Bitdefender®
MOBILE SECURITY

GHIDUL UTILIZATORULUI

Bitdefender Mobile Security

Ghidul utilizatorului

Data publicării 21.11.2022

Aviz juridic

Bitdefender

Cuprins

DESPRE ACEST GHID

Scopul și publicul țintă

Acest ghid este destinat tuturor utilizatorilor Android care au ales Bitdefender Mobile Security drept soluția de securitate pentru dispozitivele lor mobile. Informațiile prezentate aici sunt adecvate nu doar celor care dețin cunoștințe tehnice, fiind accesibil tuturor care utilizează dispozitive Android.

Vei afla cum să configurezi și să utilizezi Bitdefender Mobile Security pentru a te proteja împotriva amenințărilor și altor aplicații periculoase. Vei afla cum să valorifici Bitdefender la maximum.

Îți dorim o lectură plăcută și utilă.

Cum să folosiți acest ghid

Acest ghid este organizat în mai multe teme majore:

Introducere (page 5)

Faceți cunoștință cu produsul Bitdefender Mobile Security și interfața sa pentru utilizatori.

Caracteristici și funcții (page 11)

Află cum să utilizezi Bitdefender Mobile Security pentru a te proteja împotriva amenințărilor și aplicațiilor periculoase, cunoscând caracteristicile acestei soluții și funcționalitățile acestora.

Obține ajutor (page 49)

Unde să căutați și unde să cereți ajutor în cazul în care apar situații neprevăzute.

Convenții utilizate în acest ghid

Convenții tipografice

Manualul conține diferite stiluri de text, pentru o lectură cât mai ușoară. Aspectul și semnificația acestora sunt prezentate în tabelul de mai jos.

Aspect	Descriere
`sample syntax`	Exemplele de sintaxă sunt imprimate cu caractere `monospaced`.
https://www.bitdefender.com	Linkurile URL indică locații externe, pe serverele http sau ftp.
documentation@bitdefender.com	Adresele de e-mail sunt inserate în text ca informație de contact.
Despre acest Ghid (page 1)	Acesta este un link intern, care vă direcționează către o locație din document.
`filename`	Fișierul și directoarele sunt tipărite folosind `monospaced` font.
opțiune	Toate opțiunile de produs sunt imprimate folosind caractere **îngroșate**.
cuvânt cheie	Cuvintele cheie sau expresiile importante sunt evidențiate folosind caractere **îngroșate**.

Atenționări

Atenționările sunt note din text, marcate grafic, care oferă informații suplimentare legate de paragraful respectiv.

Nota

Nota este o scurtă observație. Deși pot fi omise, notele pot furniza informații importante, cum ar fi o caracteristică specifică sau un link către un subiect relevant.

Important

Segmentele marcate astfel necesită atenția ta și nu este recomandat să le omiți. De obicei, aici sunt furnizate informații importante, dar nu esențiale.

Avertizare

Acestea sunt informații esențiale, care trebuie tratate cu o atenție deosebită. Dacă urmezi indicațiile, nu se va întâmpla nimic rău. Este recomandat să citești și să înțelegi despre ce este vorba, deoarece aici se descrie ceva extrem de riscant.

Comentarii

Te invităm să participi la procesul de îmbunătățire al manualului. Toate informațiile prezentate au fost testate și verificate în mod riguros. Te rugăm să ne scrii despre orice inexactități pe care le vei găsi în acest manual, precum și să propui moduri prin care îl putem îmbunătăți, astfel încât să îți putem furniza o documentație ireproșabilă.

Anunțați-ne trimițând un e-mail la documentation@bitdefender.com. Scrieți toate e-mailurile dvs. legate de documentație în engleză, astfel încât să le putem procesa eficient.

1. CE ESTE BITDEFENDER MOBILE SECURITY

Activitățile online, cum ar fi plata facturilor, rezervări pentru vacanță sau achiziționarea de produse și servicii se realizează comod, fără complicații. Însă, la fel ca în cazul multor altor activități pe internet, acestea implică și riscuri mari și, dacă detaliile de securitate sunt ignorate, datele personale pot fi accesate neautorizat. Și ce poate fi mai important decât protejarea datelor stocate în conturile online și pe smartphone-ul personal?

Cu **Bitdefender Mobile Security** ai următoarele beneficii:

- Obții cea mai bună protecție pentru smartphone-ul și tableta ta Android cu un impact minim asupra autonomiei bateriei
- Te protejezi împotriva fraudelor pe mobil bazate pe linkuri
- Ai acces la serviciul nostru VPN securizat pentru o experiență rapidă, anonimă și sigură de navigare pe internet
- Localizează, blochează și șterge de la distanță informațiile de pe dispozitivul tău Android în caz de pierdere sau furt
- Îți verifici contul de e-mail pentru a afla dacă a fost implicat în breșe de securitate a datelor sau scurgeri de date

2. INTRODUCERE

2.1. Cerințe dispozitiv

Bitdefender Mobile Security funcționează pe orice dispozitiv care utilizează Android 5.0 sau orice versiune ulterioară a sistemului de operare. Este necesară o conexiune activă la internet pentru scanarea in-the-cloud a amenințărilor.

