regulă, selectați-o și faceți clic pe **Șterge**.

Pentru a edita o regulă, selectați-o și faceți clic pe **Modifică** sau faceți dublu-clic pe aceasta.Efectuați modificările necesare în fereastra de configurare.

19.2. Monitorizarea activității copiilor

BitDefender vă permite să monitorizați activitățile pe calculator ale copiilor dumneavoastră, chiar și atunci când nu sunteți prezent.

În mod implicit, atunci când Controlul parental este activat, activitățile copiilor dumneavoastră sunt înregistrate în fișiere jurnal. În acest mod, puteți întotdeauna afla exact ce site-uri web au vizitat, ce aplicații au utilizat, ce activități au fost blocate de către funcția de Control parental etc.

Puteți de asemenea să configurați BitDefender pentru a vă transmite notificări prin e-mail atunci când funcția de Control parental blochează o activitate.

19.2.1. Verificarea jurnalelor de Control parental

Pentru a vedea activitățile recente ale copiilor dumneavoastră la calculator, accesați jurnalele de Control parental.Urmați acești pași:

1. Deschideți BitDefender.
2. Faceți clic pe linkul **Jurnale** din colțul dreapta jos al ferestrei.
3. Faceți clic pe **Control parental** în meniul din stânga.

Notă
De asemenea, puteți deschide aceste jurnale din fereastra de Control parental făcând clic pe **Jurnale**.

Dacă nu utilizați același calculator împreună cu copiii dumneavoastră, puteți configura rețeaua personală BitDefender pentru a putea accesa jurnalele de Control parental de la distanță (de pe calculatorul dumneavoastră).Pentru mai multe informații, consultați *„Rețea personală”* (p. 152).

Jurnalele de Control parental oferă informații detaliate despre activitățile de pe calculator și online ale copilului dumneavoastră.Informațiile sunt organizate în mai multe file:

General
Oferă informații generale despre activitățile recente ale copiilor dumneavoastră, cum ar fi cele mai vizitate site-uri web și cele mai utilizate aplicații.

Puteți filtra informațiile în funcție de utilizator și de perioada de timp.

Jurnal aplicații
Vă ajută să aflați ce aplicații au utilizat copiii dumneavoastră recent.

Faceți dublu-clic pe evenimentele din listă pentru a vedea mai multe detalii.Pentru a șterge un jurnal, faceți clic-dreapta pe acesta și selectați **Șterge**.

Jurnal Internet
Vă ajută să aflați ce site-uri web au vizitat copiii dumneavoastră recent.

Puteți filtra informațiile în funcție de utilizator și de perioada de timp.

Alte evenimente
Vă ajută să aflați informații detaliate despre activitatea de Control parental (de exemplu atunci când Controlul parental este activat/dezactivat, ce evenimente au fost blocate).

Faceți dublu-clic pe evenimentele din listă pentru a vedea mai multe detalii.Pentru a șterge un jurnal, faceți clic-dreapta pe acesta și selectați **Șterge**.

19.2.2. Configurarea notificărilor prin e-mail

Pentru a primi notificări prin e-mail atunci când funcția de Control parental blochează o anumită activitate:

1. Deschideți BitDefender.
2. În funcție de modul de vizualizare a interfeței, accesați setările Controlului parental după cum urmează:

   Modul Intermediar
   Mergeți la fila **Securitate** și faceți clic pe **Control parental** în zona de Sarcini rapide din partea stângă a ferestrei.

   Modul Expert
   Faceți clic pe **Control parental** în meniul din stânga.

Notă

În Modul Novice și Modul Intermediar de vizualizare, puteți configura o comandă rapidă pentru a putea accesa aceste setări din pagina de stare.Pentru mai multe informații, consultați *„Instrumentele mele”* (p. 33).

3. În secțiunea Setări, selectați **Vreau să primesc un raport de activitate prin e-mail**.
4. Vi se va solicita să configurați setările contului dumneavoastră de e-mail. Faceți clic pe **Da** pentru a deschide fereastra de configurare.

Notă

Puteți deschide fereastra de configurare, mai târziu, făcând clic pe **Setări notificări**.

5. Introduceți adresa de e-mail la care vor fi trimise notificările de e-mail.
6. Configurați setările e-mail ale serverului utilizat pentru a trimite notificări prin e-mail.

Există trei opțiuni pentru a vă configura setările de e-mail:

Folosiți setările actuale ale clientului de e-mail

Această opțiune este selectată în mod implicit atunci când BitDefender reușește să importe setările serverului de e-mail de la clientul dumneavoastră de e-mail.

Faceți clic pe **Testare setări** pentru a valida setările. Dacă în timpul validării sunt identificate anumite probleme, veți primi informații legate de modul de corectare a acestora.

Selectați unul dintre serverele cunoscute

Selectați această opțiune dacă aveți un cont de e-mail la unul dintre serviciile de e-mail oferite pe internet și afișate în listă.

Faceți clic pe **Testare setări** pentru a valida setările. Dacă în timpul validării sunt identificate anumite probleme, veți primi informații legate de modul de corectare a acestora.

Doresc să configurez personal setările serverului

Dacă știți setările serverului de e-mail, selectați această opțiune și configurați-le după cum urmează:

- **Server SMTP ieșire** - introduceți adresa serverului de mail folosit pentru trimiterea mesajelor e-mail.
- Dacă serverul utilizează un alt port decât cel implicit, portul 25, introduceți numărul acestuia în câmpul corespunzător.

- Dacă serverul necesită autentificare, selectați căsuța **Serverul SMTP necesită autentificare** și introduceți numele de utilizator și parola, în câmpurile corespunzătoare.

Faceți clic pe **Testare setări** pentru a valida setările. Dacă în timpul validării sunt identificate anumite probleme, veți primi informații legate de modul de corectare a acestora.

Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

19.3. Control parental la distanță

Controlul parental la distanță vă permite să monitorizați activitățile copiilor dumneavoastră și să modificați setările acestei funcții, chiar dacă nu vă aflați acasă.Tot ce vă trebuie este un calculator cu conexiune la internet și un browser web.

Controlul parental la distanță vă oferă o manieră discretă de a verifica activitățile online ale copiilor dumneavoastră, fără a deranja.

19.3.1. Condiții preliminare privind utilizarea Controlului parental la distanță

Pentru a utiliza funcția de Control parental la distanță, trebuie întrunite următoarele condiții preliminare:

1. Instalați fie BitDefender Internet Security 2011 sau BitDefender Total Security 2011 pe calculatorul copiilor dumneavoastră.
2. Activați produsul cu ajutorul unui cont BitDefender.
3. Activați Controlul parental la distanță.
4. Calculatorul de la care doriți să accesați Controlul parental la distanță trebuie să fie conectat la internet.

19.3.2. Activarea Controlului parental la distanță

Pentru a activa Controlul parental la distanță:

1. Conectați-vă la calculatorul pe care este instalat BitDefender utilizând un cont de administrator.Puteți utiliza același cont pe care l-ați utilizat pentru a instala programul.
2. Deschideți BitDefender.
3. În funcție de modul de vizualizare a interfeței, accesați setările Controlului parental după cum urmează:

Modul Intermediar

Mergeți la fila **Securitate** și faceți clic pe **Control parental** în zona de Sarcini rapide din partea stângă a ferestrei.

Modul Expert

Faceți clic pe **Control parental** în meniul din stânga.

Notă

În Modul Novice și Modul Intermediar de vizualizare, puteți configura o comandă rapidă pentru a putea accesa aceste setări din pagina de stare.Pentru mai multe informații, consultați *„Instrumentele mele”* (p. 33).

4. Utilizați selectorul pentru a activa controlul parental la distanță.Controlul parental la distanță va fi activat pentru toate conturile de utilizator din sistem.

19.3.3. Accesarea Controlului parental la distanță

Puteți accesa Controlul parental la distanță din contul dumneavoastră BitDefender.

1. Pe un calculator cu acces la internet, deschideți un browser și accesați:

   http://myaccount.bitdefender.com

2. Conectați-vă la contul dumneavoastră BitDefender cu ajutorul numelui de utilizator și al parolei.
3. Faceți clic pe fila **Control parental** pentru a accesa tabloul de comandă a controlului parental la distanță.
4. Puteți vedea toate conturile de utilizator pentru care este activată funcția de Control parental la distanță.

   Pentru a vedea ce activități au fost blocate pentru un anumit cont de utilizator de la ultima dumneavoastră conectare, faceți clic pe linkul ce indică alertele existente.

   Pentru a verifica activitățile recente ale copiilor dumneavoastră, faceți clic pe linkul **Activitate recentă** ce corespunde contului acestora.

   Pentru a modifica setările de Control parental pentru un anumit cont de utilizator, faceți clic pe linkul **Setări** corespunzător.

19.3.4. Monitorizarea activităților copiilor dumneavoastră de la distanță

Înainte de a putea monitoriza de la distanță activitățile de pe calculator și internet ale copiilor dumneavoastră, trebuie să activați funcția de Control parental la distanță pe calculatorul acestora.Pentru mai multe informații, consultați *„Activarea Controlului parental la distanță”* (p. 114).

Pentru a verifica de la distanță acțiunile copiilor dumneavoastră la calculator:

1. Pe un calculator cu acces la internet, deschideți un browser și accesați:

   http://myaccount.bitdefender.com

2. Conectați-vă la contul dumneavoastră BitDefender cu ajutorul numelui de utilizator și al parolei.
3. Faceți clic pe fila **Control parental** pentru a accesa tabloul de comandă a controlului parental la distanță.
4. Pentru a vedea ce activități au fost blocate pentru un anumit cont de utilizator de la ultima dumneavoastră conectare, faceți clic pe linkul ce indică alertele existente.Pentru a verifica activitățile recente ale copiilor dumneavoastră, faceți clic pe linkul **Activitate recentă** ce corespunde contului acestora.

De pe pagina de alerte, puteți afla ce site-uri web, aplicații sau contacte de mesagerie instant au fost blocate de la ultima dumneavoastră conectare.

Pe pagina de activități recente, puteți găsi informații utile despre activitățile recente ale copiilor dumneavoastră:

- care sunt cele mai accesate și cele mai blocate site-uri web.
- care sunt cele mai accesate și cele mai blocate aplicații.
- care sunt cele mai contactate și mai blocate contacte din mesageria instantanee.

Puteți bloca în mod direct un site web, o aplicație sau un contact de mesagerie instant făcând clic pe linkul **Blocare** corespunzător.

Pentru a elimina o restricție, faceți clic pe linkul **Permite** corespunzător.

19.3.5. Modificarea setărilor Controlului parental la distanță

Înainte de a putea modifica de la distanță setările de Control parental configurate pentru copiii dumneavoastră, trebuie să activați Controlul parental la distanță pe calculatorul acestora.Pentru mai multe informații, consultați *„Activarea Controlului parental la distanță”* (p. 114).

Pentru a modifica setările de Control parental la distanță:

1. Pe un calculator cu acces la internet, deschideți un browser și accesați:

   http://myaccount.bitdefender.com

2. Conectați-vă la contul dumneavoastră BitDefender cu ajutorul numelui de utilizator și al parolei.
3. Faceți clic pe fila **Control parental** pentru a accesa tabloul de comandă a controlului parental la distanță.

4. Puteți vedea toate conturile de utilizator pentru care este activată funcția de Control parental la distanță.Pentru a modifica setările de Control parental pentru un anumit cont de utilizator, faceți clic pe linkul **Setări** corespunzător.

Pagina de setări afișează site-urile web, aplicațiile și contactele de mesagerie instant care sunt blocate în mod explicit de către funcția de Control parental.Pentru a elimina o restricție, faceți clic pe linkul **Permite** corespunzător.

Pentru a afla cum puteți să stabiliți restricții, consultați aceste subiecte:

„Restricționarea accesului la internet în funcție de oră” (p. 117)
„Blocarea site-urilor web” (p. 117)
„Blocarea aplicațiilor” (p. 117)
„Blocarea contactelor din mesageria instantanee” (p. 118)

Restricționarea accesului la internet în funcție de oră

Alegeți o opțiune din meniu pentru a specifica momentul la care copilul dumneavoastră are permisiunea de accesa internetul.Pentru a restricționa accesul la internet la anumite ore din zi:

1. Selectați **Programarea accesului la internet**.
2. Selectați din grilă intervalele temporale în care accesul la internet este blocat.Puteți face clic pe celule individuale sau puteți face clic și trage pentru a acoperi perioade mai lungi de timp.Pentru a porni o nouă selecție, faceți clic pe **Blocare toate** sau **Acceptare toate**.
3. Faceți clic pe **Trimitere modificări**.Modificările vor fi configurate și aplicate pe calculatorul copilului dumneavoastră după următoarea sincronizare cu site-ul web al Controlului parental la distanță (în maxim 10 minute).

Blocarea site-urilor web

Pentru a bloca un website:

1. Faceți clic pe **Blocați un alt website**.
2. Introduceți site-ul web în câmpul corespunzător. Alternativ, dacă doriți să blocați unul dintre cele mai vizitate site-uri, selectați-l din meniu.
3. Faceți clic pe **Blocare**.Site-ul web va fi adăugat pe lista de site-uri blocate.Regula va fi configurată și aplicată pe calculatorul copilului dumneavoastră după următoarea sincronizare cu website-ul Controlului parental la distanță (în maxim 10 minute).

Dacă vă răzgândiți, faceți clic pe linkul **Permite** corespunzător.

Blocarea aplicațiilor

Pentru a bloca o aplicație:

1. Faceți clic pe **Blocarea unei alte aplicații**.
2. Selectați aplicația ce va fi blocată din lista cu cele mai accesate aplicații.
3. Faceți clic pe **Blocare**.Aplicația va fi adăugată listei de aplicații blocate.Regula va fi configurată și aplicată pe calculatorul copilului dumneavoastră după următoarea sincronizare cu website-ul Controlului parental la distanță (în maxim 10 minute).

Dacă vă răzgândiți, faceți clic pe linkul **Permite** corespunzător.

Blocarea contactelor din mesageria instantanee

Pentru a bloca mesajele instantanee cu un anumit contact:

1. Faceți clic pe **Blocarea unui alt contact**.
2. Introduceți contactul din mesageria instantanee în câmpul corespunzător. În mod alternativ, dacă doriți să blocați una dintre persoanele cele mai frecvent contactate prin intermediul mesageriei instantanee, selectați-o din meniu.
3. Faceți clic pe **Blocare**.Contactul din mesageria instantanee va fi adăugat în lista de contacte blocate.Regula va fi configurată și aplicată pe calculatorul copilului dumneavoastră după următoarea sincronizare cu website-ul Controlului parental la distanță (în maxim 10 minute).

Dacă vă răzgândiți, faceți clic pe linkul **Permite** corespunzător.

20. Control date

BitDefender monitorizează zeci de potențiale puncte sensibile ale sistemului de operare, acolo unde pot acționa aplicațiile spyware, și verifică orice schimbare apărută. Acest modul blochează în mod eficient caii troieni și alte instrumente instalate de hackeri, care încearcă să vă dezvăluie identitatea și să trimită informațiile personale, cum ar fi seria cărții de credit, din calculatorul dumneavoastră, către hacker.

Controlul datelor personale include aceste componente:

- Controlul identității - vă ajută să vă asigurați că informațiile dumneavoastră personale nu sunt transmise de pe calculator fără aprobarea dumneavoastră. Această funcție scanează e-mailurile și mesajele instantanee transmise de pe calculatorul dumneavoastră precum și orice date transmise prin intermediul paginilor de internet și blochează orice informație protejată cu ajutorul regulilor de Control al identității pe care le-ați creat.
- Controlul regiștrilor - vă cere permisiunea de fiecare dată când un program încearcă să modifice informațiile din regiștri astfel încât să fie lansat la pornirea Windows.
- Controlul fișierelor cookie - vă cere permisiunea de fiecare dată când un site încearcă să seteze un cookie.
- Controlul scripturilor - vă cere permisiunea de fiecare dată când un domeniu încearcă să ruleze un script sau alt conținut activ.

În mod implicit, numai funcția de control a identității este activată.Trebuie să configurați reguli adecvate pentru Controlul identității pentru a preveni trimiterea neautorizată de informații confidențiale.Pentru mai multe informații, consultați *„Configurarea Controlului identității”* (p. 122).

Celelalte componente ale funcției de Control a datelor personale sunt interactive. Dacă le activați, vi se va solicita, prin intermediul unor ferestre de alertă, să permiteți sau să blocați anumite acțiuni atunci când vizitați site-uri web noi sau instalați un program nou. De aceea, aceste componente sunt utilizate de obicei de utilizatori avansați.

20.1. Configurarea nivelului de protecție

Nivelul de protecție vă ajută să activați sau să dezactivați cu ușurință componentele funcției de Control al datelor personale.

Pentru a configura nivelul de protecție:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Control date personale > Stare**.

3. Asigurați-vă că funcția de control parental este activată.
4. Există două opțiuni:
   - Trageți de cursor de-a lungul scalei pentru a seta nivelul de protecție corespunzător.Faceți clic pe **Nivel implicit** pentru a seta cursorul la nivelul implicit.

     Utilizați descrierea din partea dreaptă a scalei pentru a selecta nivelul de protecție care se potrivește mai bine nevoilor dumneavoastră de securitate.
   - Puteți personaliza nivelul de protecție făcând clic pe **Nivel personal**.În fereastra care va apărea, selectați controalele de protecție pe care doriți să le activați și faceți clic pe **OK**.

20.2. Control identitate

Controlul identității vă protejează împotriva furtului de date confidențiale atunci când sunteți online.

Luați în considerare un exemplu simplu: ați creat o regulă de controlare a identității care vă protejează numărul cardului de credit.Dacă un program spion reușește să se instaleze pe calculatorul dumneavoastră, acesta nu poate trimite numărul cardului dumneavoastră de credit prin e-mail, mesaje instantanee sau pagini web. Mai mult, copiii dumneavoastră nu îl pot utiliza pentru achiziții online și nu îl pot dezvălui persoanelor pe care le întâlnesc pe internet.

Pentru a afla mai multe, consultați aceste subiecte:

- *„Despre Controlul identității”* (p. 120).
- *„Configurarea Controlului identității”* (p. 122).
- *„Administrarea regulilor”* (p. 124).

20.2.1. Despre Controlul identității

Păstrarea datelor confidențiale în siguranță este o problemă importantă ce ne preocupă pe toți. Furtul de date a ținut pasul cu dezvoltarea comunicațiilor pe Internet și se folosește de noi metode de a păcăli oamenii să cedeze informațiile private.

Fie că este vorba de adresa e-mail sau de numărul cărții de credit, dacă acestea ajung în mâinile unor persoane nepotrivite vă pot aduce daune: puteți să vă treziți că aveți contul de mail plin de spam sau să constatați cu surprindere că aveți contul bancar golit.

Controlul identității vă protejează împotriva furtului de date confidențiale atunci când sunteți online.Pe baza regulilor create de dumneavoastră, Controlul identității scanează traficul web, e-mail sau de mesagerie instant care iese din calculatorul dumneavoastră în căutare de șiruri de caractere specifice (de exemplu, numărul

cardului dumneavoastră de credit). Dacă există o concordanță, site-ul web, e-mailul sau mesajul instant respectiv este blocat.

Puteți crea reguli pentru a proteja orice informație pe care o considerați personală sau confidențială, de la numărul dumneavoastră de telefon sau adresa dumneavoastră de e-mail până la informațiile referitoare la contul dumneavoastră bancar.Este oferit suport pentru mai mulți utilizatori, astfel încât utilizatorii care folosesc alte conturi de utilizator Windows să poată configura și folosi propriile reguli de protecție a identității.Dacă aveți un cont Windows de administrator, regulile pe care le creați pot fi configurate să se aplica și atunci când alți utilizatori ai calculatorului sunt conectați la conturile lor Windows.

De ce să folosiți Controlul identității?

- Controlul identității este foarte eficient în blocarea aplicațiilor spyware keylogger.Acest tip de aplicații periculoase înregistrează tot ceea ce tastați și trimite aceste înregistrări prin internet către o persoană rău intenționată (un hacker).Hackerul poate afla din datele furate informații confidențiale, cum ar fi parole și numere de conturi bancare, pe care le va folosi în beneficiul propriu.

  În eventualitatea în care o astfel de aplicație reușește să evite detecția antivirus, aceasta nu va putea trimite datele furate prin e-mail, web sau mesaje instant, dacă ați creat reguli adecvate de protecție a identității.

- Controlul identității vă poate proteja împotriva tentativelor de phishing (încercări de a fura informații personale).Cele mai frecvente tentative de phishing utilizează un e-mail înșelător pentru a vă convinge să trimiteți informatii personale prin intermediul unei pagini web false.

  De exemplu, puteți primi un e-mail care pare a fi trimis de banca dumneavoastră și care vă solicită să actualizați urgent informațiile de cont bancar.E-mailul conține un link către o pagină web unde trebuie să furnizați informațiile personale.Deși par a fi legitime, e-mailul și pagina web spre care vă trimite linkul înșelător sunt false.Dacă faceți clic pe linkul din e-mail și trimiteți informațiile dumneavoastră personale de pe pagina web falsă, veți dezvălui aceste informații persoanelor răuvoitoare care au organizat înșelătoria.

  Dacă ați creat reguli adecvate de protecție a identității, nu veți putea trimite informații personale (cum ar fi numărul cărții de credit) de pe o pagină web decât dacă ați definit în mod explicit o excepție pentru pagina web respectivă.

- Cu ajutorul regulilor de Control al identității, îi puteți împiedica pe copiii dumneavoastră să dezvăluie informații personale (cum ar fi adresa de acasă sau numărul de telefon) persoanelor pe care le cunosc pe internet. Mai mult, în cazul în care creați reguli în scopul protejării cardului dumneavoastră de credit, aceste persoane nu îl pot utiliza pentru a utiliza obiecte online fără consimțământul dumneavoastră.

20.2.2. Configurarea Controlului identității

Dacă doriți să utilizați Controlul identității, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Control date personale > Identitate**.
3. Asigurați-vă că funcția de control al identității este activată.

Notă
În cazul în care opțiunea nu poate fi configurată, mergeți la fila **Status** și activați funcția de Control parental.

4. Creați reguli pentru a vă proteja datele confidențiale.Pentru mai multe informații, consultați *„Crearea regulilor Protecției identității”* (p. 122).
5. Daca este nevoie, stabiliți anumite excepții la regulile pe care le-ați creat.De exemplu dacă ați creat o regulă pentru a vă proteja numărul cardului de credit, adăugați site-urile web unde utilizați de obicei cardul de credit la lista de excepții.Pentru mai multe informații, consultați *„Definirea excepțiilor”* (p. 123).

Crearea regulilor Protecției identității

Pentru a crea o regulă de protecție a identității, faceți clic pe butonul **Adaugă** și urmați pașii programului asistent.Puteți naviga prin programul asistent cu ajutorul butoanelor **Înainte** și **Înapoi**.Pentru a părăsi asistentul, faceți clic pe **Anulează**.

1. **Fereastra de întâmpinare**
2. **Furnizați tipul și argumentul regulei**

   Trebuie setați parametrii următori:

   - **Nume regulă** - introduceți numele regulii în acest câmp editabil.
   - **Tip regulă** - alegeți tipul regulei (adresă, nume, card de credit, PIN, etc.).
   - **Argument regulă** - introduceți datele pe care doriți să le protejați în acest câmp editabil.De exemplu, pentru a vă proteja numărul cardului dumneavoastră de credit, introduceți tot numărul sau doar o parte din el aici.

Important
Dacă introduceți mai puțin de trei caractere, vi se va solicita confirmarea acțiunii. Vă recomandăm să introduceți cel puțin trei caractere pentru a evita blocarea greșită a mesajelor și a paginilor web.

Tot ceea ce introduceți este criptat. Pentru mai multă siguranță, nu introduceți întreaga dată pe care vreți să o protejați ci doar o parte a acesteia.

3. **Selectați tipurile de trafic și utilizatorii**

   a. Selectați tipul de trafic care doriți să fie scanat de BitDefender.