2.2. Instalarea Bitdefender Mobile Security

- **Din Bitdefender Central**
  - Pe Android
    1. Accesează: https://central.bitdefender.com.
    2. Accesează contul tău Bitdefender.
    3. Selectați secțiunea **Dispozitivele mele**.
    4. Atinge **INSTALARE PROTECȚIE** și apoi **Protejează acest dispozitiv**.
    5. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, atinge butonul corespunzător.
    6. Vei fi redirecționat către aplicația **Google Play**. În ecranul Google Play, selectează opțiunea de instalare.
  - Pe Windows, macOS și iOS
    1. Mergi la: https://central.bitdefender.com.
    2. Conectați-vă la contul dvs. Bitdefender.
    3. Selectează **Dispozitivele mele** panou.
    4. Apasă pe **INSTALARE PROTECȚIE** și apoi pe **Protejează alte dispozitive**.
    5. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, apasă pe butonul corespunzător.
    6. Apasă pe **TRIMITE LINK DE DESCĂRCARE**.
    7. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că linkul pentru descărcare generat

este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceeași pași.

8. Pe dispozitivul pe care dorești să instalezi Bitdefender, accesează contul de e-mail introdus și apoi apasă pe butonul de descărcare corespunzător.

- **Din Google Play**
  Caută Bitdefender Mobile Security pentru a localiza și instala aplicația. Alternativ, scanați codul QR:

  Înainte de a trece prin pașii de validare, este necesar să accepți Contractul de Abonament. Rezervă-ți câteva momente pentru a citi Contractul de abonament întrucât acesta conține termenii și condițiile potrivit cărora poți utiliza Bitdefender Mobile Security.
  Apasă **CONTINUĂ** pentru a trece la fereastra următoare.

2.3. Accesează contul tău Bitdefender

Pentru a utiliza Bitdefender Mobile Security, trebuie să îți conectezi dispozitivul la un cont Bitdefender, Facebook, Google, Microsoft sau Apple, autentificându-te în cont din aplicație. Prima dată când deschizi aplicația, ți se va solicita să te conectezi la un cont.

Dacă ai instalat Bitdefender Mobile Security din contul Bitdefender, aplicația va încerca să se conecteze automat la acel cont

Pentru a-ți asocia dispozitivul unui cont Bitdefender:

1. Introdu adresa de e-mail și parola asociate contului tău Bitdefender în câmpurile corespunzătoare. Dacă nu ai un cont Bitdefender și dorești să îți creezi unul, selectează link-ul corespunzător.
2. Atinge **CONECTARE**.

Pentru a te conecta cu un cont de Facebook, Google sau Microsoft, selectează serviciul dorit din secțiunea Sau conectează-te cu. Vei fi

automat redirecționat către pagina de conectare a serviciului selectat. Urmează instrucțiunile pentru a-ți asocia contul cu Bitdefender Mobile Security.

> **Notă**
> Bitdefender nu are acces la informații confidențiale, precum parola contului pe care te autentifici de obicei sau datele personale ale prietenilor și contactelor.

2.4. Configurare protecție

Odată ce te-ai conectat cu succes la aplicație, se va afișa fereastra Configurare protecție. Pentru a-ți proteja dispozitivul, îți recomandăm să urmezi acești pași:

- **Status abonament**. Pentru a beneficia de protecția Bitdefender Mobile Security, trebuie să activați produsul prin achiziția unui abonament, care prevede cât timp puteți utiliza produsul. Imediat ce acesta expiră, aplicația nu mai funcționează și nu vă mai protejează dispozitivul.
  Dacă ai un cod de activare, atinge **AM UN COD**, apoi **ACTIVARE**.
  Dacă te-ai autentificat cu un cont Bitdefender nou și nu ai un cod de activare, poți utiliza produsul timp de 14 zile, gratuit.
- **Protecție web**. Dacă dispozitivul tău necesită activarea serviciului Accesibilitate în vederea activării Protecției web, atinge **ACTIVARE**. Vei fi redirecționat către meniul Accesibilitate. Selectează Bitdefender Mobile Security și activează opțiunea corespunzătoare.
- **Scaner malware**. Execută o singură scanare pentru a te asigura că dispozitivul tău nu conține amenințări. Pentru a porni procesul de scanare, atinge **SCANEAZĂ ACUM**.
  Imediat ce începe procesul de scanare, se afișează panoul de control. Aici, poți vedea starea de securitate a dispozitivului tău.

2.5. Panou de bord

Atinge pictograma Bitdefender Mobile Security din lista de aplicații a dispozitivului tău pentru a deschide interfața aplicației.

Panoul de control oferă informații despre starea de securitate a dispozitivului tău și, prin intermediul funcției Autopilot, te ajută să îmbunătățești securitatea dispozitivului tău oferindu-ți recomandări cu privire la caracteristicile disponibile.

Panoul de stare din partea de sus a ferestrei te informează cu privire la starea de securitate a dispozitivului tău folosind mesaje explicite și culori sugestive. Dacă Bitdefender Mobile Security nu prezintă avertismente, panoul de stare este verde. Atunci când a fost detectată o problemă de securitate, culoarea panoului de stare devine roșie.

Pentru a-ți oferi o metodă eficientă de operare și o protecție sporită în timp ce desfășori diferite activități, **Bitdefender Autopilot** va acționa ca asistentul tău personal în materie de securitate. În funcție de activitatea pe care o desfășori, Bitdefender Autopilot îți va oferi recomandări contextuale în funcție de modul de utilizare a dispozitivului tău și nevoile tale. Acest lucru te va ajuta să descoperi și să beneficiezi de avantajele furnizate de caracteristicile incluse în aplicația Bitdefender Mobile Security.

De fiecare dată când un anumit proces este în curs de desfășurare sau o funcție necesită răspunsul dumneavoastră, pe Panoul de bord se afișează un card cu mai multe informații și acțiuni posibile.