   - **Scanează web (trafic HTTP)** - scanează traficul HTTP (web) și blochează la ieșire toate datele ce corespund unei reguli.
   - **Scanează e-mail (trafic SMTP)** - scanează traficul SMTP (mail) și blochează trimiterea mesajelor e-mail care corespund unei reguli.
   - **Scanează MI (mesageria instant)** - scanează traficul de mesagerie instant și blochează trimiterea mesajelor instant care corespund unei reguli.

   Puteți alege să aplicați regula doar dacă datele protejate apar ca șir independent sau ținând cont de majuscule și minuscule.

   b. Preciyați utilizatorii cărora li se aplica regula.

   - **Numai mie (utilizator curent)** - regula se va aplica numai contului dvs de utilizator.
   - **Conturi utilizatori cu drepturi limitate** - regula se va aplica numai dvs și tuturor conturilor Windows cu drepturi limitate.
   - **Toți utilizatorii** - regula se va aplica tuturor conturilor Windows.

4. **Descrieți regula**

   Introduceți o scurtă descriere a regulei în câmpul editabil.Deoarece informația blocată (șirul respectiv de caractere) nu este afișată atunci când este accesată regula, descrierea trebuie să ajute la identificarea acesteia.

   Faceți clic pe **Finalizare**.Regula va apărea în tabel.

De acum înainte, orice încercare de a trimite datele specificate (prin e-mail, mesagerie instant sau prin intermediul unei pagini web) va eșua. Un mesaj de alertă va fi afișat indicând faptul că BitDefender a blocat transmiterea unor date personale.

Definirea excepțiilor

În unele cazuri, este nevoie să definiți excepții pentru anumite reguli de identitate.Considerați cazul în care creați o regulă de identitate care împiedică trimiterea numărului cardului dumneavoastră de credit prin HTTP (pe web). De fiecare dată când acesta este trimis pe o pagină web de pe contul dumneavoastră de utilizator, pagina respectivă este blocată. Dacă doriți, de exemplu, să cumpărați o pereche de pantofi prin intermediul unui magazin online (care știți că este securizat), va trebui să specificați o excepție de la regula respectivă.

Pentru a deschide fereastra în care puteți administra excepțiile, faceți clic pe **Excluderi**.

Pentru a adăuga o excepție, urmați acești pași:

1. Faceți clic pe butonul **Adaugă** pentru a adăuga o nouă înregistrare în tabel.

2. Faceți dublu-clic pe **Specificați obiectul exclus** și introduceți site-ul web, adresa de e-mail sau contactul de mesagerie instant care doriți să fie adăugate ca excepție.
3. Faceți dublu-clic pe **Tip de trafic** și alegeți din meniu opțiunea corespunzătoare tipului de adresă furnizată anterior.
   - Dacă ați specificat o adresă web, selectați **HTTP**.
   - Dacă ați specificat o adresă de e-mail, selectați **E-mail (SMTP)**.
   - Dacă ați specificat un contact IM, selectați **IM**.

Pentru a șterge o excepție de pe listă, selectațiol și faceți clic pe butonul **Șterge**.

Faceți clic pe **OK** pentru a salva modificările.

20.2.3. Administrarea regulilor

Pentru a administra regulile privind Controlul identității:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Control date personale > Identitate**.

Puteți vedea listate în tabel regulile create până în momentul de față.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.

Pentru a modifica atributele unei reguli, selectați-o și faceți clic pe butonul **Editează** sau faceți dublu-clic pe ea. Va apărea o nouă fereastră.Aici puteți modifica numele, descrierea și parametrii regulei (tip, argument și trafic). Faceți clic pe **OK** pentru a salva modificările.

20.3. Control regiștri

Una dintre părțile importante ale sistemului de operare Windows sunt **regiștrii**. Aici își păstrează Windows configurația și setările, programele instalate, informații despre utilizator și alte date.

Tot în **regiștri** sunt definite programele care sunt lansate la pornirea Windows. Virușii folosesc des această caracteristică Windows pentru a se lansa automat atunci când utilizatorul își repornește calculatorul.

Controlul Regiștrilor supraveghează regiștrii Windows – în acest fel BitDefender poate detecta troienii. BitDefender vă va alerta de fiecare dată când un program încearcă să modifice informațiile din regiștri astfel încât să fie lansat la pornirea Windows.Pentru mai multe informații, consultați *„Alerte regiștri”* (p. 40).

Pentru a configura Controlul registrului:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.

2. Mergeți la **Control date personale > Regiștri**.
3. Selectați căsuța corespunzătoare pentru a activa Controlul regiștrilor.

Notă
În cazul în care opțiunea nu poate fi configurată, mergeți la fila **Status** și activați funcția de Control parental.

Administrarea regulilor

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.

20.4. Controlul fișierelor cookie

Fișierele cookie sunt foarte comune pe Internet. Ele sunt fișiere mici salvate pe calculatorul dumneavoastră. Paginile web creează aceste fișiere pentru a vă monitoriza activitatea pe Internet și a salva informații specifice despre dumneavoastră.

În general, fișierele cookie vă fac viața mai ușoară. De exemplu ele ajută site-urile să vă rețină numele și preferințele, pentru a nu trebui să le introduceți la fiecare vizită.

Dar ele pot fi folosite și pentru a vă compromite intimitatea, urmărindu-vă obiceiurile de navigare pe Internet.

Aici vă va fi util controlul fișierelor cookie.Atunci când este activat, controlul fișierelor cookie vă va solicita permisiunea de fiecare dată când un site încearcă să seteze sau să ceara un cookie.Pentru mai multe informații, consultați *„Alerte fișiere cookie”* (p. 41).

Pentru a configura Controlul cookie:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Control date personale > Cookie**.
3. Bifați căsuța corespunzătoare pentru a activa Controlul cookie.

Notă
În cazul în care opțiunea nu poate fi configurată, mergeți la fila **Status** și activați funcția de Control parental.

4. Puteți configura reguli pentru site-urile web pe care le vizitați de obicei, însă nu este neapărat necesar.Regulile sunt create automat prin fereastra de alertă, pe baza răspunsului dumneavoastră.

Notă
Din cauza numărului mare de fișiere cookie de pe Internet, **Controlul fișierelor cookie** poate fi la început. Inițial, vă va pune foarte multe întrebări despre pagini web care încearcă să seteze cookie-uri pe calculatorul dumneavoastră. După ce adăugați paginile web pe care le folosiți frecvent în lista de reguli, navigarea va deveni la fel de ușoară ca la început.

Crearea manuală a regulilor

Pentru a crea o regulă manual, faceți clic pe butonul **Adaugă** și configurați parametrii regulii în fereastra de configurare.Puteți seta parametrii:

- **Domeniu** - introduceți adresa domeniului pentru care este creată regula.
- **Acțiune** - selectați acțiunea regulei.

Acțiune	Descriere
Permite	Fișierele cookie ale domeniul respectiv vor fi acceptate.
Interzice	Fișierele cookie ale domeniului respectiv vor fi blocate.

- **Direcție** - selectați direcția traficului.

Tip	Descriere
La ieșire	Regula se aplică numai fișierelor cookie trimise înapoi către siteul de la care au pornit.
La intrare	Regula se aplică numai fișierelor cookie recepționate.
Ambele	Regula se va aplica în ambele direcții.

Notă
Puteți accepta fișiere cookie fără a le returna: setați acțiunea **Interzice** și direcția **La ieșire**.

Faceți clic pe **Finalizare**.

Administrarea regulilor

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.Pentru a modifica parametrii regulii, selectați regula și faceți clic sau dublu-clic pe butonul **Editează**. Efectuați modificările dorite în fereastra de configurare.

20.5. Control scripturi

Scripturile și alte coduri cum ar fi elementele ActiveX și Applet-urile Java, care sunt folosite pentru a crea pagini web, pot fi programate astfel încât să aibă efecte

dăunătoare. Elemente de tipul ActiveX, de exemplu, pot avea în întregime acces la datele dumneavoastră și le pot citi sau șterge de pe calculatorul dumneavoastră, pot captura parole și intercepta mesaje cât timp sunteți conectați la Internet. Este recomandat să acceptați conținutul activ doar de la paginile web pe care le cunoașteți foarte bine și care sunt de încredere.

În cazul în care activați Controlul scripturilor, vi se va solicita permisiunea de fiecare dată când un nou website încearcă să ruleze un script sau alt conținut activ.Pentru mai multe informații, consultați *„Alerte de scripturi”* (p. 41).

Pentru a configura Controlul scripturilor:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Control date personale > Script**.
3. Selectați căsuța corespunzătoare pentru a activa Controlul scripturilor.

   Notă
   În cazul în care opțiunea nu poate fi configurată, mergeți la fila **Status** și activați funcția de Control parental.

4. Puteți configura reguli pentru site-urile web pe care le vizitați de obicei, însă nu este neapărat necesar.Regulile sunt create automat prin fereastra de alertă, pe baza răspunsului dumneavoastră.

Crearea manuală a regulilor

Pentru a crea o regulă manual, faceți clic pe butonul **Adaugă** și configurați parametrii regulii în fereastra de configurare.Puteți seta parametrii:

- **Domeniu** - introduceți adresa domeniului pentru care este creată regula.
- **Acțiune** - selectați acțiunea regulei.

Acțiune	Descriere
Permite	Rularea scripturilor este permisă.
Interzice	Rularea scripturilor este interzisă.

Faceți clic pe **Finalizare**.

Administrarea regulilor

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Șterge**.Pentru a modifica parametrii regulii, selectați regula și faceți clic sau dublu-clic pe butonul **Editează**. Efectuați modificările dorite în fereastra de configurare.

21. Firewall

Modulul Firewall vă protejează calculatorul de tentative de conexiune neautorizată la ieșire sau la intrare. Modulul este asemănător unui paznic – supraveghează conexiunea la Internet și monitorizează aplicațiile cărora le este permis accesul la Internet precum și pe cele care trebuie blocate.

Notă
În cazul unei conexiuni prin cablu sau DSL este esențial să aveți un firewall.

În Modul ascuns calculatorul este “ascuns” de aplicațiile malițioase sau de hackeri. Modulul Firewall este capabil să detecteze automat scanări de porturi (pachete trimise către o mașină pentru a găsi puncte de acces, adesea pregătind un atac) și să protejeze calculatorul împotriva acestora.

21.1. Setări de protecție

Pentru a activa/dezactiva și configura protecția firewall, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar
Mergeți la fila **Securitate** și faceți clic pe **Configurare firewall** în zona Sarcini rapide din partea stângă a ferestrei.Selectați fila **Setări** din noua fereastră care apare.

Modul Expert
Mergeți la **Firewall > Setări**.

Important
Pentru a fi protejat de atacuri de pe Internet păstrați modulul**Firewall**activat.

În partea superioară a acestei secțiuni, puteți vizualiza diferite statistici legate de activitatea identificată.

În partea de jos a secțiunii puteți vizualiza statisticile BitDefender referitoare la traficul la intrare și la ieșire. Graficul arată volumul traficului internet în ultimele două minute.

Notă
Graficul este afișat numai în Modul Expert de vizualizare.

21.1.1. Setarea acțiunii implicite

În mod implicit, BitDefender permite automat tuturor programelor din lista de programe cunoscute să acceseze rețeaua și Internetul.Pentru toate celelalte

programe, BitDefender vă va solicita prin intermediul unei ferestre de alertă să specificați acțiunea care să fie aplicată.Acțiunea specificată este aplicată de fiecare dată când respectiva aplicație necesită acces la rețea sau Internet.

Notă

To view the BitDefender white list, click the corresponding button located in the **Settings** tab in Expert View or the **Programs** tab in Intermediate View.

Puteți muta cursorul pentru a seta acțiunea implicită care să fie luată asupra aplicațiilor care necesită acces la rețea sau Internet.

- Permite toate
- Permite cunoscute
- Rapoarte
- Interzice toate

Atunci când selectați o acțiune, este afișată o scurtă descriere a acesteia.

21.1.2. Configurarea setărilor avansate de firewall

În Modul Expert de vizualizare, puteți configura setările avansate de firewall făcând clic pe **Setări avansate**.

Următoarele opțiuni sunt disponibile:

- **Activează suportul pentru Internet Connection Sharing(ICS)** - activează suportul pentru Internet Connection Sharing(ICS).

  Notă

  Această opțiune nu activează automat ICS pe sistemul dumneavoastră ci doar permite acest tip de conexiune în cazul în care o activați din sistemul de operare.

- **Detectează aplicațiile care s-au modificat de la crearea regulii de firewall** - verifică fiecare aplicație care încearcă să se conecteze la Internet pentru a vedea dacă aceasta a fost modificată de la adăugarea regulii care îi controlează accesul la Internet. Dacă aplicația a fost modificată, va fi afișată o alertă prin care vi se va cere să permiteți sau să blocați accesul aplicației la Internet.

  Notă

  Aplicațiile pot suferi modificări produse de malware.Vă recomandăm să țineți această opțiune selectată și să permiteți accesul doar acelor aplicații care vă așteptați să fi fost modificate după ce a fost creată regula care le controlează accesul.

  Aplicațiile semnate sunt presupuse a fi sigure și au un grad sporit de securitate.Puteți selecta **Ignoră modificările aplicațiilor cu semnătură digitală**

pentru a permite aplicațiilor semnate și modificate să se conecteze la Internet fără ca dvs sa primiți vreo alertă în legătură cu acest eveniment.

- **Afișează notificări wireless** - dacă sunteți conectat la o rețea fără fir (wireless), afișează ferestre informative privind anumite evenimente din rețea (de exemplu, când un calculator nou s-a conectat la rețea).
- **Blochează scanările de porturi** - detectează și blochează tentativele de a descoperi care porturi sunt deschise.

  Scanările de porturi sunt folosite în mod frecvent de hackeri pentru a detecta porturi deschise pe calculatorul dumneavoastră.Dacă este detectat un port vulnerabil, aceștia pot pătrunde în calculatorul dumneavoastră.
- **Activează reguli automate stricte** - creează reguli stricte prin intermediul ferestrei de alertă de firewall.Fiind selectată această opțiune, BitDefender vă va solicita să alegeți acțiunea și va crea reguli pentru fiecare proces diferit care deschide aplicația care necesită acces la rețea sau Internet.

21.2. Reguli privind accesul la aplicații

Pentru a administra regulile de firewall ce controlează accesul aplicațiilor la resurse din rețea și internet, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar

Mergeți la fila **Securitate** și faceți clic pe **Configurare firewall** în zona Sarcini rapide din partea stângă a ferestrei.Selectați fila **Programe** din noua fereastră care apare.

Modul Expert

Mergeți la **Firewall > Programe**.

Modul Intermediar de vizualizare vă oferă acces la setări de configurare de bază. Pentru a avea mai multe opțiuni de personalizare, utilizați Modul Expert de vizualizare.

21.2.1. Se vizualizează regulile curente

Puteți vedea în tabel programele (procesele) pentru care au fost create reguli firewall.

În Modul Expert de vizualizare, puteți afla informații detaliate despre fiecare regulă, conform celor indicate în coloanele tabelului.Pentru a vedea regulile create pentru o anumită aplicație, faceți clic pe căsuța cu + de lângă aplicația respectivă.Debifați căsuța **Ascunde regulile de sistem** pentru a vedea și regulile referitoare la procesele de sistem sau la cele ale BitDefender.

- **Proces/Tipuri rețea** - procesul și tipul de adaptor de rețea cărora li se aplică regula.Regulile sunt create automat pentru a filtra accesul la rețea sau Internet prin oricare adaptor.Pentru a filtra accesul aplicațiilor la rețea și Internet printr-un

anumit adaptor (de exemplu, printr-un adaptor de rețea wireless), puteți crea reguli manual sau puteți edita regulile existente.

- **Linie de comandă** - comanda utilizată în linia de comandă a Windows (**cmd**) pentru a porni procesul.
- **Protocol** - protocolul IP căruia i se aplică regula.Puteți vedea unul dintre următoarele protocoale:

Protocol	Descriere
Oricare	Include toate protocoalele IP.
TCP	TCP, acronimul pentru Transmission Control Protocol, permite stabilirea unei conexiuni si schimbul de date intre 2 sisteme. TCP garantează livrarea de date si primirea pachetelor trimise in aceeași ordine în care au fost expediate.
UDP	UDP, acronimul pentru User Datagram Protocol, este un protocol bazat pe IP, proiectat pentru performanțe ridicate. Jocurile și alte aplicații video folosesc adesea acest protocol.
Un număr	Reprezintă un anumit protocol IP (altul decât TCP și UDP).Puteți găsi lista completă a numerelor atribuite protocoalelor IP la adresa www.iana.org/assignments/protocol-numbers.

- **Evenimente rețea** - evenimentele de rețea căruia i se aplică regula.Pot fi luate în considerare următoarele evenimente:

Eveniment	Descriere
Conectare	Schimb preliminar de mesaje standard utilizate în cadrul protocoalelor orientate pe conexiune pentru a stabili o conexiune.În cazul protocoalelor orientate pe conexiune, traficul de date dintre două calculatoare apare numai după ce a fost stabilită conexiunea.
Trafic	Schimb de date dintre două calculatoare.
Ascultă	Stare în care o aplicație monitorizează rețeaua așteptând stabilirea unei conexiuni sau recepționarea unor informații de la o aplicație parteneră.

- **Porturi locale** - porturile de pe calculatorul dumneavoastră cărora li se aplică regula.
- **Porturi la distanță** - porturile de pe calculatorul la distanță cărora li se aplică regula.
- **Local** - dacă regula se aplică doar calculatoarelor din rețeaua locală.

- **Acțiune** - dacă aplicației îi este permis accesul la rețea sau Internet în circumstanțele date.

21.2.2. Adăugarea automată a regulilor

Având funcția **Firewall** activată, BitDefender monitorizează toate aplicațiile și creează în mod automat o regulă de fiecare dată când o aplicație încearcă să se conecteze la internet.În funcție de aplicație și de setările firewallului BitDefender, aceasta se realizează cu sau fără intervenția dumneavoastră.

Dacă utilizați Modul Novice sau Modul Intermediar de vizualizare, încercările de conectare venite din partea unor aplicații necunoscute vor fi blocate în mod automat.

În cazul în care utilizați Modul Expert de vizualizare, vi se va solicita să alegeți o anumită acțiune, prin intermediul unei ferestre de alertă, ori de câte ori o aplicație necunoscută încearcă să se conecteze la internet.

Puteți vedea aplicația care încearcă să acceseze internetul, calea către aceasta, destinația, protocolul utilizat și portul prin care aplicația încearcă să se conecteze.

Faceți clic pe **Permite** pentru a permite tot traficul (la intrare și la ieșire) generat de această aplicație de pe calculatorul local către orice destinație, prin protocolul IP respectiv și pe toate porturile. Dacă faceți clic pe **Blochează**, va fi refuzat complet accesul aplicației la Internet prin protocolul IP respectiv.

Important

Permiteți tentative de conectare la intrare doar de la adrese IP sau domenii în care aveți încredere.

Pe baza răspunsului dumneavoastră, va fi creată o regulă, care va fi aplicată și listată în tabel. Data viitoare când aplicația va încerca să se conecteze, această regulă va fi aplicată implicit.

21.2.3. Adăugarea manuală a regulilor

Crearea manuală de reguli diferă în funcție de modul de vizualizare a interfeței pe care îl utilizați.

Modul Intermediar

1. Faceți clic pe **Răsfoire** din **Adăugare nou program**.
2. Localizați programul pentru care doriți să creați o regulă și faceți clic pe **Deschidere**.
3. Faceți clic pe **Adăugare regulă**.

   Puteți observa că regula este afișată acum în tabel.
4. Selectați o acțiune din coloana **Acțiune**: permiteți sau interziceți accesul.

   Acțiunea va fi aplicată în cazul tuturor parametrilor regulilor.

Modul Expert

1. Faceți clic pe butonul **Adăugare regulă**.Va apărea fereastra de configurare.
2. Configurați parametrii principali și pe cei avansați, după cum este nevoie.
3. Faceți clic pe **OK** pentru a adăuga regula.

Regulile pot fi modificate numai la configurarea firewallului în Modul Expert de vizualizare.Pentru a modifica o regulă existentă, urmați acești pași:

1. Faceți clic pe butonul **Editare regulă** sau faceți dublu-clic pe regulă.Va apărea fereastra de configurare.
2. Configurați parametrii principali și pe cei avansați, după cum este nevoie.
3. Faceți clic pe **OK** pentru a salva modificările.

Configurarea parametrilor principali

Tabul **Principal** al ferestrei de configurare permite configurarea parametrilor principali ai regulii.

Puteți configura următorii parametri:

- **Cale program.** Faceți clic pe **Caută** și selectați aplicația căreia i se aplică regula.Dacă doriți care regula să fie aplicată tuturor aplicațiilor, selectați **Oricare**.
- **Linie de comandă.** Dacă doriți ca regula să fie aplicată doar atunci când aplicația selectată este deschisă cu o anumită comandă în linia de comandă Windows, debifați căsuța **Oricare** și introduceți respectiva comandă în câmpul corespunzător.
- **Protocol.** Selectați din meniu protocolul IP căruia i se aplică regula.
  - Dacă doriți ca regula să fie aplicată tuturor protocoalelor, selectați **Oricare**.
  - Dacă doriți ca regula să fie aplicată pentru TCP, selectați **TCP**.
  - Dacă doriți ca regula să fie aplicată pentru UDP, selectați **UDP**.
  - Dacă doriți ca regula să fie aplicată unui anumit protocol, selectați **Altul**.Va apărea un câmp editabil.Introduceți în câmpul editabil numărul atribuit protocolului care doriți să fie filtrat

    Notă

    Numerele protocoalelor IP sunt atribuite de către Internet Assigned Numbers Authority (IANA).Puteți găsi lista completă a numerelor atribuite protocoalelor IP la adresa www.iana.org/assignments/protocol-numbers.

- **Evenimente.** În funcție de protocolul selectat, alegeți evenimentele de rețea cărora li se aplică regula.Pot fi luate în considerare următoarele evenimente:

Eveniment	Descriere
Conectare	Schimb preliminar de mesaje standard utilizate în cadrul protocoalelor orientate pe conexiune pentru a stabili o conexiune.În cazul protocoalelor orientate pe conexiune, traficul de date dintre două calculatoare apare numai după ce a fost stabilită conexiunea.
Trafic	Schimb de date dintre două calculatoare.
Ascultă	Stare în care o aplicație monitorizează rețeaua așteptând stabilirea unei conexiuni sau recepționarea unor informații de la o aplicație parteneră.

- **Tipuri de adaptoare.** Selectați tipurile de adaptoare cărora li se aplică regula.
- **Acțiune.** Selectați una dintre acțiunile disponibile:

Acțiune	Descriere
Permite	Aplicației specificate îi va fi permis accesul la rețea / Internet în condițiile specificate.
Interzice	Aplicației specificate îi va fi refuzat accesul la rețea / Internet în condițiile specificate.

Configurarea parametrilor avansați

Tabul **Avansat** al ferestrei de configurare permite configurarea parametrilor avansați ai regulii.

Puteți configura următorii parametri avansați:

- **Direcție.** Selectați din meniu direcția traficului căreia i se aplică regula.

Direcție	Descriere
La ieșire	Regula nu se va aplica decât pentru traficul la ieșire.
La intrare	Regula nu se aplica decât pentru traficul la intrare.
Ambele	Regula se va aplica în ambele direcții.

- **Versiune IP.** Selectați din meniu versiunea IP (IPv4, IPv6 sau ambele) căreia i se aplică regula.
- **Adresa locală.** Specificați adresa IP locală și portul local cărora li se aplică regula după cum urmează:
  - Dacă aveți mai multe adaptoare de rețea, puteți debifa căsuța **Oricare** și introduce o anumită adresă IP.

- Dacă ați selectat TCP sau UDP ca protocol puteți seta un port specific sau o valoare între 0 și 65535. Dacă doriți ca regula să se aplice tuturor porturilor selectați **Oricare**.