Poți accesa funcțiile Bitdefender Mobile Security și poți naviga cu ușurință din bara de navigare din partea de jos:

Scaner malware

Îți permite pornirea unei scanări la cerere și activarea scanării dispozitivelor de stocare. Pentru mai multe informații, consultă capitolul Scanare malware (page 11).

Protecție web

Asigură o experiență de navigare sigură informându-te cu privire la paginile web potențial periculoase. Pentru mai multe informații, consultă capitolul Protecție web (page 13).

VPN

Criptează comunicațiile prin internet, ajutându-te să-ți păstrezi confidențialitatea indiferent de rețeaua la care ești conectat. Pentru mai multe informații, consultați capitolul VPN (page 14).

Scam Alert

Te menține în siguranță generând alerte pentru linkurile periculoase pe care le primești prin SMS, aplicații de mesagerie și orice tip de notificare. Pentru informații suplimentare, consultă Scam Alert (page 17).

Anti-furt

Vă permite să activați și să dezactivați caracteristicile Anti-Theft, precum și să configurați setările acestei funcții. Pentru mai multe informații, consultă capitolul Funcții Antifurt (page 20).

Confidențialitate cont

Verifică dacă s-au produs scurgeri de informații din conturile tale online. Pentru mai multe informații, consultă capitolul Confidențialitate cont (page 24).

Blocare aplicații

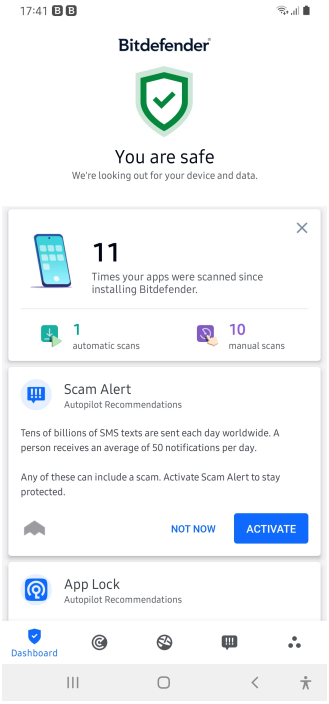
Vă permite să protejați aplicațiile instalate prin setarea unui cod de acces PIN. Pentru mai multe informații, consultă capitolul Blocare Aplicații (page 25).

Rapoarte

Păstrează o evidență a tuturor acțiunilor importante, a schimbărilor de stare și a altor mesaje critice legate de activitatea dispozitivului tău. Pentru informații suplimentare, consultă Rapoarte (page 30).

WearON

Comunică cu smartwatch pentru a te ajuta să îți găsești telefonul dacă îl rătăcești sau uiti unde l-ai lăsat. Pentru mai multe informații, consultă capitolul WearON (page 31).


17:41
Bitdefender
You are safe
We're looking out for your device and data.
11
Times your apps were scanned since installing Bitdefender.
1
automatic scans
10
manual scans
Scam Alert
Autopilot Recommendations
Tens of billions of SMS texts are sent each day worldwide. A person receives an average of 50 notifications per day.
Any of these can include a scam. Activate Scam Alert to stay protected.
NOT NOW
ACTIVATE
App Lock
Autopilot Recommendations
Dashboard

3. CARACTERISTICI ȘI FUNCȚII

3.1. Scanare malware

Bitdefender vă protejează dispozitivul și datele împotriva aplicațiilor rău intenționate, utilizând scanarea la instalare și scanarea la cerere.

Interfața Scaner malware oferă o listă cu toate tipurile de amenințări pe care Bitdefender le caută, alături de definițiile acestora. Tot ce trebuie să faci este să selectezi fiecare amenințare pentru a vizualiza definiția aferentă.

> **Notă**
> Asigura-te că dispozitivul tău mobil este conectat la internet. Dacă dispozitivul nu este conectat la internet, procesul de scanare nu va porni.

- **Scanare la instalare**
  Ori de câte ori instalezi o aplicație, Bitdefender Mobile Security o scanează automat folosind tehnologia în cloud. Același proces de scanare este inițiat la fiecare actualizare a aplicațiilor instalate.
  Dacă aplicația este depistată a fi rău intenționată, va apărea o alertă care vă va solicita dezinstalarea acesteia. Atinge **Dezinstalare** pentru a merge la ecranul de dezinstalare a aplicației respective.
- **Scanare la cerere**
  Oricând dorești să te asiguri că aplicațiile instalate pe dispozitivul tău sunt sigure în utilizare, poți iniția o scanare la cerere.
  Pentru a porni o scanare la cerere:

  1. Atinge **Scaner malware** din bara de navigare de jos.
  2. Atinge **INIȚIERE SCANARE**.

> **Notă**
> Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția Scaner Malware. După ce atingi butonul **INIȚIERE SCANARE**, selectează **Permite** pentru următoarele:
>
> - Permiți ca **Antivirus** să efectueze și să gestioneze apelurile telefonice?
> - Permiteți ca **Antivirus** să acceseze fotografii, fișiere media și fișiere stocate pe dispozitivul dumneavoastră?

Este afișată evoluția scanării și poți opri procesul în orice moment.

În mod implicit, Bitdefender Mobile Security va scana spațiile de stocare internă ale dispozitivului tău, inclusiv orice cartelă SD instalată. În acest fel, orice aplicații periculoase ce se pot afla pe cartelă pot fi detectate înainte de a produce pagube.