- **Adresa la distanță.** Specificați adresa IP și portul la distanță cărora li se aplică regula după cum urmează:
  - Pentru a filtra traficul dintre calculatorul dumneavoastră și un anumit calculator, debifați căsuța **Oricare** și introduceți adresa IP a acestuia.
  - Dacă ați selectat TCP sau UDP ca protocol puteți seta un port specific sau o valoare între 0 și 65535. Dacă doriți ca regula să se aplice tuturor porturilor selectați **Oricare**.
- **Aplică această regulă doar calculatoarelor direct conectate.** Selectați această opțiune dacă doriți ca regula să fie aplicată doar tentativelor de trafic locale.
- **Verifică procesul părinte al evenimentului original.** Puteți modifica acest parametru doar dacă ați selectat **Reguli automate stricte** (mergeți la tabul Setări și faceți clic pe **Setări avansate**).Reguli stricte înseamnă că BitDefender vă va solicita să alegeți acțiunea când o aplicație necesită acces la rețea sau Internet de fiecare dată când procesul părinte este diferit.

21.2.4. Adminstrarea avansată a regulilor

Dacă trebuie să vizualizați și să editați în detaliu regulile ce controlează aplicațiile, faceți clic pe butonul **Avansat** disponibil la configurarea firewallului în Modul Expert de vizualizare.

Puteți vedea regulile firewall listate în ordinea în care sunt aplicate.Tabelul furnizează informații complete despre fiecare regulă.

Notă

Atunci când are loc o tentativă de conexiune (la intrare sau la ieșire), BitDefender aplică acțiunea primei reguli care îndeplinește condițiile conexiunii respective.Din acest motiv, ordinea în care sunt verificate aceste reguli este foarte importantă.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Ștergere regulă**.

Pentru a modifica o regulă existentă, selectați-o și faceți clic pe butonul **Editare regulă** sau faceți dublu-clic pe aceasta.

Puteți schimba prioritatea unei reguli. Faceți clic pe butonul **Mută cu un nivel mai sus în listă** pentru a mări prioritatea regulei selectate cu un nivel, sau pe butonul **Mută cu un nivel mai jos în listă** pentru a scădea prioritatea regulei selectate cu un nivel.Pentru a atribui unei reguli prioritatea maximă, faceți clic pe butonul **Mută prima**. Pentru a atribui unei reguli prioritatea minimă, faceți clic pe butonul **Mută ultima**.

Faceți clic pe **Închide** pentru a închide fereastra.

21.2.5. Ștergerea și resetarea regulilor

Ștergerea și resetarea regulilor este posibilă numai atunci când configurați firewallul în Modul Expert de vizualizare.

Pentru a șterge o regulă, selectați-o și faceți clic pe butonul **Ștergere regulă**.Puteți selecta și șterge mai multe reguli deodată.

Dacă doriți să ștergeți toate regulile create pentru o anumită aplicație, selectați aplicația din listă și faceți clic pe butonul **Ștergere regulă**.

Dacă doriți să încărcați setul implicit de reguli stabilit pentru nivelul de încredere selectat, faceți clic pe **Resetare Reguli**.

21.3. Setări rețea

Pentru a configura setările conexiunii de rețea, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar
: Mergeți la fila **Securitate** și faceți clic pe **Configurare firewall** în zona Sarcini rapide din partea stângă a ferestrei. Selectați fila **Rețea** din fereastra care apare.

Modul Expert
: Mergeți la **Firewall > rețea**.

Coloanele din tabelul de **Configurare a rețelei** oferă informații detaliate despre rețeaua la care sunteți conectat și vă permite să configurați setările conexiunii:

- **Adaptor** - placa de rețea folosită pentru conectarea la rețea sau la Internet.
- **Tipul de rețea** - tipul de rețea la care se conectează adaptorul.În funcție de configurația adaptorului de rețea, BitDefender poate selecta în mod automat un tip de rețea sau vă va solicita informații suplimentare.

  Modificați tipul făcând clic pe săgeata ▾ din coloana **Tipul de rețea** și selectând unul dintre tipurile disponibile din listă.

Tip rețea	Descriere
Securizate (Permitere toate)	Dezactivează firewallul pentru adaptorul respectiv.
Acasă/Birou	Permite tot traficul dintre calculatorul dumneavoastră și calculatoarele din rețeaua locală.
Public	Tot traficul este filtrat.

Tip rețea	Descriere
Nesecurizate (Blocare toate)	Blochează complet traficul de rețea și Internet prin adaptorul respectiv.

- **VPN** - în cazul în care conexiunea se face la o rețea privată virtuală.

  Traficul care trece prin conexiunile VPN este filtrat în mod diferit față de cel care trece prin alte conexiuni de rețea.În cazul în care conexiunea dumneavoastră este VPN, faceți clic pe săgeata ▾ din coloana **VPN** și selectați **Da**.

În Modul Expert de vizualizare, sunt afișate două coloane suplimentare:

- **Modul Ascuns** - dacă puteți fi detectat de alte calculatoare.

  Pentru a configura modul ascuns, faceți clic pe săgeata ▾ din coloana **Mod ascuns** și selectați opțiunea dorită.

Opțiune	Descriere
activat	Modul ascuns este activat.Calculatorul dumneavoastră nu poate fi detectat nici din rețeaua locală, nici de pe Internet.
Dezactivat	Modul ascuns este dezactivat.Oricine din rețeaua locală sau de pe Internet poate da ping și detecta calculatorul dumneavoastră.
La distanță	Calculatorul dumneavoastră nu poate fi detectat din Internet.Utilizatorii din rețeaua locală pot da ping și detecta calculatorul dumneavoastră.

- **Generic** - dacă sunt aplicate reguli generice pentru această conexiune.

  Dacă se schimbă adresa IP a unui adaptor de rețea, BitDefender va modifica automat și tipul de rețea.Dacă doriți să mențineți același tip, faceți clic pe săgeata ▾ din coloana **Generic** și selectați **Da**.

21.3.1. Zone de rețea

Puteți adăuga calculatoare blocate sau permise pentru un anumit adaptor.

O zonă de încredere este un calculator în care aveți deplină încredere.Tot traficul dintre calculatorul dumneavoastră și un calculator de încredere este permis.Pentru a putea partaja resurse cu calculatoare din rețele fără fir (wireless) nesecurizate, adăugați-le ca fiind calculatoare permise.

O zonă blocată este un calculator care nu doriți să poată comunica sub nicio formă cu calculatorul dumneavoastră.

Tabelul cu **Zonele rețelei** afișează zonele curente ale rețelei pentru fiecare adaptor în parte.

Pentru a adăuga o zonă, selectați adaptorul și faceți clic pe **Adăugare zonă**.Va apărea o nouă fereastră.

Procedați astfel:

1. Selectați adresa IP a calculatorului pe care doriți să îl adăugați.
2. Selectați acțiunea:
   - **Permite** - pentru a permite tot traficul dintre calculatorul dumneavoastră și calculatorul selectat.
   - **Blochează** - pentru a bloca tot traficul dintre calculatorul dumneavoastră și calculatorul selectat.
3. Faceți clic pe **OK**.

21.4. Dispozitive

Pentru a gestiona dispozitivele conectate la rețea, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar
: Mergeți la fila **Securitate** și faceți clic pe **Configurare firewall** în zona Sarcini rapide din partea stângă a ferestrei.Selectați fila **Dispozitive** din noua fereastră care apare.

Modul Expert
: Mergeți la **Firewall > dispozitive**.

Imprimantele, faxurile și scanerele detectate în rețea și acțiunile implicite setate pentru acestea sunt listate în tabel.Pentru a modifica starea unui dispozitiv, faceți dublu-clic pe acesta în tabel și selectați o acțiune din fereastra care va apărea: permiteți sau blocați comunicațiile cu dispozitivul.

Utilizați butoanele disponibile pentru a administra lista de dispozitive:

- **Adăugare** - adăugați un dispozitiv care nu apare în listă.
- **Eliminare** - eliminați un dispozitiv selectat dintr-o listă.
- **Reîmprospătare dispozitive** - initiați o nouă scanare a rețelei pentru a actualiza lista de dispozitive.

21.5. Control conexiuni

Pentru a monitoriza activitatea actuală din rețea/internet (în TCP și UDP) organizată în funcție de aplicație și pentru a deschide jurnalul de firewall BitDefender, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Firewall > Activitate**.

Puteți vedea traficul total, sortat după aplicație. Pentru fiecare aplicație, puteți vedea conexiunile și porturile deschise, precum și statistici referitoare la viteza traficului la intrare & ieșire și cantitatea de date trimise / primite.

Dacă doriți să vedeți și procesele inactive, debifați căsuța **Ascunde procesele inactive**.

Sensul iconițelor este după cum urmează:

- Indică o conexiune la ieșire.
- Indică o conexiune la intrare.
- Indică un port deschis pe calculatorul dumneavoastră.

Fereastra prezintă, în timp real, activitatea curentă pe rețea / Internet. Pe măsură ce sunt închise conexiuni și porturi, statisticile corespunzătoare acestora dispar treptat.Același lucru se întâmplă tuturor statisticilor unei aplicații care generează trafic sau are porturi deschise atunci când o închideți.

Pentru o listă completă a evenimentelor referitoare la activitatea modulului Firewall (activare/dezactivare firewall, blocare trafic, modificare setări) sau generate de activitățile detectate de firewall (scanare de porturi, blocare tentative de conectare sau trafic conform regulilor), accesați fișierul jurnal al BitDefender Firewall făcând clic pe **Afișare jurnal**.Fișierul este localizat în directorul Common Files al utilizatorului Windows curent, la adresa: `...BitDefender\BitDefender Firewall\bdfirewall.txt`.

Dacă doriți ca jurnalul să conțină mai multe informații, selectați opțiunea **Mai multe informații**.

21.6. Depanarea firewallului

În cazul în care vă confruntați cu o problemă care considerați că este cauzată de firewallul BitDefender, aveți la dispoziție asistentul de depanare care vă va ajuta să o soluționați.

Pentru a porni programul asistent, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar
: Mergeți la fila **Securitate** și faceți clic pe **Configurare firewall** în zona Sarcini rapide din partea stângă a ferestrei.Selectați fila **Setări** din fereastra care apare și faceți clic pe **Depanare**.

Modul Expert
: Mergeți la **Firewall > Setări** și faceți clic pe **Depanare**.

Programul asistent vă va ajuta să rezolvați rapid următoarele probleme de conectivitate asociate cu configurarea firewall:

- Încerc să imprim, dar acțiunea eșuează.
- Încerc să accesez un calculator din rețeaua proprie, dar acțiunea eșuează.
- Încerc să obțin acces la internet, dar acțiunea eșuează.

Dacă niciuna dintre situațiile descrise nu descrie problema cu care vă confruntați, selectați **Altă problemă firewall** pentru a deschide fereastra **Instrument de asistență**.

Pentru mai multe informații referitoare la acest asistent, consultați secțiunea de Depanare din acest ghid

22. Vulnerabilitate

Un pas important în protejarea calculatorului dumneavoastră împotriva persoanelor răuvoitoare și a aplicațiilor malițioase este de a menține actualizat sistemul de operare și aplicațiile pe care le utilizați în mod regulat.De asemenea, pentru a preveni accesul fizic neautorizat la calculatorul dumneavoastră, trebuie configurate parole puternice (parole care nu pot fi ghicite cu ușurință) pentru fiecare cont de utilizator Windows.

BitDefender verifică în mod regulat sistemul dumneavoastră în căutare de vulnerabilități și vă informează despre problemele existente.

22.1. Căutare după vulnerabilități

Puteți căuta punctele vulnerabile și le puteți remedia pas cu pas cu ajutorul asistentului de **Scanare a vulnerabilității**.Pentru a porni programul asistent, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar
: Mergeți la fila **Securitate** și faceți clic pe **Vulnerabilități** în zona de Sarcini rapide din partea stângă a ferestrei.

Modul Expert
: Mergeți la **Vulnerabilitate > Status** și faceți clic pe **Verificați acum**.

Urmați procedura de ghidare cu șase pași pentru a îndepărta punctele vulnerabile din sistem.Puteți naviga prin programul asistent utilizând butonul **Înainte**. Pentru a părăsi asistentul, faceți clic pe **Anulează**.

1. **Protejați-vă calculatorul!**

   Selectați vulnerabilitățile de verificat

2. **Scanarea aspectelor selectate...**

   Așteptați ca BitDefender să finalizeze verificarea sistemului dumneavoastră în sensul descoperirii vulnerabilităților.

3. **Actualizări Windows**

   Puteți vedea lista actualizărilor critice și normale pentru Windows care nu sunt instalate pe calculatorul dumneavoastră.Selectați actualizările pe care doriți să le instalați.

4. **Actualizări aplicații**

   Dacă o aplicație nu este la zi, faceți clic pe linkul furnizat pentru a descărca ultima versiune a acesteia.

5. **Parole slabe**

Puteti vedea lista conturilor de utilizator Windows configurate pe calculatorul dumneavoastră și de nivelul de protecție asigurat de parola acestora.Faceți clic pe **Remediază** pentru a modifica parolele slabe.

6. **Rezumat**

   Aici puteți vedea rezultatul operației.

22.2. Stare

Pentru a vizualiza starea actuală a vulnerabilității și pentru a activa/dezactiva scanarea automată a vulnerabilității, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Vulnerabilități > Stare**.

În tabel sunt afișate problemele identificate în timpul ultimei verificări a gradului de vulnerabilitate și stadiul acestora.Puteți vedea acțiunea pe care trebuie s-o aplicați pentru a remedia fiecare vulnerabilitate, dacă este cazul. Dacă se indică **Nicio acțiune**, atunci respectiva problemă nu reprezintă o vulnerabilitate.

Important
Pentru a fi informat automat despre vulnerabilitățile sistemului sau aplicațiilor dumneavoastră, mențineți **Scanarea automată a vulnerabilităților** activată.

În funcție de problemă, pentru a remedia o anumită vulnerabilitate, procedați după cum urmează:

- Dacă sunt disponibile actualizări Windows, faceți clic pe **Instalează** în coloana **Acțiune** pentru a le instala.
- Dacă o aplicație este neactualizată, faceți clic pe **Mai multe informații** pentru a vizualiza informațiile despre versiune și pentru a găsi un link la pagina de internet a furnizorului de unde puteți instala cea mai recentă versiune a respectivei aplicații.
- Dacă un cont de utilizator Windows are o parolă slabă, faceți clic pe **Vizualizare & Remediere**, pentru a forța utilizatorul să o modifice la următoarea conectare sau schimbați-o chiar dvs.Pentru a crea o parolă puternică, utilizați o combinație de litere mari și mici, numere și caractere speciale (cum ar fi #, $ sau @).
- În cazul în care funcția de redare automată a suporturilor media este activată în Windows, faceți clic pe **Fix** pentru a o dezactiva.

22.3. Opțiuni

Pentru a configura setările de verificare automată a vulnerabilității, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Vulnerabilități > Setări**.
3. Selectați căsuțele corespunzătoare vulnerabilităților care să fie verificate în mod regulat.
   - **Actualizări Windows critice**
   - **Actualizări Windows obișnuite**
   - **Actualizări aplicații**
   - **Parole slabe**
   - **Rulare automată**

Notă

Dacă debifați căsuța corespunzătoare unei anumite vulnerabilități, BitDefender nu vă va mai avertiza despre problemele asociate.

23. Criptare chat

Conținutul mesajelor dumneavoastră instantanee trebuie să rămână doar între dumneavoastră și partenerul dumneavoastră de chat.Prin criptarea conversațiilor, vă puteți asigura că oricine încearcă să le intercepteze atunci când le primiți sau le transmiteți contactelor nu poate citi conținutul acestora.

În mod implicit, BitDefender criptează toate sesiunile dumneavoastră de chat prin mesagerie instant cu condiția ca:

- Partenerul dumneavoastră de chat are instalată o versiune de BitDefender care suportă criptarea mesageriei instant (IM), iar Criptarea IM este activată pentru aplicația de mesagerie instant folosită pentru chat.
- Atât dumneavoastră, cât si partenerul dumneavoastră de chat, să utilizați fie Yahoo Messenger, fie Windows Live (MSN) Messenger.

Important
BitDefender nu va cripta o conversație dacă un partener de chat folosește o aplicație web pentru chat, cum ar fi Meebo, sau dacă un partenere folosește Yahoo!, iar celălalt Windows Live (MSN).

Pentru a configura criptarea mesageriei instantanee:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Criptare > Criptare chat**.

Notă
Puteți configura cu ușurință criptarea mesageriei instantanee pentru fiecare partener de chat utilizând bara de instrumente BitDefender din fereastra de chat.

Implicit, criptarea mesageriei instant este activată atât pentru Yahoo Messenger, cât și pentru Windows Live (MSN) Messenger.Puteți alege să dezactivați complet criptarea mesageriei instant sau doar pentru o anumită aplicație de chat.

Sunt afișate două tabele:

- **Excluderi criptare** - afișează id-urile de utilizator și programul de mesagerie instant (IM) asociat pentru care criptarea este dezactivată.Pentru a șterge un contact din listă, selectați-l și faceți clic pe butonul **Șterge**.
- **Conexiuni curente** - afișează conexiunile de mesagerie instant curente (ID utilizator și program IM asociat) și dacă aceste conexiuni sunt criptate sau nu.O conexiune poate să nu fie criptată din următoarele motive:
  - Ați dezactivat în mod explicit criptarea pentru contactul respectiv.

▶ Contactul dumneavoastră nu are instalată o versiune de BitDefender care oferă criptare IM.

23.1. Dezactivarea criptării pentru anumiți utilizatori

Pentru a dezactiva criptarea pentru un anumit utilizator, urmați acești pași:

1. Faceți clic pe butonul **Adăugare** pentru a deschide fereastra de configurare.
2. Introduceți în câmpul editabil ID-ul utilizatorului.
3. Selectați aplicația de mesagerie instant asociată contactului.
4. Faceți clic pe **OK**.

23.2. Bara de instrumente BitDefender din fereastra de chat

Puteți configura ușor criptarea mesageriei instant folosind bara de comenzi BitDefender din fereastra de chat.

Bara de comenzi se găsește în mod normal în colțul din dreapta-jos al ferestrei de chat. Uitați-vă după logo-ul BitDefender pentru a o găsi.

Notă
Bara de comenzi arată când o conversație este criptată prin afișarea unei cheițe lângă logo-ul BitDefender.

Făcând clic pe bara de comenzi BitDefender, vă sunt oferite următoarele opțiuni:

- **Dezactivează permanent criptarea pentru contact.**
- **Invită pe contact să utilizeze criptarea.** Pentru a cripta conversația, contactul dumneavoastră trebuie să instaleze BitDefender și să utilizeze un program de mesagerie instant compatibil.
- **Adaugă pe contact în lista neagră a controlului parental.** Dacă adăugați un contact în lista neagră a controlului parental și controlul parental este activat, nu veți mai vedea mesajele instant trimise de contactul respectiv.Pentru a elimina contactul din lista neagră, faceți clic pe bara de comenzi și selectați **Elimină pe contact din lista neagră a controlului parental**.

24. Modul pentru jocuri / laptop

Modul pentru jocuri / laptop vă permite să configurați modurile de funcționare speciale ale BitDefender:

- Modul pentru jocuri modifică temporar setările produsului pentru a minimiza impactul acestora asupra performanței sistemului.
- Modul pentru laptop blochează executarea sarcinilor planificate atunci când laptopul funcționează pe baterie pentru a nu accelera consumarea acesteia.
- Modul silențios modifică temporar setările produsului pentru a reduce întreruperile în timpul vizionării unor filme sau prezentări.

24.1. Modul pentru jocuri

Modul pentru jocuri modifică temporar setările produsului pentru a minimiza impactul acestora asupra performanței sistemului.Cât timp modul pentru jocuri este activat, se aplică următoarele setări:

- Toate alertele și pop-upurile BitDefender sunt dezactivate.
- Nivelul protecției în timp real BitDefender este setat pe **Permisiv**.
- Firewallul BitDefender este setat pe **Permite tot**.Aceasta înseamnă că toate conexiunile noi (atât la intrare cât și la ieșire) sunt permise în mod automat, indiferent de portul și protocolul utilizat.
- Actualizările nu sunt efectuate în mod implicit.

Notă
Pentru a modifica această setare, mergeți la Actualizare>Setări și debifați căsuța **Nu actualiza dacă este activat modul pentru jocuri**.

În mod implicit, BitDefender intră automat în modul pentru jocuri când porniți un joc din lista de jocuri cunoscute a BitDefender sau când o aplicație ocupă întreg ecranul (fullscreen).Puteți intra manual în modul pentru jocuri utilizând combinația de taste implicită `Ctrl+Alt+Shift+G`.Este recomandat să ieșiți din modul pentru jocuri atunci când ați terminat jocul (puteți utiliza aceeași combinația de taste implicită `Ctrl+Alt+Shift+G`).

Notă
Cât timp modul pentru jocuri este activat, puteți vedea litera G pe iconița BitDefender.

Pentru a configura Modul joc:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.

2. Mergeți la **Mod joc/laptop > Mod joc**.

În partea de sus a secțiunii, puteți vedea starea modului pentru jocuri.Puteți face clic pe **Modul joc este activat** sau **Modul joc este dezactivat** pentru a modifica starea actuală.

24.1.1. Configurarea modului pentru jocuri automat

Modul pentru jocuri automat permite BitDefender să intre automat în modul pentru jocuri atunci când este detectat un joc.Puteți configura următoarele opțiuni:

- **Utilizează lista de jocuri furnizată de BitDefender** - pentru a intra automat în modul pentru jocuri când porniți un joc din lista de jocuri cunoscute a BitDefender.Pentru a vedea această listă, faceți clic pe **Administrare jocuri** și apoi pe **Listă jocuri**.
- **Acțiune pe întreg ecranul** - puteți alege să accesați Modul joc sau Modul silențios atunci când o aplicație este afișată pe întreg ecranul.
- **Întreabă dacă aplicația afișată pe întregul ecran trebuie adăugată pe lista de jocuri** - pentru a vi se solicita adăugarea unei noi aplicații pe lista de jocuri atunci când aceasta iese din modul ecran întreg.La pornirea unei noi aplicații adăugate pe lista de jocuri, BitDefender va intra automat în modul pentru jocuri.

Notă
Dacă nu doriți ca BitDefender să intre automat în modul pentru jocuri, debifați căsuța **Modul automat pentru jocuri este activat**.

24.1.2. Administrarea listei de jocuri

BitDefender intră automat în modul pentru jocuri atunci când porniți o aplicație din lista de jocuri.Pentru a vedea și administra lista de jocuri, faceți clic pe **Administrare jocuri**.Va apărea o nouă fereastră.

Noi aplicații sunt adăugate în această listă când:

- Porniți un joc de pe lista de jocuri cunoscute a BitDefender.Pentru a vedea această listă, faceți clic pe **Listă jocuri**.
- După ieșirea din full screen, adăugați aplicația în lista de jocuri prin intermediul ferestrei de alertă.

Dacă doriți să dezactivați modul automat pentru jocuri pentru o anumită aplicație din listă, debifați căsuța corespunzătoare acesteia.Puteți dezactiva modul automat pentru jocuri pentru aplicații normale care intră în full screen, cum ar fi browserele web și programele de vizionat filme.

Pentru a administra lista de jocuri, puteți utiliza butoanele plasate în partea de sus a tabelului:

- **Adăugare** - adăugați o nouă aplicație pe lista de jocuri.

- **Eliminare** - eliminați o aplicație de pe lista de jocuri.
- **Editare** - editați un element existent de pe lista de jocuri.

24.1.3. Adăugarea sau editarea jocurilor

Atunci când adăugați sau editați o înregistrare din lista de jocuri, va apărea o nouă fereastră.

Faceți clic pe **Caută** pentru a selecta aplicația sau introduceți calea completă către aplicație în câmpul editabil.

Dacă nu doriți ca BitDefender să intre automat în modul pentru jocuri atunci când aplicația selectată este pornită, selectați **Dezactivează**.

Faceți clic pe **OK** pentru a adăuga înregistrarea în lista de jocuri.