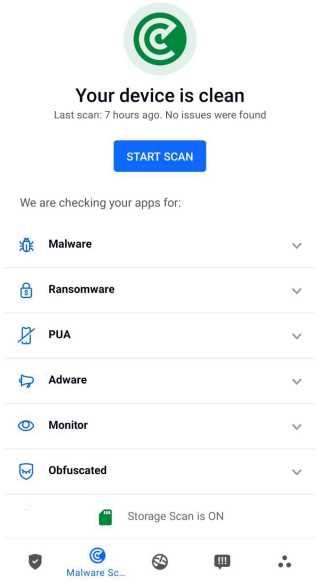
Pentru a dezactiva setarea Scanare dispozitive de stocare:

1. Atinge **Mai multe** din bara de navigare de jos.
2. Atinge **Setări**.
3. Dezactivează selectorul **Scanare dispozitive de stocare** din secțiunea Scaner programe periculoase.

Dacă este detectată orice aplicație rău intenționată, informațiile referitoare la aceasta vor fi afișate și o poți șterge apăsând butonul **DEZINSTALARE**.

Secțiunea Scanare malware afișează starea dispozitivului dumneavoastră. Când dispozitivul este în siguranță, secțiunea este evidențiată cu verde. Când este necesară o scanare a dispozitivului sau există vreo acțiune care necesită răspunsul dumneavoastră, secțiunea este evidențiată cu roșu.

Dacă folosești versiunea de Android 7.1 sau o versiune mai recentă, poți accesa o scurtătură la funcția de Scanare malware astfel încât să poți executa scanările mai rapid, fără a deschide interfața Bitdefender Mobile Security. Pentru a face acest lucru, apasă și menține apăsată pictograma Bitdefender din ecranul principal sau bara de aplicații, apoi selectează pictograma .



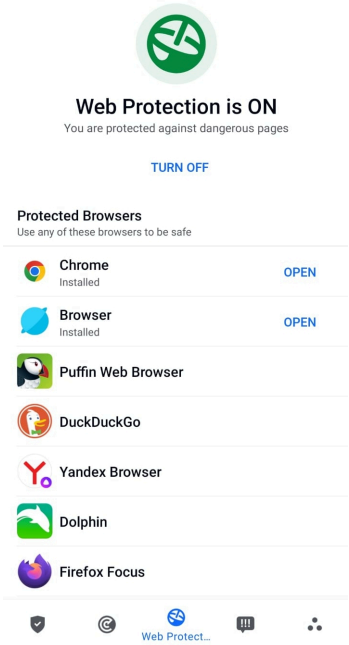
3.2. Protecție web

Caracteristica Protecție Web verifică paginile web pe care le accesezi prin browserul Android implicit, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser și Dolphin, utilizând serviciile în cloud de la Bitdefender.

Notă

Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția Securitate web.

Permiteți înregistrarea ca serviciu Accesibilitate și atingeți **PORNIRE** atunci când vi se solicită acest lucru. Atingeți **Antivirus** și activați butonul, apoi confirmați că sunteți de acord cu permisiunea dispozitivului dumneavoastră.



De fiecare dată când accesezi un site bancar, Protecția Web Bitdefender este setată să te notifice să utilizezi serviciul VPN de la Bitdefender. Notificarea apare în bara de stare. Îți recomandăm să utilizezi Bitdefender VPN în timp ce ești conectat la contul tău bancar astfel încât să fii protejat împotriva unor breșe posibile de securitate a datelor.

Pentru a dezactiva notificarea Protecție Web:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Dezactivează comutatorul corespunzător din zona Protecție Web.

3.3. VPN

Cu Bitdefender VPN își menții confidențialitatea datelor atunci când te conectezi la rețele wireless nesecurizate în aeroporturi, mall-uri, cafenele sau hoteluri. În acest fel, pot fi evitate situațiile nefericite cum ar fi furtul de date personale sau tentativele de a face IP-ul tău accesibil de către hackeri.

VPS acționează ca tunel între dispozitivul tău și rețeaua la care te conectezi, securizându-ți conexiunea, criptându-ți datele prin criptare la nivel de bancă și ascunzându-ți adresa IP oriunde te-ai afla. Traficul tău este redirecționat prin intermediul unui server separat, ceea ce face ca dispozitivul tău să fie imposibil de identificat între multitudinea de alte dispozitive care folosesc serviciile noastre. Mai mult decât atât, în timp ce ești conectat la internet prin intermediul aplicației VPN, poți accesa conținut care în mod normal este restricționat în anumite zone.

> **Notă**
> Unele țări practică cenzura online, prin urmare utilizarea aplicațiilor VPN pe teritoriul lor este interzisă prin lege. Pentru a evita consecințele legale, este posibil să apară un mesaj de avertizare atunci când încerci să utilizezi aplicația VPN de la Bitdefender pentru prima dată. Prin continuarea utilizării acestei aplicații, confirmi că îți sunt cunoscute reglementările aplicabile din țara respectivă și riscurile la care ai putea fi expus.

Există două moduri de a activa sau dezactiva Bitdefender VPN:

- Apasă **CONECTARE** în cardul VPN din Panoul de bord.
  Se afișează starea Bitdefender VPN.
- Atinge **VPN** din bara de navigare de jos și apoi **CONECTARE**.
  Selectează **CONECTARE** de fiecare dată când dorești să fii protejat atunci când te conectezi la rețele wireless nesecurizate.
  Selectează **DECONECTARE** atunci când vrei să dezactivezi conexiunea.