24.1.4. Configurarea setărilor modului pentru jocuri

Pentru a configura executarea sarcinilor programate, utilizați aceste opțiuni:

- **Activează acest modul pentru modificarea programelor sarcinilor de scanare antivirus** - pentru a împiedica rularea sarcinilor de scanare programate când Modul pentru jocuri este activat.Puteți selecta una dintre următoarele opțiuni:

Opțiune	Descriere
Sări peste sarcină	Sarcina programată nu este executată deloc.
Amână sarcina	Execută sarcina imediat după ieșirea din modul pentru jocuri.

Pentru a dezactiva automat firewallul BitDefender în modul pentru jocuri, urmați acești pași:

1. Faceți clic pe **Setări avansate**.Va apărea o nouă fereastră.
2. Selectați căsuța **Setează Firewall la Permite tot (Mod pentru jocuri) când este activat Modul pentru jocuri**.
3. Faceți clic pe **OK** pentru a salva modificările.

24.1.5. Schimbarea combinației de taste

Puteți să accesați manual Modul joc utilizând setarea implicităCtrl+Alt+Shift+Gtasta rapidă.Pentru a schimba combinația de taste, urmați acești pași:

1. Faceți clic pe **Setări avansate**.Va apărea o nouă fereastră.
2. Sub opțiunea **Utilizează combinația de taste**, setați combinația de taste dorită:

- Bifați tastele speciale pe care doriți să le folosiți: tasta Control (`Ctrl`), tasta Shift (`Shift`) sau tasta Alternate (`Alt`).
- În câmpul editabil, tastați litera corespunzătoare tastei normale pe care doriți să o folosiți.

De exemplu, dacă doriți să folosiți combinația de taste `Ctrl+Alt+D`, trebuie să bifați doar `Ctrl` și `Alt` și să tastați `D`.

Notă
Debifarea căsuței corespunzătoare opțiunii **Utilizați combinația de taste** va dezactiva combinația de taste.

3. Faceți clic pe **OK** pentru a salva modificările.

24.2. Modul pentru laptop

Modul pentru laptop este creat special pentru utilizatorii de laptopuri. Scopul acestuia este să minimizeze impactul pe care îl are BitDefender asupra consumului bateriei atunci când aceste dispozitive funcționează pe baterie.

În modul pentru laptop, sarcinile programate nu sunt executate în mod implicit.

BitDefender detectează când laptopul dumneavoastră a trecut pe baterie și intră automat în modul pentru laptop.De asemenea, BitDefender iese automat din modul pentru laptop, atunci când detectează că laptopul nu mai funcționează pe baterie.

Pentru configurarea Modului laptop:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Mod joc/laptop > Mod laptop**.

Puteți vedea dacă modul pentru laptop este activat sau nu.Dacă modul pentru laptop este activat, BitDefender va aplica setările configurate atunci când laptopul funcționează pe baterie.

24.2.1. Configurarea setărilor modului pentru laptop

Pentru a configura executarea sarcinilor programate, utilizați aceste opțiuni:

- **Activează acest modul pentru modificarea programelor sarcinilor de scanare antivirus** - pentru a împiedica rularea sarcinilor de scanare programate când Modul pentru laptop este activat.Puteți selecta una dintre următoarele opțiuni:

Opțiune	Descriere
Sări peste sarcină	Sarcina programată nu este executată deloc.

Opțiune	Descriere
Amână sarcina	Execută sarcina imediat după ieșirea din modul pentru laptop.

24.3. Mod silențios

Modul silențios modifică temporar setările de protecție pentru a minimiza impactul acestora asupra performanței sistemului.Cât timp modul silențios este activat, se aplică următoarele setări:

- Toate alertele și pop-upurile BitDefender sunt dezactivate.
- Firewallul BitDefender este setat pe **Permite tot**.Aceasta înseamnă că toate conexiunile noi (atât la intrare cât și la ieșire) sunt permise în mod automat, indiferent de portul și protocolul utilizat.
- Sarcinile de scanare programate sunt dezactivate în mod implicit.

În mod implicit, BitDefender intră în mod automat în Modul silențios atunci când urmăriți un film sau o prezentare sau când o aplicație este vizualizată pe întreg ecranul. Se recomandă să părăsiți Modul silențios după ce ați terminat de vizionat un film sau o prezentare.

Notă
Atunci când Modul silențios este activat, veți observa o modificare a iconiței BitDefender aflate lângă ceasul de pe calculatorul dumneavoastră.

Pentru a configura Modul silențios:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Mod joc/laptop > Mod silențios**.

În partea de sus a secțiunii, puteți vedea starea modului silențios.Puteți face clic pe **Modul silențios este activat** sau **Modul silențios este dezactivat** pentru a modifica starea actuală.

24.3.1. Configurarea acțiunii pe întreg ecranul

Puteți configura următoarele opțiuni:

- **Acțiune pe întreg ecranul** - puteți alege să accesați Modul joc sau Modul silențios atunci când o aplicație este afișată pe întreg ecranul.

Notă
Dacă nu doriți ca BitDefender să intre automat în modul silențios, debifați căsuța **Acțiune pe întreg ecranul**.

24.3.2. Configurarea setărilor modului silențios

Pentru a configura executarea sarcinilor programate, utilizați aceste opțiuni:

- **Activează acest modul pentru modificarea programelor sarcinilor de scanare antivirus** - pentru a împiedica rularea sarcinilor de scanare programate când Silent Mode este activat.Puteți selecta una dintre următoarele opțiuni:

Opțiune	Descriere
Sări peste sarcină	Sarcina programată nu este executată deloc.
Amână sarcina	Executați sarcina programată imediat după ieșirea din Modul silențios.

25. Rețea personală

Modulul Rețea vă permite să administrați produsele BitDefender instalate pe calculatoarele personale de pe un singur calculator.Pentru a accesa modulul Rețea personală, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar
Mergeți la fila **Rețea**.

Modul Expert
Selectați **Rețea personală**.

Notă
De asemenea, puteți adăuga o comandă rapidă în Instrumentele mele.

Pentru a putea administra produsele BitDefender instalate pe calculatoarele personale, trebuie să urmați acești pași:

1. Activați rețeaua BitDefender personală pe calculatorul dumneavoastră.Setați calculatorul ca Server.
2. Mergeți la fiecare calculator pe care doriți să-l administrați și intrați în rețea (setați parola).Setați fiecare computer ca normal.
3. Întoarceți-vă la calculatorul dumneavoastră și adăugați calculatoarele pe care doriți să le administrați.

25.1. Activarea rețelei BitDefender

Pentru a activa rețeaua personală BitDefender, urmați acești pași:

1. Faceți clic pe **Activare rețea**.Vi se va cere să configurați parola rețelei personale.
2. Introduceți aceeași parolă în ambele câmpuri editabile.
3. Setați rolul calculatorului în rețeaua personală BitDefender:
   - **Calculator server** - selectați această opțiune pe calculatorul care va fi utilizat pentru a administra toate celelalte calculatoare.
   - **Calculator normal** - selectați această opțiune pe calculatoarele care vor fi administrate de către calculatorul server.
4. Faceți clic pe **OK**.

Puteți vedea numele calculatorului apărând pe harta rețelei.

Apare butonul **Dezactivare rețea**.

25.2. Adăugarea calculatoarelor la rețeaua BitDefender

Orice computer va fi adăugat în mod automat la rețea dacă întrunește următoarele criterii:

- rețeaua personală BitDefender a fost activată pe acesta.
- rolul a fost setat la calculator normal.
- parola stabilită la activarea rețelei este identică cu parola setată pe calculatorul server.

Notă

În Modul Expert de vizualizare, puteți scana oricând rețeaua personală pentru a descoperi dacă respectivele computere întrunesc criteriile făcând clic pe butonul **Identificare automată**.

Pentru a adăuga manual un calculator la rețeaua personală BitDefender de pe calculatorul server, urmați acești pași:

1. Faceți clic pe **Adaugă calculator**.
2. Introduceți parola de administrare a rețelei și faceți clic pe **OK**.Va apărea o nouă fereastră.

   Puteți vedea lista calculatoarelor din rețea.Sensul iconițelor este după cum urmează:

   Indică un calculator online fără niciun produs BitDefender instalat.

   Indică un calculator online cu BitDefender instalat.

   Indică un calculator închis cu BitDefender instalat.
3. Puteți proceda astfel:
   - Selectați din listă numele calculatorului pe care doriți să îl adăugați.
   - Introduceți în câmpul corespunzător adresa IP sau numele calculatorului pe care doriți să îl adăugați.
4. Faceți clic pe **Adaugă**.Vi se va cere să introduceți parola de administrare a rețelei personale configurată pe calculatorul respectiv.
5. Introduceți parola de administrare a rețelei personale configurată pe calculatorul respectiv.
6. Faceți clic pe **OK**.Dacă ați furnizat parola corectă, numele calculatorului selectat va apărea pe harta rețelei.

25.3. Administrarea rețelei BitDefender

O dată ce ați creat o rețea BitDefender personală, puteți administra toate produsele BitDefender de pe un singur calculator.

Dacă plasați cursorul mouse-ului deasupra unui calculator de pe harta rețelei, puteți vedea informații sumare despre acesta (nume, adresă IP, numărul de probleme care afectează securitatea sistemului, starea înregistrării).

Dacă faceți clic pe numele unui calculator de pe harta rețelei, puteți vedea toate sarcinile administrative pe care le puteți rula de la distanță pe calculatorul respectiv.

- **Înregistrează BitDefender pe acest calculator**

  Vă permite să înregistrați BitDefender pe acest calculator, prin introducerea unei serii de înregistrare.

- **Stabilește o parola pentru setări pe un calculator la distanță**

  Vă permite să creați o parolă pentru a restricționa accesul la setările BitDefender pe acest calculator.

- **Execută o sarcină de scanare la cerere**

  Vă permite să executați o scanare la cerere pe calculatorul la distanță. Aveți posibilitatea să efectuați oricare din următoarele sarcini de scanare: Scanare My Documents, scanare de sistem sau scanare profundă de sistem.

- **Remediază toate problemele de pe acest calculator**

  Vă permite să rezolvați problemele care afectează securitatea acestui calculator, urmând pașii programului asistent Remediază probleme.

- **Vizualizare istoric/evenimente**

  Vă permite să accesați modulul **Istoric&Evenimente** al produsului BitDefender instalat pe acest calculator.

- **Actualizează**

  Inițiază procesul de Actualizare a produsului BitDefender instalat pe acest calculator.

- **Setează profilul de control parental**

  Vă permite să stabiliți categoria de vârstă care va fi folosită de filtrul web al modulului Control Parental pe acest calculator.

- **Stabilește acest calculator ca server de actualizare al acestei rețele**

  Vă permite să setați acest calculator ca server de actualizare pentru toate produsele BitDefender instalate pe calculatoarele din aceasta rețea.Prin folosirea acestei opțiuni, se va reduce traficul pe internet, pentru că numai un calculator din rețea se va conecta la internet pentru a descărca actualizări.

- **Scoate calculatorul din rețeaua personală**

  Vă permite să scoateți un calculator din rețea.

Atunci când interfața BitDefender se află în Modul Intermediar de vizualizare, puteți rula mai multe sarcini pe toate computerele administrate în același timp făcând clic pe butoanele corespunzătoare.

- **Scanează tot** - vă permite să scanați toate calculatoarele administrate în același timp.
- **Actualizează tot** - vă permite să actualizați toate calculatoarele administrate în același timp.
- **Înregistrează tot** - vă permite să înregistrați toate calculatoarele administrate în același timp.

Înainte de a executa o sarcină pe un anumit calculator, vi se va cere să furnizați parola locală de administrare a rețelei.Introduceți parola de administrare a rețelei și faceți clic pe **OK**.

Notă

Dacă doriți să executați mai multe sarcini, puteți bifa **Nu mă mai avertiza în sesiunea curentă**.Selectând această opțiune, nu vi se va mai cere să introduceți această parolă în sesiunea curentă.

26. Actualizare

În fiecare zi sunt descoperite și identificate noi programe periculoase (malware). De aceea, este foarte importantă actualizarea BitDefender cu ultimele semnături malware.

Dacă sunteți conectat la Internet, prin bandă largă sau ADSL, BitDefender se ocupă singur de actualizări. Implicit, BitDefender caută actualizări când deschideți calculatorul și apoi la fiecare **oră**.

Dacă o actualizare este disponibilă, vi se va cere să confirmați actualizarea sau aceasta va fi realizată automat, în funcție de setările de actualizare automată.

Procesul de actualizare este realizat progresiv, ceea ce înseamnă că fișierele care trebuie actualizate sunt înlocuite unul câte unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.

Important
Pentru a fi protejat împotriva celor mai noi amenințări, mențineți **Actualizarea automată** activată.

Actualizările sunt de mai multe tipuri:

- **Actualizări pentru motoarele Antivirus** - pentru că apar tot timpul noi viruși, fișierele care conțin semnăturile de viruși trebuie actualizate pentru a asigura protecție permanentă, la zi, împotriva acestora. Acest tip de actualizare mai este cunoscut și ca **actualizarea semnăturilor de viruși**.
- **Actualizări ale motoarelor Antispam** - se vor adăuga noi reguli filtrelor euristic și URL și noi imagini filtrului de imagini. Astfel, eficiența motorului Antispam va crește. Acest tip de actualizare se mai numește **actualizare antispam**.
- **Actualizări ale motoarelor antispyware** - se vor adăuga noi semnături spyware la baza de date. Acest tip de actualizare se mai numește **Actualizare Antispyware**.
- **Actualizare de produs** - la lansarea unei noi versiuni de produs, noi caracteristici și tehnici de scanare sunt introduse pentru a îmbunătăți performanțele produsului. Acest tip de actualizare se mai numește **upgrade**.

26.1. Efectuarea unei actualizări

Actualizarea automată poate fi realizată oricând făcând clic pe **Actualizează acum**. Acest tip de actualizare este cunoscut și ca **actualizare la cererea utilizatorului**.

Pentru actualizarea BitDefender, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Novice
Faceți clic pe iconița **Actualizează acum** din zona Protejați-vă calculatorul.

Modul Intermediar
Mergeți la fila **Securitate** și faceți clic pe **Actualizează acum** în zona de Sarcini rapide din partea stângă a ferestrei.

Modul Expert
Mergeți la **Actualizare > Actualizare**.

Modulul **Actualizare** se va conecta la serverul de actualizare BitDefender și va verifica dacă sunt disponibile noi semnături. Dacă sunt detectate noi semnături, în funcție de opțiunile setate în secțiunea Setări actualizare la cerere, vi se va cere să confirmați actualizarea sau aceasta va fi realizată automat.

Important
Poate fi necesar ca după realizarea unei actualizări să reporniți calculatorul. Este recomandat să faceți acest lucru cât mai repede posibil.

Notă

Dacă vă conectați la Internet prin dial-up, atunci este recomandat să actualizați manual BitDefender în mod regulat.Pentru mai multe informații, consultați *„Cum să actualizați BitDefender în cazul unei conexiuni lente la internet”* (p. 181).

26.2. Configurarea setărilor de actualizare

Actualizările pot fi realizate din rețeaua locală, de pe Internet, direct sau printr-un server proxy.Implicit, BitDefender va căuta actualizări la fiecare oră, pe Internet, și va instala actualizările disponibile fără a vă mai avertiza.

Pentru a configura setările de actualizare:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Actualizare > Setări**.
3. Configurați setările după cum este nevoie.Pentru a afla ce face o opțiune, țineți cursorul mouse-ului deasupra ei și citiți descrierea afișată în partea de jos a ferestrei.
4. Faceți clic pe **Salvează** pentru a salva modificările.

Pentru a aplica setările implicite, faceți clic pe **Nivel implicit**.

Setările de actualizare sunt grupate în patru categorii (**Setări locație de actualizare**, **Setări actualizare automată**, **Setări actualizare la cerere** și **Setări avansate**). Fiecare categorie va fi descrisă separat.

26.2.1. Configurarea locațiilor de actualizare

Pentru a seta locațiile de actualizare, utilizați opțiunile din categoria **Setări locație de actualizare**.

Notă
Configurați aceste setări doar dacă sunteți conectat la o rețea locală care stochează local semnături malware ale BitDefender sau dacă vă conectați la internet printr-un server proxy.

Pentru o actualizare mai sigură și mai rapidă, puteți configura două locații de actualizare: o **Locație de actualizare principală** și o **Locație de actualizare alternativă**. Implicit, acestea sunt setate la fel: `http://upgrade.bitdefender.com`.

Pentru a modifica una dintre locațiile de actualizare, introduceți adresa URL a serverului local în câmpul **URL** corespunzător locației pe care doriți să o modificați.

Notă
Vă recomandăm să setați ca locație principală de actualizare serverul local și să lăsați neschimbată adresa locației de actualizare alternative, ca o măsură de siguranță în caz că serverul local devine indisponibil.

În cazul în care compania utilizează un server proxy pentru conectarea la Internet, selectați **Utilizare proxy** și apoi faceți clic pe **Setări proxy** pentru a configura setările proxy.Pentru mai multe informații, consultați„Setări conexiune” (p. 58)

26.2.2. Configurarea actualizării automate

Pentru a configura procesul de actualizare realizat automat de BitDefeneder, utilizați opțiunile din categoria **Setări actualizare automată**.

Puteți specifica numărul de ore dintre două căutări consecutive după actualizări în câmpul **Frecvență actualizare**. Intervalul implicit dintre actualizări este de o oră.

Pentru a specifica modul în care să fie realizată actualizarea automată, selectați una dintre următoarele opțiuni:

- **Actualizare discretă** - BitDefender descarcă și realizează actualizarea automat.
- **Anunță înainte de a descărca actualizări** - de fiecare dată când o actualizare este disponibilă, veți fi anunțat înainte de a o descărca.
- **Anunță înainte de a instala actualizări** - de fiecare dată când o actualizare a fost descărcată, veți fi anunțat înainte de a o instala.

26.2.3. Configurarea actualizării manuale

Pentru a specifica cum să fie realizată actualizarea manuală (actualizarea la cererea utilizatorului), selectați una dintre opțiunile din categoria **Setări actualizare manuală**:

- **Actualizare discretă** - actualizarea manuală va fi realizată automat în fundal, fără intervenția utilizatorului.
- **Anunță înainte de a descărca actualizări** - de fiecare dată când o actualizare este disponibilă, veți fi anunțat înainte de a o descărca.

26.2.4. Configurarea setărilor avansate

Pentru ca procesul de actualizare al BitDefender să nu vă afecteze munca, configurați opțiunile din categoria **Setări avansate**:

- **Nu cere restart pentru actualizare** - Dacă o actualizare necesită repornirea sistemului, produsul își va continua funcționarea folosind fișierele vechi până când utilizatorul va reporni calculatorul din proprie inițiativă. Utilizatorului nu i se va cere repornirea calculatorului și astfel actualizarea BitDefender nu va interfera cu activitatea utilizatorului.
- **Nu actualiza dacă o scanare este în progres** - BitDefender nu se va actualiza dacă o scanare este în desfășurare. Astfel, procesul de actualizare BitDefender nu va interfera cu sarcinile de scanare.

  Notă
  Dacă BitDefender este actualizat în timpul unei scanări, procesul de scanare va fi anulat.

- **Nu actualiza dacă este activat Modul pentru jocuri** - BitDefender nu se va actualiza dacă funcționează în Modul pentru jocuri.Astfel, puteți minimiza influența produsului asupra performanțelor sistemului în timpul jocului.
- **Activează partajarea actualizărilor** - Dacă doriți să reduceți influența traficului din rețea asupra performanței sistemului în timp actualizărilor, utilizați opțiunea de partajare.
- **Încarcă fișiere BitDefender de pe acest PC** - BitDefender vă permite să partajați cele mai recente semnături antivirus disponibile pe calculatorul dumneavoastră cu alți utilizatori BitDefender.

Ghid de instrucțiuni

27. Cum scanez fișiere și directoare?

Scanarea cu BitDefender este ușoară și flexibilă.Există mai multe metode de a seta BitDefender să scaneze fișiere și directoare după viruși și alte coduri malware:

- Utilizând meniul contextual Windows
- Utilizând sarcini de scanare
- Utilizând bara de scanare

Imediat ce ați inițiat o scanare, va apărea programul asistent de scanare care vă va ghida de-a lungul acestui proces.Pentru informații detaliate despre acest program asistent, consultați secțiunea *„Programul asistent de scanare”* (p. 70).

Notă

Pentru a afla cum puteți scana cu BitDefender atunci când Windows funcționează în Safe Mode, consultați *„Cum scanez calculatorul în Safe Mode?”* (p. 195).

27.1. Utilizând meniul contextual Windows

Aceasta este metoda cea mai ușoară și recomandată pentru a scana un fișier sau un director de pe calculatorul dumneavoastră.Faceți clic-dreapta pe obiectul pe care doriți să-l scanați și selectați **Scanează cu BitDefender** din meniu.Urmați programul asistent de scanare pentru a finaliza scanarea.

Iată câteva situații în care este recomandată folosirea acestei metode de scanare:

- Suspectați un anumit fișier sau director că este infectat.
- Atunci când descărcați de pe Internet fișiere care credeți că ar putea fi periculoase.
- Scanați un director comun din rețea înainte de a copia fișiere din acesta pe calculatorul dumneavoastră.

27.2. Utilizând sarcini de scanare

Dacă doriți să vă scanați calculatorul sau anumite directoare în mod regulat, este indicat să utilizați sarcini de scanare.Sarcinile de scanare specifică locațiile care trebuie scanate de BitDefender, precum și opțiunile de scanare și acțiunile care trebuie aplicate. În plus, aveți posibilitatea să le programați pentru a fi executate în mod regulat sau la o anumită oră.

Pentru a vă scana calculatorul utilizând sarcini de scanare, trebuie să deschideți BitDefender și să rulați sarcina de scanare dorită.Pașii de urmat pentru rularea sarcinii de scanare variază în funcție de modul de vizualizare a interfeței cu utilizatorul.

Rularea sarcinilor de scanare în Modul Novice

În Modul Novice, puteți executa o serie de sarcini de scanare preconfigurate.Faceți clic pe butonul **Securitate** și alegeți sarcina de scanare dorită.Urmați programul asistent de scanare pentru a finaliza scanarea.

Rularea sarcinilor de scanare în Modul Intermediar

În Modul Intermediar puteți rula o serie de sarcini de scanare preconfigurate. De asemenea, puteți configura și rula sarcini de scanare personalizate, pentru a scana doar anumite locații de pe calculator folosind opțiunile de scanare alese de dumneavoastră.Urmați acești pași pentru a rula o sarcină de scanare în Modul Intermediar:

1. Faceți clic pe tabul **Securitate**.
2. În zona Sarcini rapide din partea stângă, faceți clic pe **Scanare completă** și selectați sarcina de scanare dorită.Pentru a configura și executa o scanare personalizată, faceți clic pe **Scanare personalizată** .
3. Urmați programul asistent de scanare pentru a finaliza scanarea.Dacă ați ales să efectuați o scanare personalizată, trebuie să parcurgeți programul asistent de scanare personalizată.

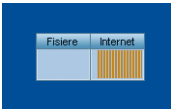
Rularea sarcinilor de scanare în Modul Expert

În Modul Expert, puteți rula toate sarcinile de scanare preconfigurate și, de asemenea, puteți schimba opțiunile lor de scanare. În plus, puteți crea sarcini de scanare personalizate pentru a scana anumite locații de pe calculator.Urmați acești pași pentru a rula o sarcină de scanare în Modul Expert:

1. Faceți clic pe **Antivirus** în meniul din stânga.
2. Faceți clic pe tabul **Scanare viruși**.Aici găsiți o serie de sarcini de scanare standard și puteți crea propriile sarcini de scanare.
3. Faceți dublu-clic pe sarcina de scanare pe care doriți să o rulați.
4. Urmați programul asistent de scanare pentru a finaliza scanarea.

27.3. Utilizând bara de scanare

Bara de scanare este o reprezentare grafică a activității de scanare din sistemul dumneavoastră.Această fereastră mică este disponibilă, implicit, numai în Modul Expert.



Bara de scanare

Puteți utiliza bara de scanare pentru a scana rapid fișiere și directoare.Trageți fișierul sau directorul care doriți să fie scanat peste bara de scanare.Urmați programul asistent de scanare pentru a finaliza scanarea.

Notă

Pentru mai multe informații, consultați *„Bara de scanare”* (p. 21).

28. Cum creez o sarcină de scanare personalizată?

Pentru a crea o sarcină de scanare, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar

Mergeți la fila **Securitate** și faceți clic pe **Scanare personalizată** în zona de Sarcini rapide din partea stângă a ferestrei.

Va apărea un asistent care vă va ajuta să creați o sarcină de scanare.Puteți naviga prin programul asistent cu ajutorul butoanelor **Înainte** și **Înapoi**.Pentru a părăsi asistentul, faceți clic pe **Anulează**.

1. **Bine ați venit!**
2. **Selectarea țintei**

   Faceți clic pe **Adaugă obiect** pentru a selecta fișierele sau directoarele ce vor fi scanate.

   Faceți clic pe **Setări avansate**.În fila **Generalități**, ajustați opțiunile de scanare prin deplasarea cursorului pe scală.Dacă doriți să configurați opțiunile de scanare în detaliu, faceți clic pe **Personalizare**.Accesați fila **Programare** pentru a selecta momentul când va fi efectuată sarcina.
3. **Finalizare**

   Aici puteți introduce numele sarcinii și, opțional, puteți adăuga sarcina de scanare în zona de Sarcini rapide.

   Faceți clic pe **Pornire scanare** pentru a crea sarcina și a lansa asistentul de scanare.

Modul Expert

1. Mergeți la **Antivirus > Scanare viruși**.
2. Faceți clic pe **Sarcină nouă**. Va apărea o nouă fereastră.

   Notă

   Puteți de asemenea să faceți clic-dreapta pe o sarcină de scanare predefinită, cum ar fi **Scanare profundă** și selectați **Clonare sarcină**.Acest lucru este util atunci când creați noi sarcini, deoarece puteți modifica setările unei sarcini duplicate.

3. În fila **Generalități**, introduceți numele sarcinii și ajustați opțiunile de scanare prin deplasarea cursorului pe scală.

   Dacă doriți să configurați opțiunile de scanare în detaliu, faceți clic pe **Personalizare**.

4. Mergeți la fila **Căi** pentru a selecta ținta de scanat. Faceți clic pe **Adăugare element(e)** pentru a selecta fișierele sau directoarele ce urmează a fi scanate.
5. Accesați fila **Programare** pentru a selecta momentul când va fi efectuată sarcina.
6. Faceți clic pe **Ok** pentru a salva sarcina.Noua sarcină va apărea sub sarcinile definite de utilizator și poate fi editată, eliminată sau executată în orice moment din această fereastră.

29. Cum programez o scanare a calculatorului?

Este recomandat să vă scanați calculatorul periodic pentru a-l proteja de viruși.BitDefender vă permite să programați sarcini de scanare, astfel încât să vă puteți scana automat calculatorul.

Pentru a programa BitDefender să vă scaneze calculatorul, urmați acești pași:

1. Deschideți BitDefender.
2. În funcție de modul de vizualizare a interfeței, procedați după cum urmează:

   Modul Intermediar
   Mergeți la fila **Securitate** și faceți clic pe **Configurare antivirus** în zona de Sarcini rapide din partea stângă a ferestrei.

   Modul Expert
   Faceți clic pe **Antivirus** în meniul din stânga.
3. Faceți clic pe tabul **Scanare viruși**.Aici găsiți o serie de sarcini de scanare standard și puteți crea propriile sarcini de scanare.

   - Sarcinile de sistem sunt disponibile și pot fi rulate pe orice cont de utilizator Windows.
   - Sarcinile de utilizator sunt disponibile și pot fi rulate numai de către utilizatorul care le-a creat.

   Acestea sunt sarcinile de scanare standard pe care le puteți programa:

   Scanare completă sistem
   Scanează întregul sistem, cu excepția arhivelor.În configurația implicită, se scanează după toate tipurile de aplicații periculoase, cu excepția celor de tip rootkit.

   Quick Scan
   Scanarea rapidă utilizează o tehnologie de scanare "in-the-cloud" (online) pentru a detecta aplicațiile periculoase ce rulează pe sistemul dumneavoastră. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o fracțiune din resursele de sistem necesare pentru o scanare antivirus obișnuită.

   Scanare automată la conectare
   Scanează obiectele executate atunci când un utilizator se conectează la Windows.Pentru a utiliza această sarcină, trebuie să o programați să ruleze la pornirea sistemului.În mod implicit, scanarea autologon este dezactivată.

   Scanare profundă
   Scanează întregul sistem.În configurația implicită, se scanează după toate tipurile de aplicații periculoase care amenință securitatea sistemului

dumneavoastră, cum ar fi virușii, aplicațiile spion, adware, obiecte ascunse (rootkituri) și altele.

Documentele mele

Utilizați această sarcină pentru a scana directoare importante ale utilizatorului curent: `My Documents`, `Desktop` și `StartUp`. Astfel, veți asigura siguranța documentelor dumneavostră, un spațiu de lucru sigur și rularea la pornirea sistemului a unor aplicații necompromise.

Dacă niciuna dintre aceste sarcini de scanare nu este potrivită scopului dumneavoastră, puteți crea o nouă sarcină de scanare, pe care o puteți programa apoi pentru a rula după cum este necesar.

4. Faceți clic-dreapta pe sarcina de scanare dorită și selectați **Planifică**.Va apărea o nouă fereastră.
5. Programați sarcina să ruleze după cum este necesar:
   - Pentru a rula sarcina de scanare o singură dată, selectați **O singură dată** și specificați data și ora începerii.
   - Pentru a rula sarcina de scanare la pornirea sistemului, selectați **La pornirea sistemului**.Puteți indica după cât timp de la pornirea sistemului să fie rulată sarcina (în minute).
   - Pentru a rula sarcina de scanare periodic, selectați **Periodic** și specificați cât de des să ruleze, precum și data și ora începerii.

   Notă

   De exemplu, pentru a vă scana calculatorul în fiecare sâmbătă, la ora 2 dimineața, trebuie să configurați programul după cum urmează:

   a. Selectați **Periodic**.

   b. În câmpul **La fiecare**, tastați 1 și apoi selectați **săptămâni** din meniu.În acest fel, sarcina este rulată o dată pe săptămână.

   c. Setați ca dată de început următoarea zi de sâmbătă.

   d. Setați ora începerii la `2:00:00` .

6. Faceți clic pe **OK** pentru a salva programul.Sarcina de scanare va rula în mod automat conform programului pe care l-ați definit.Dacă aveți calculatorul închis atunci când sarcina trebuie să ruleze, aceasta va fi executată imediat ce deschideți calculatorul.

30. Cum creez conturi de utilizator Windows?

Un cont de utilizator Windows reprezintă un profil unic care include toate setările, privilegiile și fișierele personale ale fiecărui utilizator în parte.

Conturile Windows permit administratorului calculatorului să controleze accesul fiecărui utilizator.

Configurarea de conturi de utilizator este utilă atunci când calculatorul este utilizat în comun de părinți și copii - un părinte poate configura conturi pentru fiecare copil în parte.

Alegeți sistemul de operare pe care îl aveți pentru a afla cum puteți crea conturi Windows.

- Windows XP:
  1. Conectați-vă la calculatorul dumneavoastră pe un cont de administrator.
  2. Faceți clic pe Start, Panoul de comandă și apoi faceți clic pe Conturi de utilizator.
  3. Faceți clic pe Creare cont nou.
  4. Introduceți numele utilizatorului. Puteți utiliza numele întreg al persoanei, prenumele sau porecla acesteia. Apoi faceți clic pe Înainte.
  5. Pentru tipul de cont, alegeți Limitat și apoi Creați cont. Conturile limitate sunt potrivite pentru copii deoarece aceștia nu pot realiza modificări la nivelul întregului sistem sau instala anumite aplicații.
  6. Noul dumneavoastră cont va fi creat și îl veți vedea listat pe ecranul de Administrare a conturilor.
- Windows Vista sau Windows 7:
  1. Conectați-vă la calculatorul dumneavoastră pe un cont de administrator.
  2. Faceți clic pe Start, Panoul de comandă și apoi faceți clic pe Conturi de utilizator.
  3. Faceți clic pe Creare cont nou.
  4. Introduceți numele utilizatorului. Puteți utiliza numele întreg al persoanei, prenumele sau porecla acesteia. Apoi faceți clic pe Înainte.
  5. Pentru tipul de cont, faceți clic pe Standard și apoi Creați cont. Conturile limitate sunt potrivite pentru copii deoarece aceștia nu pot realiza modificări la nivelul întregului sistem sau instala anumite aplicații.
  6. Noul dumneavoastră cont va fi creat și îl veți vedea listat pe ecranul de Administrare a conturilor.

Notă

După ce ați adăugat noi conturi de utilizator, puteți crea parole pentru conturi.

31. Cum actualizez BitDefender printr-un server proxy?

În mod normal, BitDefender detectează și importă în mod automat setările proxy ale sistemului dumneavoastră.Dacă vă conectați la internet printr-un server proxy, este posibil să fie nevoie să găsiți setările proxy și să configurați BitDefender în mod corespunzător.Pentru a afla cum să procedați, consultați *„Cum aflu care sunt setările mele proxy?”* (p. 208).

După găsirea setărilor proxy, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **General > Setări**.
3. Faceți clic pe **Setări proxy** din **Setări de conexiune**.
4. Introduceți setările proxy în câmpurile corespunzătoare.
5. Faceți clic pe **OK**.

Notă
Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport”* (p. 199).

32. Cum trec la un produs superior din gama BitDefender 2011?

Cu BitDefender 2011 puteți trece rapid de la un produs BitDefender 2011 la altul.

Să ne gândim la următorul scenariu: utilizați de ceva timpBitDefender Internet Security 2011 2011 și de curând v-ați decis să alegeți BitDefender Total Security 2011 și caracteristicile suplimentare pe care acesta le asigură.

Tot ce trebuie să faceți este să achiziționați o serie de înregistrare pentru produsul BitDefender 2011 la care doriți să treceți și să o introduceți în fereastra de înregistrare a produsului BitDefender 2011 pe care îl utilizați în prezent.

Urmați acești pași:

1. Deschideți BitDefender.
2. Faceți clic pe linkul **Informații licență** din partea inferioară a ferestrei.Va apărea fereastra de înregistrare.
3. Introduceți seria de înregistrare și faceți clic pe **Înregistrare**.
4. BitDefender vă va informa că respectiva serie de înregistrare este destinată unui alt produs și vă va oferi opțiunea de a-l instala.Faceți clic pe linkul corespunzător și urmați procedura ghidată în trei pași pentru a efectua actualizarea.
   a. **Confirmarea acțiunii**
   b. **Actualizare în desfășurare**

      Așteptați ca BitDefender să finalizeze procesul de actualizare.Aceasta va dura câteva minute.
   c. **Actualizare finalizată**

      Procesul s-a finalizat. Poate fi necesară o repornire a sistemului.

Depanare probleme și asistență profesională

33. Depanarea problemelor

Acest capitol prezintă anumite probleme cu care vă puteți confrunta la utilizarea BitDefender și vă oferă soluții posibile la aceste probleme.Majoritatea acestor probleme pot fi soluționate prin configurarea adecvată a setărilor produsului.

Dacă problema dumneavoastră nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic a BitDefender folosind informațiile din capitolul *„Suport”* (p. 199).

33.1. Probleme la instalare

Acest articol vă ajută să remediați problemele care apar cel mai des la instalarea BitDefender.Aceste probleme sunt grupate în următoarele categorii:

- Erori de validare a instalării: asistentul de instalare nu poate fi rulat din cauza unei anumite situații a sistemului dumneavoastră.
- Instalări eșuate: ați inițiat instalarea din asistentul de instalare, dar procesul nu s-a finalizat.

33.1.1. Erori de validare a instalării

Când porniți asistentul de instalare, sunt verificate o serie de condiții pentru validarea necesară inițierii instalării. În tabelul de mai jos sunt prezentate cel mai des întâlnite erori de validare a instalării și soluții pentru remedierea lor.

Eroare	Descriere & Soluție
Nu aveți drepturile necesare pentru instalarea programului.	Pentru a rula asistentul de instalare și pentru a instala BitDefender, aveți nevoie de drepturi de administrator.Puteți proceda în oricare dintre următoarele modalități: ● Conectați-vă la un cont Windows de administrator și rulați din nou asistentul de instalare. ● Faceți clic-dreapta pe fișierul de instalare și selectați **Rulează ca**.Introduceți numele de utilizator și parola corespunzătoare unui cont Windows de administrator al sistemului.
Programul de instalare a detectat o versiune anterioară BitDefender, care nu a fost dezinstalată corect.	BitDefender a fost instalat anterior pe sistemul dvs, dar versiunea respectivă nu a fost dezinstalată complet. Acest fapt împiedică instalarea unei noi versiuni BitDefender.

Eroare	Descriere & Soluție
	Pentru a remedia această eroare și pentru a instala BitDefender, urmați acești pași: 1. Mergeți la www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră. 2. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator. 3. Reporniți calculatorul. 4. Reporniți asistentul de instalare BitDefender.
Produsul BitDefender nu este compatibil cu sistemul dumneavoastră de operare.	Sistemul de operare pe care încercați să instalați BitDefender nu este compatibil cu acesta.Consultați *„Cerințe de sistem”* (p. 2) pentru a afla care sunt sistemele de operare care permit instalarea BitDefender. Dacă sistemul dumneavoastră de operare este Windows XP cu Service Pack 1 sau fără niciun pachet de servicii, puteți să instalați Service Pack 2 sau mai recent și apoi să rulați din nou asistentul de instalare.
Fișierul de instalare este destinat unui alt tip de procesor.	Dacă obțineți o astfel de eroare, înseamnă că încercați să rulați o versiune incorectă a fișierului de instalare. Există două versiuni ale fișierului de instalare BitDefender: una pentru procesoare pe 32 de biți și cealaltă pentru procesoare pe 64 de biți. Pentru a vă asigura că aveți versiunea corectă pentru sistemul dumneavoastră, descărcați fișierul de instalare direct de la www.bitdefender.com .

33.1.2. Instalare eșuată

Există mai multe forme de manifestare a unei instalări eșuate:

- În timpul instalării apare un ecran de eroare. Vi se poate solicita să anulați instalarea sau vi se poate pune la dispoziție un buton prin care să rulați un instrument de dezinstalare, care va curăța sistemul.

Notă
Imediat după inițierea instalării, puteți fi informat că nu există suficient spațiu liber pe disk pentru instalarea BitDefender. În acest caz, eliberați spațiul necesar pe partiția pe care doriți să instalați BitDefender și apoi reluați sau reinițiati instalarea.

- Instalarea nu înaintează și, eventual, sistemul se blochează. Sistemul reacționează numai după repornire.
- Instalarea s-a finalizat, dar nu puteți folosi funcțiile BitDefender, parțial sau în totalitate.

Pentru a reuși instalarea BitDefender după o tentativă eșuată, urmați acești pași:

1. **Curățați sistemul după instalarea eșuată.** Dacă instalarea eșuează, unele chei de regiștri și fișiere BitDefender pot rămâne în sistemul dumneavoastră. Aceste rămășite pot împiedica instalarea ulterioară a BitDefender. De asemenea, ele pot afecta funcționarea și stabilitatea sistemului. De aceea, este necesar să le ștergeți înainte de a încerca să reinstalați produsul.

   Dacă acesta este cazul, cea mai simplă soluție de urmat este reprezentată de eliminarea completă a BitDefender din sistem, urmată de reinstalarea acestuia.Pentru mai multe informații, consultați *„Cum dezinstalez complet BitDefender?”* (p. 208).

2. **Verificați cauzele posibile ale instalării eșuate.** Înainte de a începe reinstalarea produsului, verificați dacă există și eliminați posibilele cauze ale instalării inițiale eșuate:

   a. Verificați dacă aveți instalată orice altă soluție de securitate pentru că ea ar putea perturba funcționarea normală a BitDefender. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați BitDefender.

   b. De asemenea, este recomandat să verificați dacă sistemul dumneavoastră este infectat.Puteți proceda în oricare dintre următoarele modalități:

      - Folosiți BitDefender Rescue CD și eliminați orice pericol existent.Pentru mai multe informații, consultați *„BitDefender Rescue CD”* (p. 191).
      - Deschideți o fereastra Internet Explorer, mergeți la www.bitdefender.com și efectuați o scanare online (faceți clic pe butonul **Scanare online**).

3. Încercați din nou să instalați BitDefender.Este recomandat să descărcați și să rulați cea mai recentă versiune a fișierului de instalare de pe www.bitdefender.com.

4. Dacă instalarea eșuează, vă rugăm să contactați BitDefender pentru suport, folosind informațiile din secțiunea *„Suport”* (p. 199).

33.2. Sistemul meu funcționează lent

De obicei, după instalarea unui program de securitate, este posibil să se producă o ușoară încetinire a funcționării sistemului, fapt ce este normal într-o anumită măsură.

În cazul în care observați o încetinire semnificativă, această problemă poate apărea din următoarele motive:

- **BitDefender nu este singurul program de securitate instalat în sistem.**

  Deși BitDefender caută și dezinstalează programele de securitate detectate în timpul instalării, se recomandă să îndepărtați orice alte programe antivirus pe care le-ați utilizat înainte de a iniția instalarea BitDefender.Pentru mai multe informații, consultați *„Cum dezinstalez alte soluții de securitate?”* (p. 206).

- **Cerințele minime de sistem pentru rularea BitDefender nu sunt întrunite.**

  În cazul în care calculatorul dumneavoastră nu întrunește cerințele minime de sistem, acesta va începe să funcționeze încet, în special atunci când mai multe aplicații rulează în același timp.Pentru mai multe informații, consultați *„Cerințe de sistem minime”* (p. 2).

- **Unitățile de hard disc sunt prea fragmentate.**

  Fragmentarea fișierelor încetinește accesul la acestea și scade performanțele sistemului.

  Pentru a vă defragmenta partițiile de disc folosind instrumentul din Windows, urmați calea din meniul Start al Windows: **Start → All Programs → Accessories → System Tools → Disk Defragmenter**.

33.3. Nu începe scanarea

Acest tip de problemă poate avea două cauze principale:

- **O instalare anterioară a BitDefender care nu a fost complet eliminată sau o instalare necorespunzătoare a BitDefender**.

  Dacă acesta este cazul, cea mai simplă soluție de urmat este reprezentată de eliminarea completă a BitDefender din sistem, urmată de reinstalarea acestuia.Pentru mai multe informații, consultați *„Cum dezinstalez complet BitDefender?”* (p. 208).

- **BitDefender nu este singura soluție de securitate instalată în sistemul dumneavoastră**.

  În acest caz, urmați acești pași:

  1. Dezinstalați cealaltă soluție de securitate.Pentru mai multe informații, consultați *„Cum dezinstalez alte soluții de securitate?”* (p. 206).
  2. Eliminați complet BitDefender din sistem.
  3. Reinstalați BitDefender în sistem.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport”* (p. 199).

33.4. Nu mai pot utiliza o aplicație

Această problemă apare când încercați să utilizați un program care a funcționat normal înainte de instalarea BitDefender.

Vă puteți confruntа cu una dintre următoarele situații:

- Este posibil să primiți un mesaj din partea BitDefender referitor la faptul că programul încearcă să efectueze o modificare asupra sistemului.
- Este posibil să primiți un mesaj de eroare din partea programului pe care încercați să-l utilizați.

Acest tip de situație apare când Active Virus Control detectează din greșeală anumite aplicații ca fiind rău intenționate.

Active Virus Control este un modul BitDefender care monitorizează în mod constant aplicațiile care rulează pe sistemul dumneavoastră și raportează acele aplicații care sunt posibil rău intenționate.Deoarece această opțiune se bazează pe un sistem euristic, pot exista situații în care aplicații legitime să fie raportate de Active Virus Control.

Atunci când se întâmplă aceasta, puteți exclude aplicația respectivă de la monitorizarea efectuată de Active Virus Control.

Pentru a adăuga programul în lista de excluderi, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus > Scut**.
3. Faceți clic pe **Setări avansate**.
4. În noua fereastră, mergeți la tabul **Excluderi**, faceți clic pe butonul **Adaugă** și mergeți la locația fișierului .exe al programului (aflat de obicei în `C:\Program Files`).
5. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.
6. Închideți fereastra BitDefender și verificați dacă problema persistă.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport”* (p. 199).

33.5. Nu mă pot conecta la internet

Este posibil să observați că un program nu se mai poate conecta la internet sau accesa serviciile de rețea după instalarea BitDefender.

Asistentul de depanare vă va ajuta să identificați și să rezolvați problema de conexiune.Pentru pornirea asistentului, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar
Mergeți la fila **Securitate** și faceți clic pe **Configurare firewall** în zona Sarcini rapide din partea stângă a ferestrei.Selectați fila **Setări** din fereastra care apare și faceți clic pe **Depanare**.

Modul Expert
Mergeți la **Firewall > Setări** și faceți clic pe **Depanare**.

Urmați procedura ghidată în trei pași pentru a începe depanarea.Puteți naviga prin programul asistent cu ajutorul butonului **Înainte**.Pentru a părăsi asistentul, faceți clic pe **Anulează**.

1. **Bine ați venit!**

   Selectați **Încerc să obțin acces la internet, dar acțiunea eșuează**.

2. **Identificarea problemei**

   Faceți clic pe **Selectare aplicație** și **Caută** pentru a localiza fișierul .exe al programului (aflat de obicei în `C:\Program Files`, de exemplu Firefox.exe).Faceți clic pe **Adaugă**.

3. **Soluție recomandată**

   Alegeți **Da, permite accesul**.Faceți clic pe **Finalizare** și verificați dacă problema persistă.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport”* (p. 199).

33.6. Nu pot utiliza imprimanta

În funcție de rețeaua la care sunteți conectat, firewallul BitDefender poate bloca conexiunea dintre calculatorul dumneavoastră și o imprimantă din rețea.

În acest caz, cea mai bună soluție este să configurați BitDefender pentru a permite în mod automat efectuarea de conexiuni către și de la imprimanta respectivă.

Asistentul de depanare vă va ajuta să identificați și să rezolvați problema de conexiune.Pentru pornirea asistentului, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar
Mergeți la fila **Securitate** și faceți clic pe **Configurare firewall** în zona Sarcini rapide din partea stângă a ferestrei.Selectați fila **Setări** din fereastra care apare și faceți clic pe **Depanare**.

Modul Expert
Mergeți la **Firewall > Setări** și faceți clic pe **Depanare**.

Urmați procedura ghidată în trei pași pentru a începe depanarea.Puteți naviga prin programul asistent cu ajutorul butonului **Înainte**.Pentru a părăsi asistentul, faceți clic pe **Anulează**.

1. **Bine ați venit!**

   Selectați **Încerc să imprim, dar acțiunea eșuează**.

2. **Identificarea problemei**

   Faceți clic pe **Selectare imprimantă**.Selectați imprimanta din listă, după nume sau adresa IP.Dacă nu puteți găsi dispozitivul în listă, introduceți manual adresa IP în câmpul editabil.Faceți clic pe **Adaugă**.

3. **Soluție recomandată**

   Alegeți **Da, permite accesul**.Faceți clic pe **Finalizare** și verificați dacă problema persistă.