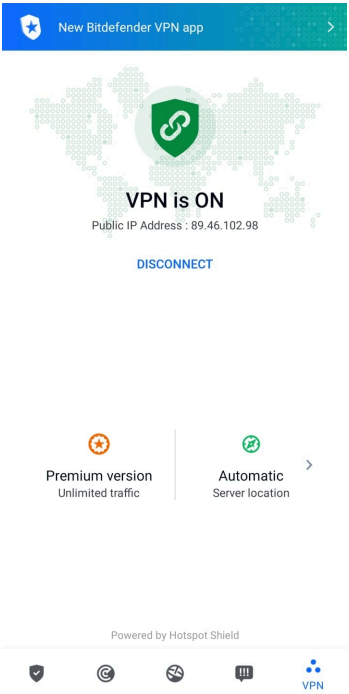
> **Notă**
> Când pornești pentru prima dată VPN-ul ți se cere să permiți Bitdefender să configureze o conexiune VPN care să monitorizeze traficul pe rețea. Apasă **OK** pentru a continua.

Dacă dispozitivul tău utilizează Android 7.1 sau o versiune ulterioară, poți accesa Bitdefender VPN printr-o comandă rapidă, fără să deschizi interfața Bitdefender Mobile Security.

Pentru a face acest lucru, apasă și menține apăsată pictograma Bitdefender din ecranul principal sau bara de aplicații, apoi selectează pictograma .

Pentru a economisi bateria, îți recomandăm să oprești funcția VPN atunci când nu ai nevoie de ea.

Dacă ai un abonament premium și dorești să te conectezi la un anumit server, apasă Locație Server din funcția VPN și apoi selectează locația dorită. Pentru detalii referitoare la abonamentele VPN, accesează



3.3.1. Setări VPN

Pentru o configurare avansată a VPN-ului tău:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.

În zona VPN, poți configura următoarele opțiuni:

- Acces rapid VPN - în bara de stare a dispozitivului tău va apărea o notificare care îți permite să pornești rapid VPN-ul.

- Avertizare rețea Wi-Fi publică - de fiecare dată când te conectezi la o rețea Wi-Fi publică, ești notificat în bara de stare a dispozitivului tău să folosești VPN.

3.3.2. Abonamente

Bitdefender VPN oferă gratuit o cotă de trafic zilnică de 200 MB pe dispozitiv pentru a-ți securiza conexiunea oricând ai nevoie, conectându-te automat la locația optimă a serverului.

Pentru a obține trafic nelimitat și acces nerestricționat la conținutul din întreaga lume alegând o locație de server în funcție de preferințe, efectuează upgrade la versiunea Premium.

Poți să efectuezi oricând un upgrade la versiunea Premium a Bitdefender VPN atingând **Activare Premium** din fereastra VPN.

Abonamentul Bitdefender Premium VPN este independent de abonamentul Bitdefender Mobile Security, ceea ce înseamnă că îl vei putea utiliza cât timp este valabil, indiferent de starea abonamentului tău pentru soluția de securitate. În cazul în care abonamentul Bitdefender Premium VPN expiră, dar abonamentul Bitdefender Mobile Security este încă activ, vei reveni la versiunea gratuită.

Bitdefender VPN este un produs pentru mai multe platforme, disponibil în cadrul produselor Bitdefender compatibile cu Windows, macOS, Android și iOS. După ce faci upgrade la planul Premium, îți vei putea folosi abonamentul pe toate produsele, cu condiția să te conectezi cu același cont Bitdefender.

Notă

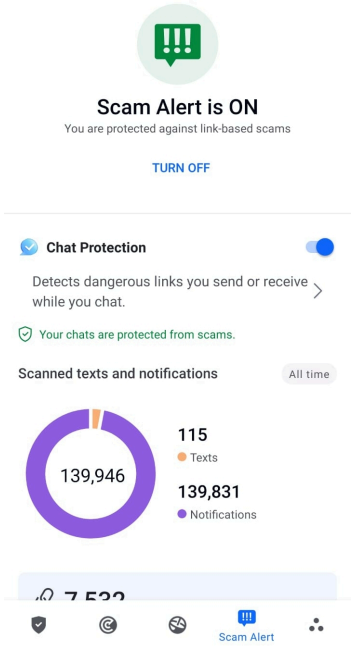
De asemenea, Bitdefender VPN funcționează și ca o aplicație independentă pe toate sistemele de operare compatibile, și anume pe Windows, macOS, Android și iOS.

3.4. Scam Alert

Caracteristica Scam Alert aplică, în prim plan, o serie de măsuri de prevenție, gestionând situații posibil periculoase înainte ca acestea să aibă șansa să devină o problemă, inclusiv cu amenințările malware. Scam Alert monitorizează în timp real toate mesajele SMS și notificările Android primite.

În momentul în care un link periculos ajunge într-un mesaj pe telefonul tău, pe ecran va apărea un avertisment. Bitdefender îți va oferi două opțiuni. Prima este să respingi informația. A doua opțiune este **VIZUALIZARE DETALII**. Aceasta îți oferă mai multe informații despre incident, precum câteva sfaturi esențiale, cum ar fi:

- Nu deschide și nici nu transmite mai departe linkul detectat.
- În cazul mesajelor SMS, ștergeți mesajul, dacă este posibil.
- Blochează expeditorul dacă acesta nu este un contact de încredere.
- Dezinstalează aplicația care trimite linkuri periculoase în notificări.



Notă

Din cauza limitărilor sistemului de operare Android, Bitdefender nu poate șterge mesajele text și nu poate aplica măsuri directe mesajelor SMS sau altor surse de notificări periculoase. Dacă ignori avertismentul Scam Alert și încerci să deschizi linkul periculos, caracteristica Protecție web a Bitdefender îl va detecta automat, împiedicând infectarea dispozitivului tău.

3.4.1. Activarea caracteristicii Scam Alert

Pentru a activa Scam Alert, trebuie să permiți accesul aplicației Bitdefender Mobile Security la mesajele SMS și la sistemul de notificare:

1. Deschide aplicația Bitdefender Mobile Security instalată pe telefonul sau tableta ta Android.
2. În ecranul principal al aplicației Bitdefender, selectează opțiunea **Scam Alert** din bara de navigare de jos, apoi atinge **ACTIVARE**.
3. Atinge butonul **PERMITE**.
4. În lista de acces la notificări, schimbă butonul asociat Bitdefender Security în poziția **PORNIT**.
5. Confirmă acțiunea apăsând pe **PERMITE**.
6. Revino la ecranul Scam Alert și apasă pe **PERMITE** pentru ca Bitdefender să poată scana mesajele SMS pe care le primești.

3.4.2. Protecție chat în timp real

Mesajele chat sunt un mijloc foarte convenabil pentru a ține legătura, însă sunt și cea mai simplă cale prin care linkuri periculoase pot ajunge la tine.

Când caracteristica Protecție chat este activă, protecția oferită de modulul Scam Alert se extinde de la texte și notificări la chaturi, asigurându-se că sunt sigure împotriva atacurilor pe bază de linkuri, detectând linkurile periculoase pe care le trimiți sau primești atunci când comunici prin chat.

Pentru a activa caracteristica Protecție chat:

1. Deschideți aplicația Bitdefender Mobile Security instalată pe telefonul sau tableta dvs. Android.
2. În ecranul principal al aplicației Bitdefender, selectează opțiunea **Scam Alert** din bara de navigare de jos.
3. În partea de sus a filei Scam Alert, vei observa caracteristica Protecție chat. Schimbă butonul corespunzător acesteia în poziția **ACTIVAT**.

Notă
În prezent, caracteristica Protecție Chat este compatibilă cu următoarele aplicații:

- WhatsApp
- Facebook Messenger
- Telegram
- Discord

3.5. Funcții Antifurt

Bitdefender vă permite să localizați dispozitivul și să preveniți accesul neautorizat la datele dvs.

Tot ce trebuie să faceți este să activați funcția Antifurt pe dispozitiv și, apoi, când este cazul, veți putea accesa **Bitdefender Central** de pe orice browser, de oriunde.

Notă
Interfața Anti-furt include și un link către aplicația noastră Bitdefender Central în Google Play Store. Poți folosi acest link pentru a descărca aplicația, în cazul în care nu ai făcut deja acest lucru.

Bitdefender Mobile Security oferă următoarele caracteristici Anti-furt:

Localizare de la distanță

Vizualizați locația curentă a dispozitivului dumneavoastră pe Google Maps. Locația este actualizată la fiecare 5 secunde, așadar îl puteți localiza dacă este în mișcare.

Precizia locației depinde de modul în care o poate identifica Bitdefender:

- Dacă funcția GPS este activată pe dispozitiv, locația sa poate fi indicată cu precizie pe o rază de câțiva metri atâta timp cât se află în raza sateliților GPS (mai exact, nu într-o clădire).
- Dacă dispozitivul este înăuntru, locația sa poate fi stabilită la intervale de zeci de metri dacă funcția Wi-Fi este activată și există pe raza sa rețele wireless.
- Altfel, locația va fi stabilită utilizând numai informațiile rețelei mobile, care nu poate oferi o precizie mai mare de câteva sute de metri.

Blocare de la distanță

Blochează ecranul dispozitivului tău și setează un cod PIN numeric pentru deblocarea acestuia.

Ștergere de la distanță

Șterge toate datele tale personale de pe dispozitivul tău înstrăinat.

Expedierea unei alerte pe dispozitiv (Alarmă)

Expediază de la distanță un mesaj care va fi afișat pe ecranul dispozitivului sau declanșați un sunet puternic care să fie redat în difuzorul telefonului.

Dacă pierzi dispozitivul, poți informa persoană care îl găsește cum ți-l poate returna prin afișarea unui mesaj pe ecranul dispozitivului.

Dacă ați rătăcit dispozitivul și se poate să nu fie foarte departe de dumneavoastră (de exemplu, undeva în casă sau în birou), ce metodă ar fi mai bună pentru a-l găsi decât ca dispozitivul să emită un sunet puternic? Sunetul va fi redat chiar și când dispozitivul se află în modul silențios.

3.5.1. Activarea funcției Antifurt

Pentru a activa funcțiile Antifurt, urmează procesul de configurare din cardul Antifurt disponibil în Panoul de bord.

Alternativ, puteți activa funcția Antifurt urmând pașii de mai jos:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atinge **Anti-furt**.
3. Atinge **ACTIVARE**.
4. Se va lansa următoarea procedură, care te va ajuta să activezi această funcție:

   Notă
   Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția Antifurt.