În cazul în care programul asistent de depanare indică faptul că problema nu este cauzată de către firewallul BitDefender de pe calculatorul dumneavoastră, verificați dacă nu există alte cauze potențiale, cum ar fi următoarele:

- Firewallul de pe celălalt calculator poate bloca partajarea de fișiere și imprimante cu calculatorul dumneavoastră.
  - Dacă se folosește Windows Firewall, acesta poate fi configurat să permită partajarea de fișiere și imprimante, după cum urmează: deschideți fereastra de setări a Windows Firewall, tabul **Exceptions**, și selectați căsuța **File and Printer Sharing**.
  - Dacă se folosește un alt program firewall, consultați documentația sau fișierul de ajutor ale acestuia.
- Cauze generale care pot împiedica folosirea sau conectarea la imprimanta partajată:
  - Poate fi necesar să vă conectați la un cont Windows de administrator pentru a avea acces la imprimanta partajată.
  - Numai anumite calculatoare și anumiți utilizatori pot accesa imprimanta partajată. Dacă partajați imprimanta dumneavoastră, verificați restricțiile de acces stabilite pentru aceasta pentru a vedea dacă utilizatorul de pe celălalt calculator o poate accesa.Dacă încercați să vă conectați la o imprimantă partajată, întrebați utilizatorul de pe celălalt calculator dacă vi se permite accesul la imprimantă.
  - Imprimanta conectată la calculatorul dumneavoastră sau la celălalt calculator nu este partajată.
  - Imprimanta partajată nu este adăugată pe calculator.

Notă

Pentru a afla cum să administrați imprimantele partajate (partajarea unei imprimante, stabilirea sau eliminarea permisiunilor de acces la o imprimantă, conectarea la o imprimantă de rețea sau partajată), mergeți la Centrul de Asistență și Suport al Windows (în meniul Start, faceți clic pe **Help and Support**).

- Accesul la o imprimantă din rețea poate fi restricționat pentru anumite calculatoare sau pentru anumiți utilizatori. Este recomandat să consultați administratorul rețelei pentru a afla dacă vă puteți conecta la imprimanta în cauză.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport"* (p. 199).

33.7. Nu pot partaja fișiere cu un alt calculator

În funcție de rețeaua la care sunteți conectat, firewallul BitDefender poate bloca conexiunea dintre sistemul dumneavoastră și un alt calculator.Drept urmare, nu mai puteți partaja fișiere cu celălalt calculator.În acest caz, cea mai bună soluție este să configurați BitDefender pentru a permite în mod automat efectuarea de conexiuni către și de la sistemul respectiv.

Asistentul de depanare vă va ajuta să identificați și să rezolvați problema de conexiune.Pentru pornirea asistentului, deschideți BitDefender și, în funcție de modul de vizualizare a interfeței, procedați după cum urmează:

Modul Intermediar
: Mergeți la fila **Securitate** și faceți clic pe **Configurare firewall** în zona Sarcini rapide din partea stângă a ferestrei.Selectați fila **Setări** din fereastra care apare și faceți clic pe **Depanare**.

Modul Expert
: Mergeți la **Firewall > Setări** și faceți clic pe **Depanare**.

Urmați procedura ghidată în trei pași pentru a începe depanarea.Puteți naviga prin programul asistent cu ajutorul butonului **Înainte**.Pentru a părăsi asistentul, faceți clic pe **Anulează**.

1. **Bine ați venit!**

   Selectați **Încerc să accesez un calculator din rețeaua proprie, dar acțiunea eșuează**.

2. **Identificarea problemei**

   Faceți clic pe **Selectare calculator**.Selectați calculatorul din listă, după nume sau adresa IP.Dacă nu puteți găsi calculatorul în listă, introduceți manual adresa IP în câmpul editabil.Faceți clic pe **Adaugă**.

3. **Soluție recomandată**

   Alegeți **Da, permite accesul**.Faceți clic pe **Finalizare** și verificați dacă problema persistă.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport"* (p. 199).

33.8. Conexiunea mea la internet este lentă

Această situație poate apărea după instalarea BitDefender.Problema poate fi cauzată de erori de configurare a firewallului BitDefender.

Pentru a remedia această situație, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Firewall > Setări**.
3. Debifați căsuța **Firewallul este activat** pentru a dezactiva temporar firewallul.
4. Verificați dacă vă puteți conecta la internet atunci când firewallul BitDefender este dezactivat.
   - Dacă în continuare nu vă puteți conecta la internet, este posibil ca problema să nu fie cauzată de BitDefender. Contactați furnizorul dumneavoastră de servicii de internet pentru a verifica dacă este funcțională conexiunea la nivelul acestuia.

     În cazul în care primiți o confirmare din partea furnizorului dumneavoastră de servicii de internet că respectiva conexiune este funcțională la nivelul său, iar problema încă persistă, contactați BitDefender conform descrierii din secțiunea *„Suport”* (p. 199).
   - Dacă reușiți să vă conectați la internet după dezactivarea firewallului BitDefender, urmați acești pași:
     a. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
     b. Mergeți la **Firewall > Setări** și selectați căsuța pentru a activa firewallul.
     c. Faceți clic pe **Setări avansate**, selectați **Activează Internet Connection Sharing** și debifați **Blochează scanările de porturi**.
     d. Mergeți la tabul **Rețea** din fereastra principală.
     e. Extindeți meniul derulant din coloana **Tip rețea** și selectați **Acasă/ Serviciu**.
     f. Mergeți la coloana **Generic** și setați opțiunea **Da**. Setați **Modul ascuns** pe **La distanță**.
     g. Verificați dacă vă puteți conecta la internet.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport”* (p. 199).

33.9. Cum să actualizați BitDefender în cazul unei conexiuni lente la internet

Dacă dispuneți de o conexiune lentă la internet (cum ar fi cea de tip dial-up), în timpul procesului de actualizare pot apărea erori.

Pentru a vă menține actualizat sistemul cu cele mai recente semnături malware BitDefender, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Actualizare > Setări**.
3. Din **Setările de actualizare manuală**, selectați **Anunță înainte de a descărca actualizări**.
4. Faceți clic pe **Salvează** și mergeți la tabul **Actualizare**.
5. Faceți clic pe **Actualizează acum** și veți vedea că va apărea o nouă fereastră.
6. Selectați numai **Actualizări semnături** și apoi faceți clic pe **OK**.
7. BitDefender va descărca și va instala numai actualizările semnăturilor malware.

33.10. Calculatorul meu nu este conectat la internet. Cum actualizez BitDefender?

În cazul în care calculatorul dumneavoastră nu este conectat la internet, trebuie să descărcați manual actualizările pe un calculator cu acces la internet și apoi să le transferați pe calculatorul dumneavoastră utilizând un dispozitiv de stocare portabil, cum ar fi un stick USB.

Urmați acești pași:

1. Pe un calculator cu acces la internet, deschideți un browser și accesați:

   www.bitdefender.com/site/view/Desktop-Products-Updates.html

2. În coloana **Actualizare manuală**, faceți clic pe linkul corespunzător produsului și arhitecturii sistemului dumneavoastră.În cazul în care nu știți dacă sistemul dumneavoastră Windows rulează pe 32 sau 64 biți, vă rugăm să consultați *„Utilizez o versiune Windows pe 32 biți sau pe 64 biți?”* (p. 207).
3. Salvați fișierul denumit `weekly.exe` în sistem.
4. Transferați fișierul descărcat pe un dispozitiv de stocare portabil, cum ar fi un stick USB, și apoi în calculatorul dumneavoastră.
5. Faceți dublu-clic pe fișier și urmați indicațiile programului asistent.

33.11. Serviciile BitDefender nu răspund

Acest articol vă ajută să remediați problema *Serviciile BitDefender nu răspund*.Această problemă poate apărea în următoarele situații:

- Iconița BitDefender din bara de sistem apare în gri și o fereastră pop-up vă informează că serviciile BitDefender nu răspund.
- Fereastra BitDefender indică faptul că serviciile BitDefender nu răspund.

Problema poate fi cauzată de:

- o actualizare importantă este în curs de instalare.
- erori temporare de comunicare între serviciile BitDefender.
- unele dintre serviciile BitDefender sunt oprite.
- alte soluții de securitate rulează pe calculatorul dumneavoastră, în același timp cu BitDefender.
- viruși de pe sistemul dvs afectează funcționarea normală a BitDefender.

Pentru a remedia această problemă, încercați următoarele soluții:

1. Așteptați câteva momente pentru a vedea dacă apar schimbări.Eroarea poate fi temporară.
2. Reporniți calculatorul și așteptați câteva momente până când se încarcă BitDefender. Deschideți BitDefender pentru a vedea dacă eroarea persistă.De obicei, repornirea calculatorului rezolvă problema.
3. Verificați dacă aveți instalată orice altă soluție de securitate pentru că ea ar putea perturba funcționarea normală a BitDefender. Vă recomandăm să dezinstalați toate celelalte soluții de securitate și apoi să reinstalați BitDefender.
4. Dacă eroarea persistă, este posibil să existe o problemă mai gravă (de exemplu, calculatorul dumneavoastră ar putea fi infectat cu un virus care afectează funcționarea BitDefender).Vă rugăm să contactați BitDefender pentru suport, folosind informațiile din secțiunea *„Suport”* (p. 199).

33.12. Filtrul Antispam nu funcționează corect

Acest articol vă ajută să remediați următoarele probleme legate de funcționarea filtrului antispam al BitDefender:

- Mai multe mesaje e-mail legitime sunt marcate ca `[spam]`.
- Multe mesaje spam nu sunt marcate corespunzător de filtrul antispam.
- Filtrul antispam nu detectează niciun mesaj spam.

33.12.1. Mesaje legitime sunt marcate ca [spam]

Mesaje legitime sunt marcate ca `[spam]` pentru că filtrul antispam BitDefender le percepe ca atare.În mod normal, puteți rezolva această problemă printr-o configurare adecvată a filtrului Antispam.

BitDefender adaugă automat într-o Listă de prieteni destinatarii mesajelor e-mail trimise de dumneavoastră.Mesajele e-mail primite de la persoanele din Lista de prieteni sunt considerate a fi legitime. Ele nu sunt verificate de filtrul antispam și, astfel, nu sunt marcate niciodată ca `[spam]`.

Configurarea automată a Listei de prieteni nu previne erorile de detecție care pot apărea în următoarele situații:

- Primiți multe mesaje comerciale nesolicitate, ca urmare a înscrierii pe diferite site-uri web. În acest caz, soluția este să adăugați adresele de e-mail de la care primiți astfel de mesaje în Lista de prieteni.
- O parte semnificativă a mesajelor e-mail pe care le primiți sunt trimise de oameni cărora nu le-ați scris niciodată pe e-mail, cum ar fi: clienți, potențiali parteneri de afaceri și alții. În acest caz, sunt necesare alte soluții.

Dacă folosiți unul dintre clienții de mail în care BitDefender se integrează, încercați următoarele soluții:

1. Indicați erorile de detecție. Aceasta folosește la antrenarea Motorului de învățare (Bayesian) al filtrului antispam și permite prevenirea erorilor de detecție ulterioare. Motorul de învățare analizează mesajele indicate și învață tiparele acestora.Următoarele mesaje e-mail care corespund acelor tipare nu vor fi marcate ca `[spam]`.
2. Reduceți nivelul de protecție antispam. Prin scăderea nivelului de protecție antispam, filtrul antispam va avea nevoie de mai multe indicii pentru a clasifica un mesaj e-mail ca spam.Încercați această soluție numai dacă multe mesaje legitime (inclusiv mesaje comerciale solicitate) sunt incorect detectate ca spam.
3. Re-educați Motorul de învățare (filtrul Bayesian). Încercați această soluție numai dacă soluțiile anterioare nu au dat rezultate satisfăcătoare.

Notă

BitDefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat.Pentru o listă completă a clienților de mail admiși, consultați *„Cerințe software”* (p. 2).

Dacă folosiți un alt client de mail, nu puteți indica erorile de detecție și antrena Motorul de învățare. Pentru a rezolva problema, încercați să reduceți nivelului protecției antispam.

Adăugați contactele pe Lista de prieteni

Dacă folosiți un client de mail admis, puteți adăuga foarte ușor expeditorii de mesaje legitime pe Lista de prieteni.Urmați acești pași:

1. În clientul dumneavoastră de mail, selectați un mesaj e-mail al expeditorului pe care doriți să-l adăugați pe Lista de prieteni.
2. Faceți clic pe butonul **Adaugă prieten** din bara de instrumente antispam BitDefender.
3. Vi se poate cere să confirmați adresa adăugată pe Lista de prieteni.Selectați **Nu mai afișa acest mesaj** și faceți clic pe **OK**.

Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.

Dacă folosiți un alt client de mail, puteți adăuga contacte pe Lista de prieteni din interfața BitDefender.Urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Faceți clic pe **Antispam** în meniul din stânga.
3. Faceți clic pe tabul **Stare**.
4. Faceți clic pe **Administrează prieteni**.Va apărea o fereastră de configurare.
5. Introduceți adresa de e-mail a expeditorului de la care doriți să primiți întotdeauna mesaje e-mail și faceți clic pe butonul pentru a adăuga adresa pe Lista de prieteni.
6. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Indicați erorile de detecție

Dacă folosiți un client de mail admis, puteți corecta cu ușurință filtrul antispam (indicând care mesaje e-mail nu ar trebui marcate ca `[spam]`). Astfel, veți îmbunătăți considerabil eficiența filtrului antispam.Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele legitime pe care BitDefender le-a marcat incorect ca `[spam]`.
4. Faceți clic pe butonul **Adaugă prieten** din bara de instrumente antispam BitDefender, pentru a adăuga expeditorul pe Lista de prieteni.Este posibil să vi se ceară să faceți clic pe **OK**, pentru confirmare.Veți primi toate mesajele de la această adresă, indiferent de conținutul lor.
5. Faceți clic pe butonul **Nu este Spam** din bara de instrumente antispam BitDefender (localizată, de obicei, în zona de sus a ferestrei clientului de mail).

Aceasta îi indică Motorului de învățare faptul că mesajul selectat nu este spam. Mesajul e-mail va fi mutat în directorul Inbox.Următoarele mesaje e-mail care corespund acelor tipare nu vor mai fi marcate ca [spam].

Reduceți nivelul protecției antispam

Pentru a reduce nivelul protecției antispam, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Faceți clic pe **Antispam** în meniul din stânga.
3. Faceți clic pe tabul **Stare**.
4. Mutați cursorul mai jos pe scală.

Este recomandat să reduceți protecția numai cu un nivel și apoi să așteptați îndeajuns de mult timp încât să puteți evalua rezultatele. Dacă multe mesaje e-mail legitime sunt încă marcate ca [spam], puteți reduce și mai mult nivelul protecției antispam. Dacă observați că numeroase mesaje spam nu sunt detectate, este recomandat să nu reduceți nivelul protecției antispam.

Re-educați Motorul de învățare (Bayesian)

Înainte de a educa Motorul de învățare (Bayesian), pregătiți un director care să conțină numai mesaje SPAM și un altul doar cu mesaje legitime. Motorul de învățare le va analiza și va învăța caracteristicile definitorii pentru mesajele spam sau legitime pe care le primiți de obicei. Pentru ca educarea să fie eficientă, trebuie să existe cel puțin 50 de mesaje din fiecare categorie.

Pentru a reseta baza de date Bayesiană și pentru a re-educa Motorul de învățare, urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Pe bara de instrumente antispam BitDefender, faceți clic pe butonul **Asistent** pentru a porni programul asistent de configurare antispam.
3. Faceți clic pe **Înainte**.
4. Selectați **Omite** și faceți clic pe **Înainte**.
5. Selectați **Șterge baza de date a filtrului antispam** și faceți clic pe **Înainte**.
6. Selectați directorul care conține mesaje legitime și faceți clic pe **Înainte**.
7. Selectați directorul care conține mesaje SPAM și faceți clic pe **Înainte**.
8. Faceți clic pe **Finalizează** pentru a începe procesul de educare.
9. Când educarea a luat sfârșit, faceți clic pe **Închide**.

Solicitați ajutor

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport"* (p. 199).

33.12.2. Multe mesaje spam nu sunt detectate

Dacă primiți multe mesaje spam care nu sunt marcate `[spam]`, trebuie să configurați filtrul antispam BitDefender, pentru a-i îmbunătăți eficiența.

Dacă folosiți unul dintre clienții de mail în care BitDefender se integrează, încercați următoarele soluții, pe rând:

1. Indicați erorile de detecție. Aceasta folosește la antrenarea Motorului de învățare (Bayesian) al filtrului antispam și, de obicei, îmbunătățește eficiența detecției antispam. Motorul de învățare analizează mesajele indicate și învață tiparele acestora.Următoarele mesaje e-mail care corespund acelor tipare vor fi marcate ca `[spam]`.
2. Adăugați spammerii pe Lista de spammeri. Mesajele e-mail primite de la adrese de pe Lista de spammeri sunt marcate automat ca `[spam]`.
3. Creșteți nivelul protecției antispam. Prin creșterea nivelului de protecție antispam, filtrul antispam va avea nevoie de mai puține indicii pentru a clasifica un mesaj e-mail ca spam.
4. Re-educați Motorul de învățare (filtrul Bayesian). Folosiți această soluție când detecția antispam nu mai este eficientă și indicarea mesajelor spam nedetectate nu mai funcționează.

Notă

BitDefender se integrează în clienții de mail cel mai frecvent utilizați, printr-o bară de instrumente antispam ușor de utilizat.Pentru o listă completă a clienților de mail admiși, consultați *„Cerințe software"* (p. 2).

Dacă folosiți un alt client de mail, nu puteți indica mesaje spam și antrena Motorul de învățare. Pentru a rezolva problema, încercați să creșteți nivelului protecției antispam și să adăugați spammeri pe Lista de spammeri.

Indicați mesajele spam nedetectate

Dacă folosiți un client de mail admis, puteți indica cu ușurință care mesaje e-mail ar fi trebuit să fie detectate ca spam. Astfel, veți îmbunătăți considerabil eficiența filtrului antispam.Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți la directorul Inbox.
3. Selectați mesajele spam nedetectate.

4. Faceți clic pe butonul **Este Spam** din bara de instrumente antispam BitDefender (localizată, de obicei, în zona de sus a ferestrei clientului de mail). Aceasta îi indică Motorului de învățare faptul că mesajele selectate sunt spam. Acestea sunt marcate imediat ca `[spam]` și mutate în directorul de mesaje nesolicitate (junk).Următoarele mesaje e-mail care corespund acelor tipare vor fi marcate ca `[spam]`.

Adăugați spammeri pe Lista de spammeri

Dacă folosiți un client de mail admis, puteți adăuga foarte ușor expeditorii de mesaje spam pe Lista de spammeri.Urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Mergeți în directorul cu mesaje nesolicitate (junk), în care sunt mutate mesajele spam.
3. Selectați mesajele pe care BitDefender le-a marcat ca `[spam]`.
4. Faceți clic pe butonul **Adaugă spammer** din bara de instrumente antispam BitDefender.
5. Vi se poate cere să confirmați adresa adăugată pe Lista de spammeri.Selectați **Nu mai afișa acest mesaj** și faceți clic pe **OK**.

Dacă folosiți un alt client de mail, puteți să adăugați manual spammeri pe Lista de spammeri, din interfața BitDefender. Este recomandat să procedați astfel numai atunci când ați primit mai multe mesaje spam de la aceeași adresă de e-mail.Urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Faceți clic pe **Antispam** în meniul din stânga.
3. Faceți clic pe tabul **Stare**.
4. Faceți clic pe **Administrează spammeri**.Va apărea o fereastră de configurare.
5. Introduceți adresa de e-mail a spammerului și faceți clic pe butonul pentru a adăuga adresa pe Lista de spammeri.
6. Faceți clic pe **OK** pentru a salva modificările și închide fereastra.

Creșteți nivelul protecției antispam

Pentru a crește nivelul protecției antispam, urmați acești pași:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Faceți clic pe **Antispam** în meniul din stânga.
3. Faceți clic pe tabul **Stare**.

4. Mutați cursorul mai sus pe scală.

Re-educați Motorul de învățare (Bayesian)

Înainte de a educa Motorul de învățare (Bayesian), pregătiți un director care să conțină numai mesaje SPAM și un altul doar cu mesaje legitime. Motorul de învățare le va analiza și va învăța caracteristicile definitorii pentru mesajele spam sau legitime pe care le primiți de obicei. Pentru ca educarea să fie eficientă, trebuie să existe cel puțin 50 de mesaje în fiecare categorie.

Pentru a reseta baza de date Bayesiană și pentru a re-educa Motorul de învățare, urmați acești pași:

1. Deschideți clientul dumneavoastră de mail.
2. Pe bara de instrumente antispam BitDefender, faceți clic pe butonul **Asistent** pentru a porni programul asistent de configurare antispam.
3. Faceți clic pe **Înainte**.
4. Selectați **Omite** și faceți clic pe **Înainte**.
5. Selectați **Șterge baza de date a filtrului antispam** și faceți clic pe **Înainte**.
6. Selectați directorul care conține mesaje legitime și faceți clic pe **Înainte**.
7. Selectați directorul care conține mesaje SPAM și faceți clic pe **Înainte**.
8. Faceți clic pe **Finalizează** pentru a începe procesul de educare.
9. Când educarea a luat sfârșit, faceți clic pe **Închide**.

Solicitați ajutor

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport"* (p. 199).

33.12.3. Filtrul antispam nu detectează niciun mesaj spam

Dacă niciun mesaj spam nu este marcat ca `[spam]`, este posibil să existe probleme legate de filtrul Antispam BitDefender.Înainte de a remedia această problemă, asigurați-vă că ea nu se datorează următoarelor cauze:

- Protecția antispam BitDefender este disponibilă numai pentru clienții de e-mail configurați să primească mesaje e-mail prin protocolul POP3.Aceasta înseamnă că:
  - Mesajele e-mail primite prin servicii de e-mail oferite online (cum ar fi Yahoo, Gmail, Hotmail sau altele) nu sunt supuse verificării antispam de către BitDefender.

▶ Dacă aveți un client de e-mail configurat să primească mesaje prin alt protocol decât POP3 (de exemplu IMAP4), BitDefender nu supune aceste mesaje unei verificări antispam.

Notă

POP3 este unul dintre cele mai des folosite protocoale de descărcare a mesajelor e-mail de pe un server de mail.Dacă nu știți ce protocol folosește clientul dumneavoastră de e-mail pentru a descărca mesajele, întrebați persoana care l-a configurat.

- BitDefender Internet Security 2011 nu scanează traficul POP3 generat de Lotus Notes.

Verificați, de asemenea, dacă nu a intervenit una din următoarele cauze:

1. Asigurați-vă că modulul Antispam este activat.
   a. Deschideți BitDefender.
   b. Faceți clic pe butonul **Opțiuni** din colțul dreapta sus al ferestrei și alegeți **Preferințe**.
   c. În categoria Setări de securitate, verificați starea protecției antispam.

   Dacă protecția Antispam este dezactivată, aceasta este cauza problemei dvs. Activați protecția Antispam și monitorizați funcționarea acesteia pentru a vedea dacă problema este rezolvată.
2. Deși este puțin probabil, verificați dacă dumneavoastră (sau altcineva) ați configurat BitDefender să nu marcheze mesajele spam ca `[spam]`.
   a. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
   b. Faceți clic pe **Antispam** în meniul din stânga și apoi pe tabul **Setări**.
   c. Asigurați-vă că opțiunea **Marchează mesajele cu spam în subiect** este selectată.

O soluție posibilă este repararea sau reinstalarea produsului. Dacă doriți, puteți contacta BitDefender pentru suport, folosind informațiile din secțiunea *„Suport”* (p. 199).

33.13. Nu s-a reușit dezinstalarea BitDefender

Acest articol vă ajută să remediați erorile care pot apărea la dezinstalarea BitDefender.Sunt posibile două situații:

- În timpul dezinstalării apare un ecran de eroare. Ecranul oferă un buton pentru rularea unui instrument de dezinstalare, care va curăța sistemul.
- Dezinstalarea nu înaintează și, eventual, sistemul se blochează. Faceți clic pe **Anulează** pentru a abandona dezinstalarea. Dacă anularea nu este posibilă, reporniți sistemul.

Dacă dezinstalarea eșuează, unele chei de regiștri și fișiere BitDefender pot rămâne în sistemul dumneavoastră. Aceste rămășite pot împiedica instalarea ulterioară a BitDefender. De asemenea, ele pot afecta funcționarea și stabilitatea sistemului.Pentru a dezinstala BitDefender complet de pe sistemul dumneavoastră, trebuie să rulați instrumentul de dezinstalare.