   Pentru activare, urmați pașii de mai jos:

   a. Atinge **Activare Anti-furt** apoi **ACTIVARE**.

   b. Permite permisiuni pentru **Antivirus** să acceseze locația dispozitivului tău

   a. **Acordă permisiuni de administrator**

Aceste drepturi sunt esențiale pentru operarea modulului Antifurt și este obligatoriu să fie acordate pentru a putea continua.

b. **Setează codul PIN al aplicației**
Pentru a împiedica accesul neautorizat la dispozitivul tău, este necesară configurarea unui cod PIN. La fiecare accesare a dispozitivului tău, este necesar să se introducă mai întâi acest PIN. Ca soluție alternativă, pe dispozitivele care acceptă autentificarea prin intermediul amprentei digitale, se poate utiliza confirmarea pe bază de amprentă digitală în locul codului PIN configurat.
Același cod PIN este utilizat și de App Lock pentru protejarea aplicațiilor instalate.

c. **Activează Foto instant**
De fiecare dată când cineva va încerca să îți deblocheze dispozitivul fără succes, în timp ce funcția Instantanee este activată, Bitdefender îi va face o fotografie.
Mai exact, de fiecare dată când se introduce greșit, de trei ori consecutiv, codul PIN, parola, sau confirmarea pe bază de amprentă, care au fost setate de tine pentru a-ți proteja dispozitivul, se va realiza o fotografie cu camera secundară. Imaginea este salvată împreună cu data și ora, precum și motivul realizării, și poate fi vizualizată atunci când deschizi Bitdefender Mobile Security pentru a accesa fereastra Antifurt.
Ca soluție alternativă, poți vizualiza fotografia respectivă din contul tău Bitdefender:

i. Mergi la: https://central.bitdefender.com.

ii. Conectează-te la contul personal.

iii. Selectează **Dispozitivele mele** panou.

iv. Selectează dispozitivul tău Android și apoi fila **Anti-furt**.

v. Atinge ⋮ de lângă **Vezi fotografiile instantanee** pentru a vedea cele mai recente fotografii surprinse.
Sunt salvate doar cele mai recente două fotografii.

Odată ce funcția Anti-Theft este activată, poți activa sau dezactiva comenzile Control web individual din fereastra Anti-Furt prin atingerea opțiunilor corespunzătoare.

3.5.2. Folosirea funcțiilor Anti-Theft din Bitdefender Central

> **Notă**
> Toate funcțiile Antifurt solicită ca opțiunea **Date de fundal** să fie activă în setările Utilizare date ale dispozitivului dumneavoastră.

Pentru a accesa caracteristicile Antifurt din contul Bitdefender:

1. Accesează **Bitdefender Central**.
2. Selectează **Dispozitivele mele** panou.
3. În fereastra **DISPOZITIVELE MELE**, selectează cardul de dispozitiv dorit apăsând pe butonul **Vizualizare detalii** corespunzător.
4. Selectați secțiunea **Antifurt**.
5. Apasă pe butonul care corespunde caracteristicii pe care dorești să o utilizezi:
   Localizare - afișează locația dispozitivului tău pe Google Maps.
   Afișează IP - afișează ultima adresă IP a dispozitivului selectat.
   Alertă - tastează un mesaj care să se afișeze pe ecranul dispozitivului tău și/sau setează dispozitivul să genereze o alarmă sonoră.
   Blocare - blochează dispozitivul și setează un cod PIN pentru a-l debloca.
   Ștergere - șterge toate datele din dispozitivul tău.

> **Important**
> După ce ștergi un dispozitiv, este oprită funcționarea tuturor funcțiilor Anti-Theft.

3.5.3. Setări Antifurt

Dacă dorești să activezi sau să dezactivezi comenzile la distanță:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Anti furt**.
3. Activează sau dezactivează opțiunile dorite.

3.6. Confidențialitate cont

Funcția Confidențialitate cont Bitdefender detectează dacă s-au produs breșe de securitate a datelor la nivelul conturilor pe care le folosești pentru a efectua plăți și cumpărături online sau pentru a te conecta la diverse aplicații sau site-uri web. Datele care ar putea fi stocate într-un cont includ parole, date de pe cardurile bancare sau informații privind contul bancar și, dacă acestea nu sunt securizate în mod corespunzător, se poate produce un furt de identitate sau o încălcare a confidențialității.

Starea de confidențialitate a unui cont este afișată imediat după validare.

Reverificările automate sunt setate să ruleze în fundal, însă se pot efectua, de asemenea, scanări manuale zilnic.

Se vor afișa notificări de fiecare dată când se descoperă noi scurgeri de informații care implică oricare dintre conturile de e-mail validate.

Pentru a începe să-ți păstrezi în siguranță datele personale:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atinge **Confidențialitate cont**.
3. Selectează **ÎNCEPE UTILIZAREA**.
4. Adresa de e-mail utilizată pentru a-ți crea contul Bitdefender va fi afișată și adăugată automat pe lista de conturi monitorizate.
5. Pentru a adăuga un cont nou, apasă pe **ADĂUGARE CONT** din fereastra Confidențialitate cont și apoi introdu adresa de e-mail.
   Atinge **ADĂUGARE** pentru a continua.
   Bitdefender trebuie să valideze acest cont înainte de a afișa informații private. Prin urmare, se va trimite un e-mail conținând un cod de validare către adresa de e-mail furnizată.
   Verifică-ți inbox-ul și apoi introdu codul primit în secțiunea **Confidențialitate cont** a aplicației. Dacă nu găsești e-mail-ul de validare în Inbox, verifică directorul Spam.
   Se afișează starea de confidențialitate a contului validat.

Dacă se identifică scurgeri de informații pe oricare dintre conturile tale, îți recomandăm să modifici parola acestora cât mai curând posibil. Pentru a crea o parolă puternică și sigură, ia în considerare aceste sfaturi:

- Folosește cel puțin opt caractere.

- Include litere mari și mici.
- Adaugă cel puțin un număr sau simbol, precum #, @, % sau !.