Pentru mai multe informații, consultați *„Cum dezinstalez complet BitDefender?”* (p. 208).

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport”* (p. 199).

34. Eliminarea virușilor din sistem

Virușii și celelalte amenințări malware vă pot afecta sistemul în moduri diferite, iar modul de acțiune al BitDefender depinde de tipul de atac malware.Deoarece virușii își schimbă comportamentul în mod frecvent, este dificil de stabilit un model privind comportamentul și acțiunile acestora.

Există cazuri când BitDefender nu poate elimina în mod automat infecția malware din sistemul dumneavoastră.În astfel de cazuri, este necesară intervenția dumneavoastră.

Dacă problema dumneavoastră nu este prezentată aici sau dacă soluțiile oferite nu vă sunt de ajutor, puteți contacta echipa de suport tehnic a BitDefender folosind informațiile din capitolul *„Suport”* (p. 199).

34.1. BitDefender Rescue CD

Rescue CD BitDefender este o funcție inclusă în majoritatea CD-urilor de instalare BitDefender care permite scanarea și dezinfectarea tuturor hard disk-urilor existente înainte de lansarea sistemului de operare.Vă poate ajuta de asemenea să salvați date de pe sistemul dumneavoastră Windows, dacă acesta a fost compromis, pe un dispozitiv detașabil.

Dacă nu dețineți un BitDefender Rescue CD, îl puteți descărca sub forma unei imagini ISO din această locație:

http://download.bitdefender.com/rescue_cd/

Descărcați fișierul .iso și scrieți-l pe un CD sau DVD, folosind programul preferat.

Scanarea sistemului cu BitDefender Rescue CD

Pentru a vă scana sistemul folosind BitDefender Rescue CD, urmați acești pași:

1. Configurați BIOS-ul calculatorului dumneavoastră pentru a porni sistemul de operare de pe CD.
2. Plasați CD-ul în unitate și reporniți calculatorul.
3. Așteptați până ce apare ecranul BitDefender și selectați **Start Rescue CD BitDefender** în limba dorită.
4. Așteptați finalizarea procesului de pornire. Aceasta poate dura câteva momente.
5. De îndată ce sistemul de operare a fost pornit, semnăturile de BitDefender sunt actualizate automat. În același timp, sunt scanate toate partițiile detectate ale hard-discului.

Salvarea datelor cu BitDefender Rescue CD

Să presupunem că nu vă puteți porni sistemul dumneavoastră Windows, din cauza unor probleme necunoscute. În același timp, trebuie neapărat să accesați date importante de pe calculatorul dumneavoastră. Aici este util BitDefender Rescue CD.

Pentru a vă salva datele de pe calculator pe un dispozitiv de stocare portabil, cum ar fi un stick de memorie USB, urmați acești pași:

1. Configurați BIOS-ul calculatorului dumneavoastră pentru a porni sistemul de operare de pe CD.
2. Plasați CD-ul în unitate și reporniți calculatorul.
3. Așteptați până ce apare ecranul BitDefender și selectați **Start Rescue CD BitDefender** în limba dorită.
4. Așteptați finalizarea procesului de pornire. Aceasta poate dura câteva momente.
5. De îndată ce sistemul de operare a fost pornit, semnăturile de BitDefender sunt actualizate automat. În același timp, sunt scanate toate partițiile detectate ale hard-discului.

   Partițiile de pe hard disc vor apărea pe desktop. Pentru a vizualiza conținutul unei partiții într-o fereastră similară cu Windows Explorer, faceți dublu-clic pe aceasta.

   Notă

   Atunci când lucrați cu BitDefender Rescue CD, numele partițiilor sunt afișate conform convențiilor din mediul Linux. Partițiile care nu au fost etichetate în Windows vor apărea sub forma `[LocalDisk-0]`, corespunzătoare partiției Windows `(C:)`, `[LocalDisk-1]`, corespunzătoare partiției `(D:)` și așa mai departe.

6. Conectați dispozitivul de stocare portabil într-unul dintre porturile USB ale calculatorului dumneavoastră.În câteva momente, o fereastră va apărea indicând conținutul dispozitivului.
7. Puteți copia fișiere și directoare așa cum ați proceda în mod normal, în mediul Windows.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport”* (p. 199).

34.2. Ce trebuie să fac atunci când BitDefender găsește viruși pe calculatorul meu?

Puteți afla că în calculatorul dumneavoastră se află un virus într-unul dintre aceste moduri:

- V-ați scanat calculatorul și BitDefender a găsit elemente infectate pe acesta.
- O alertă de viruși vă informează că BitDefender a blocat unul sau mai mulți viruși pe calculatorul dumneavoastră.

În astfel de situații, actualizați BitDefender pentru a vă asigura că aveți cele mai recente semnături malware și porniți o scanare profundă a sistemului.

După finalizarea scanării, selectați acțiunea dorită pentru elementele infectate (dezinfectare, ștergere, mutare în carantină).

Avertisment
În cazul în care considerați că fișierul face parte din sistemul de operare Windows sau că nu este un fișier infectat, nu urmați acești pași și contactați serviciul de asistență clienți BitDefender cât mai curând posibil.

Dacă acțiunea selectată nu a putut fi efectuată, iar jurnalul de scanare indică o infectare care nu a putut fi eliminată, trebuie să ștergeți fișierul/fișierele manual:

Prima metodă poate fi utilizată în modul normal:

1. Dezactivați protecția antivirus în timp real a BitDefender.Pentru a afla cum să procedați, consultați *„Cum activez/dezactivez protecția în timp real?"* (p. 208).
2. Afișați elementele ascunse din Windows.Pentru a afla cum să procedați, consultați *„Cum pot afișa elementele ascunse din Windows?"* (p. 209).
3. Mergeți la locația unde se găsește fișierul infectat (verificați jurnalul de scanare) și ștergeți-l.
4. Activați protecția antivirus în timp real a BitDefender.

În cazul în care prima metodă nu a reușit să elimine infecția, urmați acești pași:

1. Reporniți sistemul în Safe Mode.Pentru a afla cum să procedați, consultați *„Cum pot reporni sistemul în Safe Mode?"* (p. 207).
2. Afișați elementele ascunse din Windows.
3. Mergeți la locația unde se găsește fișierul infectat (verificați jurnalul de scanare) și ștergeți-l.
4. Reporniți sistemul în mod normal.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport"* (p. 199).

34.3. Cum șterg un virus dintr-o arhivă?

O arhivă este un fișier sau o colecție de fișiere comprimate într-un format special, în scopul reducerii spațiului de pe hard-disc necesar stocării fișierelor.

Unele dintre aceste formate sunt formate deschise, ceea ce permite BitDefender să scaneze în interiorul acestora și apoi să ia măsurile corespunzătoare pentru eliminarea infecțiilor.

Alte formate de arhivă sunt închise complet sau parțial, iar BitDefender poate identifica numai prezența virușilor din acestea însă nu poate lua niciun fel de măsură în acest sens.

Dacă BitDefender vă anunță că a fost detectat un virus într-o arhivă și nu este disponibilă nicio acțiune, aceasta înseamnă că eliminarea virusului nu este posibilă din cauza restricțiilor legate de setările referitoare la permisiunile arhivelor.

Iată cum puteți elimina un virus stocat într-o arhivă:

1. Identificați arhiva care conține virusul prin realizarea unei scanări profunde a sistemului.
2. Dezactivați protecția antivirus în timp real a BitDefender.
3. Accesați locația arhivei și dezarhivați-o utilizând o aplicație de arhivare, cum ar fi WinZip.
4. Identificați fișierul infectat și ștergeți-l.
5. Ștergeți arhiva inițială pentru a vă asigura că fișierul infectat este eliminat în totalitate.
6. Recomprimați fișierele într-o nouă arhivă utilizând o aplicație de arhivare, cum ar fi WinZip.
7. Activați protecția antivirus în timp real a BitDefender și porniți o scanare profundă a sistemului pentru a vă asigura că nu mai există nicio altă infecție.

Notă

Este important de reținut faptul că un virus aflat într-o arhivă nu reprezintă o amenințare imediată la adresa sistemului dumneavoastră deoarece virusul trebuie să fie dezarhivat și executat pentru a putea infecta calculatorul.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport”* (p. 199).

34.4. Cum șterg un virus dintr-o arhivă de e-mail?

BitDefender poate de asemenea să identifice viruși din bazele de date de e-mail și arhivele de e-mail stocate pe disc.

Uneori este necesară identificarea mesajului infectat utilizând informațiile puse la dispoziție în raportul de scanare și ștergerea acestuia în mod manual.

Iată cum puteți elimina un virus stocat într-o arhivă de e-mail:

1. Scanați baza de date de e-mail folosind BitDefender.

2. Dezactivați protecția antivirus în timp real a BitDefender.
3. Deschideți raportul de scanare și utilizați informațiile de identificare (Subiect, De la, Către) aferente mesajelor infectate pentru a le localiza în clientul de e-mail.
4. Ștergeți mesajele infectate.Majoritatea clienților de e-mail mută mesajul șters într-un director de recuperare, de unde acesta poate fi recuperat.Trebuie să vă asigurați că mesajul este șters și din acest director de recuperare.
5. Arhivați directorul în care se află mesajul infectat.
   - În Outlook Express:În meniul File, faceți clic pe Folder și apoi pe Compact All Folders.
   - În Microsoft Outlook:În meniul File, faceți clic pe Data File Management.Selectați fișierele din directoarele personale (.pst) pe care intenționați să le compactați și faceți clic pe Settings.Faceți clic pe Compact.
6. Activați protecția antivirus în timp real a BitDefender.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport"* (p. 199).

34.5. Cum scanez calculatorul în Safe Mode?

Opțiunea Scanare manuală BitDefender vă permite să scanați un anumit director sau partiție de hard-disc, fără a crea o sarcină de scanare.

Această funcționalitate a fost concepută pentru a fi utilizată atunci când Windows funcționează în Safe Mode.

Dacă sistemul dumneavoastră este infectat cu un virus care nu poate fi eliminat în urma unei scanări normale, puteți încerca să eliminați virusul pornind Windows în Safe Mode și scanând fiecare partiție de hard-disc folosind opțiunea Scanare manuală BitDefender.

Pentru a afla cum puteți accesa Safe Mode, consultați *„Cum pot reporni sistemul în Safe Mode?"* (p. 207).

1. Pentru a vă scana calculatorul folosind Scanarea manuală BitDefender, urmați calea din meniul Start al Windows: **Start → Toate programele → BitDefender 2011 → Scanare manuală BitDefender**.
2. Faceți clic pe **Adaugă director** pentru a selecta ținta de scanare. Va apărea o nouă fereastră.
3. Selectați ținta scanării :
   - pentru a vă scana desktopul, selectați **Desktop**.
   - pentru a scana o întreagă partiție de pe hard-disc, selectați-o din **My Computer**.
   - pentru a scana un anumit director, căutați și selectați directorul respectiv.

4. Faceți clic pe **Ok** și pe **Continuă** pentru a începe scanarea.
5. Urmați programul asistent de scanare pentru a finaliza scanarea.

34.6. Ce este de făcut atunci când BitDefender a detectat un fișier curat ca fiind infectat?

Există situații când BitDefender marchează în mod greșit un fișier legitim ca fiind o amenințare.Pentru a corecta această eroare, adăugați fișierul în secțiunea de excluderi a BitDefender:

1. Dezactivați protecția antivirus în timp real a BitDefender.Pentru a afla cum să procedați, consultați *„Cum activez/dezactivez protecția în timp real?"* (p. 208).
2. Afișați elementele ascunse din Windows.Pentru a afla cum să procedați, consultați *„Cum pot afișa elementele ascunse din Windows?"* (p. 209).
3. Restaurați fișierul din zona de carantină.
4. Introduceți fișierul în zona de excluderi.
5. Activați protecția antivirus în timp real a BitDefender.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport"* (p. 199).

34.7. Cum să curățați fișierele infectate din System Volume Information

Directorul System Volume Information se află într-o zonă a hard-discului creată de către sistemul de operare și utilizată de Windows pentru stocarea de informații critice referitoare la configurația sistemului.

Motoarele BitDefender pot detecta orice fișiere infectate stocate de către System Volume Information, însă aceasta fiind o zonă protejată, fișierele nu pot fi șterse.

Fișierele infectate detectate în directoarele System Restore vor apărea în jurnalul de scanare după cum urmează:

```
?:\System Volume Information\_restore{B36120B2-BA0A-4E5D-…
```

Pentru a șterge complet și imediat fișierele infectate din locul unde sunt stocate, dezactivați și reactivați funcția System Restore.

Atunci când funcția System Restore este dezactivată, toate punctele de restaurare sunt șterse.

Atunci când funcția System Restore este activată din nou, sunt create noi puncte de restaurare conform programării și evenimentelor apărute.

Pentru a dezactiva funcția System Restore, urmați acești pași:

- **Pentru Windows XP:**

1. Urmați această cale: **Start** → **All Programs** → **Accessories** → **System Tool** → **System Restore**
2. Faceți clic pe **System Restore Settings** în partea stângă a ferestrei.
3. Bifați căsuța **Turn off System Restore** pentru toate unitățile și faceți clic pe **Apply**.
4. Atunci când sunteți avertizat că toate punctele de restaurare vor fi șterse, faceți clic pe **Yes** pentru a continua.
5. Pentru a activa funcția System Restore, debifați căsuța **Turn off System Restore** pentru toate unitățile și faceți clic pe **Apply**.

- **Pentru Windows Vista:**

1. Urmăriți această cale: **Start** → **Control Panel** → **System and Maintenance** → **System**
2. În panoul stâng, faceți clic pe **System protection**.

   Dacă vi se solicită să introduceți o parolă de administrator sau să confirmați, introduceți parola sau confirmați.
3. Pentru a dezactiva funcția System Restore, debifați căsuțele corespunzătoare fiecărei unități și faceți clic pe **Ok**.
4. Pentru a activa funcția System Restore, bifați căsuțele corespunzătoare fiecărei unități și faceți clic pe **Ok**.

- **Pentru Windows 7:**

1. Faceți clic pe **Start**, clic-dreapta pe **Computer** și alegeți **Properties**.
2. Faceți clic pe linkul **System protection** din panoul stâng.
3. Din opțiunile **System protection**, selectați fiecare literă de unitate și faceți clic pe **Configure**.
4. Selectați **Turn off system protection** și faceți clic pe **Apply**.
5. Faceți clic pe **Delete**, pe **Continue** atunci când vi se solicită acest lucru și apoi pe **Ok**.

Dacă aceste informații nu v-au fost de folos, vă rugăm să contactați BitDefender pentru asistență, așa cum se arată în secțiunea *„Suport”* (p. 199).

34.8. Ce reprezintă fișierele protejate prin parolă din jurnalele de scanare?

Aceasta reprezintă doar o notificare referitoare la faptul că BitDefender a detectat aceste fișiere ca fiind protejate fie prin parolă, fie cu o anumită formă de criptare.

Cel mai frecvent, elementele protejate prin parolă sunt următoarele:

- Fișiere care aparțin unei alte soluții de securitate.
- Fișiere care aparțin sistemului de operare.

Pentru a putea scana conținutul, aceste fișiere trebuie să fie extrase sau decriptate.

În cazul în care conținutul respectiv este extras, BitDefender va scana automat conținutul pentru a vă proteja calculatorul.Dacă doriți să scanați acele fișiere folosind BitDefender, trebuie să contactați producătorul produsului pentru a obține mai multe detalii despre respectivele fișiere.

Noi vă recomandăm să ignorați acele fișiere deoarece acestea nu reprezintă o amenințare pentru sistemul dumneavoastră.

34.9. Ce reprezintă elementele omise din jurnalul de scanare?

Toate fișierele care apar ca fiind omise în raportul de scanare nu conțin niciun fel de viruși.

Pentru performanțe sporite, BitDefender nu scanează fișiere care nu au fost modificate de la ultima scanare.

34.10. Ce reprezintă fișierele supracomprimate din jurnalul de scanare?

Elementele supracomprimate sunt elemente care nu au putut fi extrase de către motorul de scanare sau elemente pentru care timpul necesar decriptării ar fi fost prea lung ducând la instabilitatea sistemului.

Supracomprimarea se referă la faptul că BitDefender a sărit peste scanarea respectivei arhive deoarece dezarhivarea acesteia s-a dovedit a consuma prea mult din resursele sistemului. Conținutul va fi scanat în timp real, la accesare, dacă este cazul.

34.11. De ce BitDefender a șters în mod automat un fișier infectat?

În cazul în care este detectat un fișier infectat, BitDefender va încerca în mod automat să-l dezinfecteze.Dacă dezinfectarea nu reușește, fișierul este mutat în carantină pentru a bloca infecția.

Pentru anumite tipuri de malware, dezinfectarea nu este posibilă deoarece fișierul detectat este în întregime periculos. În astfel de situații, fișierul infectat este șters de pe disc.

Acesta este cazul fișierelor de instalare care sunt descărcate de pe site-uri web nesigure.Dacă vă aflați într-o astfel de situație, descărcați fișierul de instalare de pe site-ul web al producătorului sau de pe un alt site web sigur.

35. Suport

BitDefender se străduiește să ofere clienților săi un nivel neegalat în ceea ce privește rapiditatea și acuratețea suportului tehnic.Dacă vă confruntați cu o problemă sau aveți o întrebare referitoare la produsul BitDefender deținut, puteți utiliza un număr de resurse online pentru a găsi rapid o soluție sau un răspuns.Sau, dacă preferați, puteți contacta serviciul de asistență clienți al BitDefender. Reprezentanții noștri vă vor răspunde la întrebări la timp și vă vor oferi asistența de care aveți nevoie.

35.1. Resurse online

Sunt disponibile mai multe resurse online pentru a vă ajuta la soluționarea problemelor și întrebărilor referitoare la produsul BitDefender.

- BitDefender Knowledge Base:http://www.bitdefender.com/help
- forumul de suport al BitDefender:http://forum.bitdefender.com
- portalul de securitate informatică Malware City:http://www.malwarecity.com
- tutorialele video

De asemenea, puteți folosi motorul de căutare preferat pentru a afla informații suplimentare privind securitatea calculatoarelor, produsele și compania BitDefender.

35.1.1. BitDefender Knowledge Base

BitDefender Knowledge Base este o bază online de informații despre produsele BitDefender. Stochează, într-un format accesibil, rapoarte ale echipelor de suport și dezvoltare cu privire la rezultatele suportului tehnic continuu și ale activităților de eliminare a bugurilor BitDefender împreună cu articole mai generale despre prevenția virușilor, administrarea soluțiilor BitDefender și explicații detaliate, și multe alte articole.

BitDefender Knowledge Base este pusă la dispoziția publicului. Această multitudine de informații reprezintă încă o cale de a oferi clienților BitDefender asistența tehnică de care au nevoie. Toate cererile valide de informații sau rapoarte despre buguri venind de la clienții BitDefender ajung în cele din urmă în BitDefender Knowledge Base, ca rapoarte asupra eliminării bugurilor, fișe de lucru sau articole informative pentru a suplimenta fișierele de suport ale produsului.

BitDefender Knowledge Base este disponibilă oricând la adresa http://kb.bitdefender.com.

35.1.2. Forumul de suport al BitDefender

Forumul de suport al BitDefender le oferă utilizatorilor BitDefender o modalitate facilă de a obține ajutor și de a-i ajuta pe alții.

În cazul în care produsul dumneavoastră BitDefender nu funcționează bine, nu poate înlătura anumiți viruși de pe calculator sau dacă aveți întrebări referitoare la modul de funcționare, postați problema sau întrebarea pe forum.

Reprezentanții de suport tehnic ai BitDefender monitorizează forumul pentru a verifica noile postări cu scopul de a vă ajuta. De asemenea, puteți obține un răspuns sau o soluție de la un utilizator BitDefender cu mai multă experiență.

Înainte de a posta problema sau întrebarea, sunteți rugat să verificați în forum existența unui subiect similar sau corelat.

Forumul de suport al BitDefender este disponibil la http://forum.bitdefender.com, în 5 limbi diferite: engleză, germană, franceză, spaniolă și română.Faceți clic pe linkul **Home & Home Office Protection** pentru a accesa secțiunea dedicată produselor pentru consumatori individuali.

35.1.3. Portalul Malware City

Portalul Malware City constituie o sursă bogată de informații privind securitatea informatică. Aici puteți afla informații despre diversele pericole la care este expus calculatorul dumneavoastră atunci când este conectat la internet (malware, phishing, spam, infracțiuni cibernetice).Un dicționar util vă ajută la înțelegerea termenilor de securitate a calculatoarelor cu care nu sunteți familiarizați.

Se postează în mod regulat noi articole pentru a vă ține la curent cu cele mai recente pericole descoperite, tendințele actuale din domeniul securității și alte informații din domeniul securității calculatoarelor.

Pagina web a Malware City este http://www.malwarecity.com.

35.1.4. Tutoriale video

Tutorialele video vă vor conduce pas cu pas prin procedura de configurare a produsului.Acestea sunt create într-o manieră directă și realistă care transmite mesajele la destinație.

Cel mai important obiectiv este asigurarea unei experiențe plăcute prin oferirea de informații de nivel de bază și intermediar privind principiile de securitate, modul de configurare și modul de utilizare a BitDefender.

Principalul obiectiv este înlocuirea necesarului de asistență specializată prin utilizarea de tutoriale video pentru produse care oferă informații strict legate de modul de utilizare și configurare a BitDefender.

De exemplu, în loc să apelați la serviciul de asistența clienți al BitDefender pentru instrucțiuni sau să încercați să urmați proceduri complicate, puteți urmări și respecta pașii prezentați în cadrul tutorialelor video.

35.2. Solicitarea ajutorului

Secțiunea **Depanare probleme și asistență profesională** vă oferă informațiile necesare referitoare la cele mai frecvent întâlnite probleme atunci când utilizați acest produs.

Dacă nu găsiți o soluție la problema dumneavoastră printre resursele puse la dispoziție, ne puteți contacta direct:

- „Contactați-ne direct din cadrul produsului dumneavoastră BitDefender” (p. 201)
- „Contactați-ne prin intermediul bazei noastre de cunoștințe online” (p. 202)

Important

Pentru a contacta serviciul de asistență clienți BitDefender, produsul dumneavoastră BitDefender trebuie să fie activat.Pentru mai multe informații, consultați *„Înregistrare și Contul meu”* (p. 52).

Contactați-ne direct din cadrul produsului dumneavoastră BitDefender

Dacă dispuneți de o conexiune la internet funcțională (acces la internet), puteți contacta BitDefender pentru asistență direct din fereastra programului dumneavoastră.

Pentru a solicita asistență, puteți utiliza asistența integrată care vă este pusă la dispoziție în cadrul produsului.

Pentru a utiliza asistența integrată, urmați acești pași:

1. Deschideți BitDefender.
2. Faceți clic pe linkul **Asistență** din colțul dreapta jos al ferestrei.
3. Acum aveți două opțiuni:
   - Efectuați o căutare în baza noastră de date după informațiile de care aveți nevoie.
   - Selectați departamentul în funcție de problema întâlnită.

     Licențiere se ocupă de achiziții, licențe, despăgubiri sau reînnoiri.

     Asistența tehnică acoperă aspecte legate de produsul însuși și de funcționarea acestuia.

     Luptă împotriva malware se referă la probleme legate de viruși.
4. Citiți articolele sau documentele relevante și încercați soluțiile propuse.
5. Dacă soluția nu vă rezolvă problema, utilizați linkul din articol pentru a lansa instrumentul de asistență.
6. Introduceți-vă adresa de e-mail, selectați departamentul și scrieți o scurtă descriere a problemei respective.

Faceți clic pe **Înainte**.

7. Vă rugăm să așteptați câteva minute pentru ca BitDefender să adune informații referitoare la produs. Aceste informații îi vor ajuta pe inginerii noștri să găsească o soluție la problema dumneavoastră.

   Faceți clic pe **Înainte**.

8. Faceți clic pe **Finalizare** pentru a transmite informațiile serviciului de asistență clienți al BitDefender. Veți fi contactat cât mai curând posibil.

Contactați-ne prin intermediul bazei noastre de cunoștințe online

Dacă nu puteți accesa informațiile necesare utilizând produsul BitDefender, consultați baza noastră de cunoștințe online:

1. Mergeți la http://www.bitdefender.com/help.BitDefender Knowledge Base oferă numeroase articole care conțin soluții la probleme legate de utilizarea soluțiilor BitDefender.
2. Căutați în BitDefender Knowledge Base articole care vă pot ajuta să rezolvați problema pe care o întâmpinați.
3. Citiți articolele sau documentele relevante și încercați soluțiile propuse.
4. Dacă soluția nu vă rezolvă problema, utilizați linkul din articol pentru a contacta serviciul de asistență clienți al BitDefender.
5. Contactați reprezentanții BiDefender prin e-mail, pe chat sau la telefon.

36. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. În ultimii 10 ani BitDefender a câștigat o reputație indisputabilă în depășirea așteptărilor clienților și partenerilor, căutând în mod constant mijloace pentru o comunicare eficientă. Nu ezitați să ne contactați indiferent ce problemă sau întrebare ați avea.

36.1. Adrese Web

Departament de vânzări: sales@bitdefender.ro
Suport tehnic:www.bitdefender.com/help
Documentație: documentation@bitdefender.com
Programe de Parteneriat: partners@bitdefender.com
Marketing: marketing@bitdefender.com
Relații Media: pr@bitdefender.com
Cariere: jobs@bitdefender.com
Subscrieri viruși: virus_submission@bitdefender.com
Subscrieri spam: spam_submission@bitdefender.com
Raportare abuz: abuse@bitdefender.com
Website-ul produsului:http://www.bitdefender.com
Arhive ftp ale produsului:ftp://ftp.bitdefender.com/pub
Distribuitori locali:http://www.bitdefender.com/site/Partnership/list/
BitDefender Knowledge Base:http://kb.bitdefender.com

36.2. Distribuitori locali

Distribuitorii locali BitDefender sunt pregătiți să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale.

Pentru a găsi un distribuitor BitDefender în țara dumneavoastră:

1. Mergeți la http://www.bitdefender.com/site/Partnership/list/.
2. Datele de contact ale distribuitorilor locali BitDefender ar trebui să se afișeze automat. În caz contrar, folosiți instrumentul Partner Locator din meniul din stânga pentru a selecta zona și țara de reședință.
3. În cazul în care nu găsiți un distribuitor BitDefender în țara dumneavoastră, nu ezitați să ne contactați prin e-mail la adresa sales@bitdefender.com.Vă rugăm să scrieți mesajul în engleză pentru a ne da posibilitatea să vă ajutăm cu promptitudine.

36.3. Filialele BitDefender

Sucursalele BitDefender sunt pregătite să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale. Adresele lor precum și modul în care pot fi contactate sunt date mai jos.

Romania

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest
Fax: +40 21 2641799
Telefon vânzări: +40 21 2063470
E-mail vânzări: sales@bitdefender.ro
Suport tehnic: http://www.bitdefender.ro/suport
Site web: http://www.bitdefender.ro

U.S.A

BitDefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
Telefon (birou&vânzări): 1-954-776-6262
Vânzări: sales@bitdefender.com
Suport tehnic: http://www.bitdefender.com/help
Web: http://www.bitdefender.com

Germany

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
Birou: +49 2301 91 84 222
Vânzări: vertrieb@bitdefender.de
Suport tehnic: http://kb.bitdefender.de
Web: http://www.bitdefender.de

Marea Britanie și Irlanda

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
E-mail: info@bitdefender.co.uk
Telefon: +44 (0) 8451-305096

Vânzări: sales@bitdefender.co.uk
Suport tehnic: http://www.bitdefender.com/help
Web: http://www.bitdefender.co.uk

Spain

BitDefender España, S.L.U.
Avda. Diagonal, 357, 1º 1ª
08037 Barcelona
Fax: +34 93 217 91 28
Telefon: +34 902 19 07 65
Vânzări: comercial@bitdefender.es
Suport tehnic: www.bitdefender.es/ayuda
Site web: http://www.bitdefender.es

37. Informații utile

Acest capitol prezintă câteva proceduri importante pe care trebuie să le aveți în vedere înainte de a începe depanarea unei probleme tehnice.

Remedierea unei probleme de natură tehnică a BitDefender necesită anumite cunoștințe despre Windows; ca atare, următoarele instrucțiuni se referă în mare măsură la sistemul de operare Windows.

37.1. Cum dezinstalez alte soluții de securitate?

Principalul motiv pentru utilizarea unei soluții de securitate este de a asigura protecția și siguranța datelor dumneavoastră.Ce se întâmplă însă când aveți mai multe produse de securitate instalate în același sistem?

Atunci când utilizați mai multe soluții de securitate pe același calculator, sistemul devine instabil.Programul de instalare a BitDefender Internet Security 2011 detectează în mod automat alte programe de securitate și vă oferă opțiunea de a le dezinstala.

Dacă nu ați dezinstalat celelalte soluții de securitate în timpul instalării inițiale, urmați acești pași:

- Pentru **Windows XP**:
  1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Add / Remove programs**.
  2. Așteptați câteva momente până când este afișată lista programelor instalate.
  3. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Remove**.
  4. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.
- Pentru **Windows Vista** și **Windows 7**:
  1. Faceți clic pe **Start**, mergeți la **Control Panel** și faceți clic pe **Programs and Features**.
  2. Așteptați câteva momente până când este afișată lista programelor instalate.
  3. Găsiți numele programului pe care doriți să-l dezinstalați și selectați **Uninstall**.
  4. Așteptați ca procesul de dezinstalare să ia sfârșit, iar apoi reporniți sistemul.

Dacă nu reușiți să dezinstalați cealaltă soluție de securitate, faceți rost de instrumentul de dezinstalare de pe site-ul web al furnizorului sau contactați-l direct pentru a vă oferi instrucțiuni de dezinstalare.

37.2. Cum pot reporni sistemul în Safe Mode?

Safe Mode este un mod de funcționare de diagnosticare, utilizat în principal pentru depanarea problemelor care afectează funcționarea normală a sistemului Windows.Printre astfel de probleme se numără driverele incompatibile și virușii ce împiedică pornirea normală a sistemului Windows.În Safe Mode funcționează numai câteva aplicații, iar Windows încarcă doar driverele de bază și un minim de componente ale sistemului de operare.Acesta este motivul pentru care majoritatea virușilor sunt inactivi atunci când Windows se află în Safe Mode și pot fi eliminați cu ușurință.

Pentru a porni Windows în Safe Mode:

1. Reporniți calculatorul.
2. Apăsați tasta **F8** de mai multe ori înainte ca Windows să pornească pentru a avea acces la meniul de pornire.
3. Selectați **Safe Mode** din meniul de pornire și apăsați pe **Enter**.
4. Așteptați până ce Windows se încarcă în Safe Mode.
5. Acest proces se finalizează cu un mesaj de confirmare.Faceți clic pe **Ok** pentru a confirma.
6. Pentru a porni Windows în mod normal, reporniți pur și simplu sistemul.

37.3. Utilizez o versiune Windows pe 32 biți sau pe 64 biți?

Pentru a identifica dacă utilizați un sistem de operare pe 32 sau 64 de biți, urmați acești pași:

- Pentru **Windows XP**:
  1. Faceți clic pe **Start**.
  2. Mergeți la **My Computer** din meniul **Start**.
  3. Faceți clic-dreapta pe **My Computer** și selectați **Properties**.
  4. Dacă vedeți **x64 Edition** sub **System**, sistemul care rulează pe calculatorul dumneavoastră este o versiune Windows XP pe 64 biți.

     Dacă nu vedeți **x64 Edition** în listă, sistemul care rulează pe calculatorul dumneavoastră este o versiune Windows XP pe 32 biți.
- Pentru **Windows Vista** și **Windows 7**:
  1. Faceți clic pe **Start**.
  2. Localizați **Computer** din meniul **Start**.
  3. Faceți clic-dreapta pe **Computer** și selectați **Properties**.
  4. Sub **System** veți găsi informații referitoare la sistemul dumneavoastră.

37.4. Cum aflu care sunt setările mele proxy?

Pentru a găsi aceste setări, urmați acești pași :

- Pentru Internet Explorer 8:
  1. Deschideți Internet Explorer.
  2. Selectați **Tools** > **Internet Options**.
  3. În fila **Connections**, faceți clic pe **LAN settings**.
  4. Consultați secțiunea **Use a proxy server for your LAN** și veți vedea **adresa** și **portul** serverului proxy.
- Pentru Mozilla Firefox 3.6:
  1. Deschideți Firefox.
  2. Selectați **Tools** > **Options**.
  3. În fila **Advanced**, accesați fila **Network**.
  4. Faceți clic pe **Setări**.
- Pentru Opera 10.51:
  1. Deschideți Opera.
  2. Selectați **Tools** > **Preferences**.
  3. În fila **Advanced**, accesați fila **Network**.
  4. Faceți clic pe butonul **Proxy servers** pentru a deschide fereastra cu setările proxy.

37.5. Cum dezinstalez complet BitDefender?

Urmați acești pași pentru a dezinstala corect BitDefender:

1. Mergeți la www.bitdefender.com/uninstall și descărcați instrumentul de dezinstalare pe calculatorul dumneavoastră.
2. Rulați instrumentul de dezinstalare de pe un cont cu drepturi de administrator.
3. Reporniți calculatorul.

37.6. Cum activez/dezactivez protecția în timp real?

BitDefender oferă protecție continuă în timp real împotriva unui număr mare de amenințări malware scanând toate fișierele accesate, mesajele e-mail și comunicațiile prin programe de mesagerie instant (ICQ, NetMeeting, Yahoo Messenger, MSN Messenger).

În mod normal, protecția în timp real a BitDefender este activată și nu trebuie să o dezactivați.

Atunci când încercați să depanați o problemă sau să eliminați un virus, este posibil să fie nevoie să dezactivați protecția în timp real. Acestea se aplică în cazul uneia dintre următoarele situații:

- O încetinire a funcționării sistemului după instalarea BitDefender
- O problemă cu unul dintre programe sau una dintre aplicații după instalarea BitDefender
- Mesaje de eroare care ar putea apărea imediat după instalarea BitDefender

Urmați acești pași pentru a putea activa/dezactiva temporar protecția în timp real:

1. Deschideți BitDefender, faceți clic pe **Opțiuni** în colțul din dreapta sus al ferestrei și alegeți **Mod Expert**.
2. Mergeți la **Antivirus** > **Scut**.
3. Debifați căsuța **Protecția în timp real este activată** pentru a dezactiva temporar protecția antivirus (sau selectați-o dacă doriți să activați protecția).
4. Trebuie să confirmați alegerea prin selectarea din meniu a duratei dezactivării protecției în timp real.

Notă

Pașii pentru dezactivarea protecției în timp real asigurate de BitDefender trebuie utilizați ca soluție temporară și numai pe intervale scurte de timp.

37.7. Cum pot afișa elementele ascunse din Windows?

Acești pași sunt utili în acele cazuri în care aveți de-a face cu o situație în care este implicat un malware și trebuie să găsiți și să eliminați fișierele infectate, care pot fi ascunse.

Urmați acești pași pentru a afișa obiectele ascunse din Windows:

1. Faceți clic pe **Start**, mergeți la **Control Panel** și selectați **Folder Options**.
2. Mergeți la fila **View**.
3. Selectați **Display contents of system folders** (exclusiv pentru Windows XP).
4. Selectați **Show hidden files and folders**.
5. Debifați **Hide file extensions for known file types**.
6. Debifați **Hide protected operating system files**.
7. Faceți clic pe **Aplicare** și apoi pe **Ok**.

Vocabular

ActiveX

ActiveX este un mod de scriere a programelor astfel încât să poată fi apelate de celelalte programe și sisteme de operare. Tehnologia ActiveX este utilizată pentru realizarea de pagini Web interactive care se comportă ca niște aplicații și nu ca niște simple pagini statice. Cu elemente de ActiveX, utilizatorii pot răspunde la întrebări, să utilizeze butoane și să interacționeze și în alte moduri cu pagina Web. Controalele ActiveX sunt adesea scrise utilizând limbajul Visual Basic.

Active X este cunoscut pentru lipsa totală de control al securității; experții în securitatea calculatoarelor descurajează utilizarea lui pe Internet.

Adware

Aplicația adware este adesea combinată cu o aplicație gazdă care este oferită gratuit dacă utilizatorul acceptă aplicația adware. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licențiere care explică scopul aplicației, nu este comisă nicio infracțiune.

Totuși, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanțele sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații le adună pot cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licențiere.

Arhivă

Un disc, o casetă sau un director care conține fișiere de rezervă.

Un fișier care conține unul sau mai multe fișiere într-un format comprimat.

Backdoor

Reprezintă o gaură de securitate realizată în mod deliberat. Motivația acestor "găuri" nu este întotdeauna malițioasă: unele sisteme de operare, de exemplu, sunt puse în circulație cu conturi privilegiate pentru tehnicienii din service sau de responsabilii cu mentenanță produsului din partea vânzătorului.

Sector de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului și altele). În cazul discurilor de startup, sectorul de boot conține un program care încarcă sistemul de operare.

Virus de boot

Reprezintă un virus care infectează sectorul de boot al unui disc fix sau al unei dischete. Orice încercare de a face boot de pe o dischetă infectată cu un virus de boot va determina virusul să devină activ în memorie. Din acest moment de fiecare dată când veți realiza boot-area sistemului, virusul va deveni activ în memorie.

Browser

Este prescurtarea de la Web Browser, o aplicație utilizată pentru a localiza și încărca pagini web. Două din cele mai populare browsere sunt Mozilla Firefox și Microsoft Internet Explorer. Ambele sunt browsere grafice, ceea ce înseamnă că pot afișa atât imagini cât și text. În plus, cele mai moderne browsere pot prezenta informații multimedia, incluzând sunet și animație.

Linie de comandă

Într-o interfață linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.

Cookie

Un cookie reprezintă un set de date pe care un server Web îl transmite către un browser atunci când utilizatorul vizitează prima oară site-ul și care este actualizat de fiecare dată când utilizatorul accesează din nou site-ul. Serverul, la fel ca și browserul, salvează informațiile despre utilizator conținute în cookie. Aceste informații sunt stocate sub forma unui fișier text în directoarele de sistem ale browserelor Netscape și Explorer;nu toate browserele suportă cookie. Fișierele cookie stochează informații cum ar fi numele utilizatorului și parola, cât și ce părți din site au fost vizitate. Browserul împarte fiecare cookie doar cu server-ul care l-a generat, celelalte servere le pot citi doar pe cele generate de ele. Unele fișiere cookie sunt programate cu dată de expirare, astfel încât ele vor fi șterse automat după o anumită perioadă de timp.

Drive de disc

Este un dispozitiv care citește date de pe un disc și scrie date pe un disc.

Un drive de hard disc citește / scrie date de pe / pe hard disc.

Un drive de floppy accesează dischetele floppy.

Drive-ele de disc pot fi sau interne (incorporate în interiorul unui calculator) sau externe (plasate într-o locație separată care este conectată la calculator).

Descărcare

Reprezintă copierea (de obicei a unui întreg fișier) de pe o sursă principală pe un dispozitiv periferic. Termenul este adesea utilizat pentru a descrie procesul de copiere a unui fișier de pe un serviciu on-line pe calculatorul unui utilizator. De asemenea se mai poate referi și la copierea unui fișier de pe un server de rețea pe un calculator din rețea.

E-mail

Se referă la poșta electronică. Acesta este un serviciu care transmite mesaje prin intermediul rețelei locale sau globale.

Evenimente

O acțiune sau întâmplare detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi executarea unui clic cu mouse-ul sau apăsarea unei taste, sau întâmplări în sistem cum ar fi epuizarea memoriei.

Fals pozitiv

Apare atunci când un analizator detectează un fișier ca fiind infectat când de fapt acesta nu este infectat.

Extensie de fișier

Reprezintă porțiunea dintr-un nume de fișier ce urmează după caracterul punct, și care indică tipul de date pe care le stochează fișierul.

Multe sisteme de operare, cum ar fi Unix, VMS, and MS-DOS, utilizează extensii de fișiere. De obicei aceasta este formată din una până la trei caractere (unele sisteme de operare mai vechi nu suportă mai mult de trei). De exemplu: "txt" pentru fișierele text oarecare, "c" pentru fișierele sursă scrise în limbajul C, etc.

Metoda euristică

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruși noi. Această metodă de scanare nu se bazează pe semnături de viruși cunoscuți. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. Totuși ocazional poate raporta un cod suspicios în programe normale, generând așa-numitul "fals pozitiv".

IP

Internet Protocol - Un protocol rutabil din suita protocoalelor TCP / IP căruia i se atribuie adresarea IP, rutarea, fragmentarea cât și reasamblarea pachetelor IP.

Applet-uri Java

Reprezintă un program Java care este proiectat să ruleze doar pe pagini web. Pentru a utiliza un applet pe o pagină web, trebuie specificate numele applet-ului și mărimea acestuia. Când este accesată o pagină web, browserul descarcă applet-ul de pe un server și îl rulează pe mașina utilizatorului (clientul). Applet-urile diferă de aplicații prin aceea că sunt guvernate de un protocol de securitate strict.

Astfel că, deși pot rula pe calculatorul unui utilizator, ele nu pot citi sau scrie date pe aceste calculatoare. Applet-urile sunt restricționate de domeniul de care aparțin în ceea ce privește scrierea și citirea datelor.

Virus de macro

Un tip de virus informatic este acela inclus ca macro într-un document. Multe aplicații cum ar fi de exemplu Microsoft Word și Excel suportă limbaje macro puternice.

Aceste limbaje permit încapsularea de macro-uri în documente și execută aceste macro-uri de fiecare dată când este deschis documentul.

Client de mail

Un client de mail este o aplicație care vă permite să trimiteți și să recepționați mesaje.

Memorie

Reprezintă arii de stocare a datelor din interiorul calculatorului. Termenul de memorie desemnează locul de stocare a datelor pe chipuri și pe cel al cuvintelor pe casete sau cd-uri audio. Fiecare calculator dispune de o anumită capacitate de memorie fizică, referită de obicei prin memorie principală sau RAM.

Metoda ne-euristică

Această metodă de scanare se bazează pe semnături specifice de viruși. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus și din acest motiv nu generează fals pozitiv.

Programe împachetate

Reprezintă un fișier în format comprimat. Multe din sistemele de operare și aplicații conțin comenzi care vă dau posibilitatea de a împacheta un fișier astfel încât să ocupe mai putină memorie. De exemplu, să presupunem că aveți un fișier text care conține zece caractere reprezentând spații. În mod normal, acesta ar necesita zece biți de memorie pentru a fi stocați.

Totuși, un program care împachetează fișiere va înlocui caracterele de spațiu printr-un caracter reprezentând spațiu, urmat de un număr care reprezintă numărul de spații care este înlocuit. În acest caz, cele zece caractere reprezentând spațiu ar necesita doar doi biți. Aceasta este doar un exemplu de comprimare - există multe alte metode în afară de aceasta.

Cale

Reprezintă direcția exactă către un fișier de pe un calculator. Această direcție este specificată utilizând sistemul ierarhic de organizare a fișierelor de sus în jos.

Ruta între două puncte, cum ar fi de exemplu canalul de comunicație între două computere.

Phishing

Reprezintă acțiunea de a trimite un e-mail către un utilizator, pretinzând a fi o companie legitimă, în încercarea de a păcăli utilizatorul să furnizeze informații confidențiale ce vor fi folosite la furtul identității. E-mailul îndreaptă utilizatorul către un site Web unde acesta este rugat să actualizeze informații personale, cum ar fi parole și numere de card de credit, de asigurări sociale și de conturi bancare pe care compania respectivă deja le are. Site-ul Web este însă fals și folosit pentru a fura informațiile despre utilizator.

Virus polimorf

Reprezintă un virus care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, asemenea viruși sunt greu de identificat.

Port

Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. Există porturi interne pentru conectarea hard discurilor, monitoarelor și tastaturilor. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului și a altor dispozitive periferice.

În rețelele TCP / IP și UDP acestea reprezintă un punct terminus al unei conexiuni logice. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Fișier de raport

Reprezintă un fișier care listează acțiunile care au avut loc. BitDefender menține un fișier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fișierelor, numărul de arhive și fișiere scanate, câte fișiere infectate și suspecte au fost găsite.

Rootkit

Un rootkit este un set de unelte soft ce oferă acces la nivel de administrator în interiorul unui sistem. Termenul a fost utilizat pentru prima oară pentru sistemele de operare UNIX și se referea la unelte recompilate ce furnizau intrușilor drepturi administrative, permițându-le să își ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fișiere, loginuri și jurnale. Acestea pot de asemenea să intercepteze date de la terminale, conexiuni la rețea sau perifice dacă sunt dotate cu softul adecvat.

Rootkiturile nu sunt malițioase prin natură. De exemplu, sistemele și chiar unele aplicații ascunde fișiere critice utilizând rootkituri. Totuși, ele sunt folosite în general pentru a ascunde aplicații malițioase sau prezența intrușilor în sistem. În combinație cu aplicații malițioase, rootkiturile constituie o mare amenințare pentru securitatea și integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fișiere și jurnale și evita detecția.

Script

Un alt termen pentru fișiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.

Spam

Termen ce acoperă întreagă gamă a mesajelor electronice nesolicitate.

Spyware

Reprezintă orice software care strânge informații despre utilizator prin intermediul conexiunii la Internet fără știrea acestuia, de obicei în scopuri publicitare. Aplicațiile spyware sunt de obicei primite ca parte ascunsă a unui program de tip freeware sau shareware, ce poate fi descărcat de pe Internet; totuși, trebuie știut că majoritatea aplicațiilor de tip shareware și freeware nu

conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe Internet și transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail și chiar parole și numere de carduri de credit.

Asemănarea dintre spyware și un cal troian este faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obișnuit de a deveni victima unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fișiere care sunt disponibile astăzi.

Pe lângă problemele legate de etică și intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât și a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la Internet a utilizatorului. Deoarece folosesc memorie și resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

Elemente din startup

Orice fișier plasat în acest director se va deschide de fiecare dată când calculatorul este pornit. De exemplu, un sunet care se va auzi atunci când este pornit calculatorul sau chiar aplicații sunt considerate elemente de startup. În mod normal, un alias al programului este plasat în acest director, și nu direct fișierul.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată în bara de sarcini Windows (de obicei în partea de jos, lângă ceas) și conține pictograme miniaturale pentru accesul rapid la aplicații de sistem cum ar fi cele legate de fax, imprimantă, modem, volum și altele. Faceți dublu-clic sau clic-dreapta cu mouse-ul pe o pictogramă pentru a vizualiza și accesa detaliile și comenzile.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul Internet și care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware și sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât și convenții folosite în conectarea rețelelor și rutării traficului.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de viruși, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai insidioase tipuri de troieni este acela care pretinde că elimină virușii de pe calculatorul dumneavoastră, dar în loc de aceasta introduce viruși pe calculatorul dumneavoastră.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii oferă dușmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar

după ce troienii aduc acest cal în interiorul orașului lor, din interiorul calului ies o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraș și să captureze Troia.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiași produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteți instala actualizarea.

BitDefender dispune de modulul său propriu care realizează actualizarea automatică sau manuală.

Virus

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără știrea dumneavoastră și rulează independent de voința dumneavoastră. Cea mai mare parte a virușilor se pot și înmulți. Toți virușii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar și un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus și mai periculos este acela care este capabil să se răspândească în rețea și poate să treacă de sistemele de securitate.

Semnătură de virus

Reprezintă tiparul binar al unui virus, utilizat de un program antivirus pentru detecția și eliminarea virusului.

Vierme

Reprezintă un program care se autopropagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.