După securizarea unui cont care a fost implicat într-o scurgere de informații, poți confirma modificările marcând încălcările identificate ca fiind Rezolvat(e). Pentru a face acest lucru:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Confidențialitatea contului**.
3. Selectează contul pe care tocmai l-ai securizat.
4. Apasă pe încălcarea față de care ți-ai securizat contul.
5. Apasă **REZOLVAT** pentru a confirma securizarea contului.

După ce toate încălcările de securitate sunt marcate ca fiind **Rezolvate**, contul nu va mai apărea ca fiind implicat într-o încălcare de securitate, cel puțin până când nu se detectează o nouă încălcare de securitate.

Pentru a dezactiva opțiunea de notificare la fiecare scanare automată:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Dezactivează butonul corespunzător din zona Confidențialitate cont.

3.7. Blocare Aplicații

Aplicațiile instalate, cum ar fi e-mail, fotografii sau mesaje, pot conține date personale pe care dorești să le menții confidențiale prin restricționarea selectivă a accesului la acestea.

Funcția de Blocare aplicații te ajută să blochezi accesul nedorit la aplicații prin setarea unui cod de acces PIN. Codul PIN pe care îl configurezi trebuie să aibă cel puțin 4 cifre, însă nu mai mult de 8, și va trebui să îl introduci de fiecare dată când accesezi aplicațiile restricționate selectate.

Poți utiliza autentificarea biometrică (precum confirmarea cu ajutorul amprentei sau prin recunoaștere facială) în locul codului PIN configurat.

3.7.1. Activarea App Lock

Pentru a restricționa accesul la aplicațiile selectate, configurați funcția Blocare aplicații din cardul afișat în Panoul de bord după activarea funcție Antifurt.

Alternativ, poți activa funcția Blocare aplicații urmând pașii de mai jos:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atinge **Blocare aplicație**.
3. Atingeți **PORNIȚI**.
4. Permite accesul la datele privind utilizarea pentru Bitdefender Security.
5. Permite **trimiterea de notificări în timpul utilizării altor aplicații**.
6. Reveniți la aplicație, configurați codul de acces și apoi atingeți **CONFIGURARE PIN**.

> **Notă**
> Acest pas este disponibil numai dacă nu ai configurat anterior codul PIN în secțiunea Antifurt.

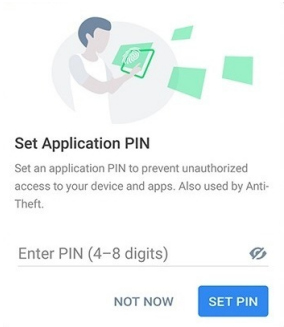
7. Activează opțiunea Fotografiere pentru a putea identifica orice intrus care încearcă să îți acceseze datele.

> **Notă**
> Sunt necesare permisiuni suplimentare pentru Android 6 în legătură cu funcția Instantanee. Pentru a o activa, permiteți ca **Antivirus** să facă fotografii și să înregistreze clipuri video.

8. Selectează aplicațiile pe care dorești să le protejezi:

Introducerea codului PIN sau aplicarea amprentei greșite de cinci ori consecutiv activează o sesiune de întrerupere a funcționării de 30 de secunde. Astfel, orice încercare de a accesa aplicațiile protejate va fi blocată.

> **Notă**
> Același cod PIN este utilizat și de aplicația Antifurt pentru a te ajuta să îți localizezi dispozitivul.



3.7.2. Mod de blocare

La prima adăugare a unei aplicații la secțiunea Blocare aplicații, apare ecranul Mod blocare aplicații. De aici poți alege momentul în care funcția Blocare aplicații ar trebui să protejeze aplicațiile instalate pe dispozitivul tău.

Poți selecta una dintre următoarele opțiuni:

- **Solicită deblocare de fiecare dată** - de fiecare dată când sunt accesate aplicațiile blocate, va trebui să utilizezi codul PIN sau amprenta pe care le-ai setat.
- **Păstrează deblocat până la oprirea ecranului** - vei putea accesa la aplicațiile până la oprirea ecranului.
- **Blocare după 30 de secunde** - poți ieși și accesa din nou aplicațiile tale deblocate în interval de 30 de secunde.

Dacă dorești să modifici setarea selectată:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Atinge **Solicită deblocare de fiecare dată** din secțiunea Blocare aplicații.
4. Alege opțiunea dorită.

3.7.3. Setări Blocare Aplicații

Pentru o configurare avansată a funcției Blocare aplicații:

1. Atingeți **Mai mult** pe bara de navigare de jos.

2. Atingeți **Setări**.

În zona Blocare aplicații, poți configura următoarele opțiuni:

- **Sugestie aplicații sensibile** - vei primi o notificare de blocare de fiecare dată când instalezi o aplicație sensibilă.
- **Solicită deblocare de fiecare dată** - selectează una dintre opțiunile de blocare și deblocare.
- **Deblocare inteligentă** - păstrează aplicațiile deblocate cât timp ești conectat la rețele Wi-Fi sigure.
- **Randomizare taste** - împiedică citirea codului PIN prin randomizarea poziției cifrelor.

3.7.4. Foto Instant

Cu funcția Bitdefender Foto instant îi poți surprinde pe prietenii sau rudele tale când nu se așteaptă. Astfel, îi poți învăța să nu-și mai arunce privirile curioase prin fișierele tale personale sau aplicațiile pe care le folosești.

Această caracteristică funcționează foarte simplu: de fiecare dată când codul PIN sau amprenta setate pentru a vă proteja aplicațiile sunt introduse greșit de trei ori consecutiv, se realizează o fotografie prin camera frontală. Imaginea este salvată împreună cu data și ora, precum și motivul realizării, și poate fi vizualizată atunci când deschideți Bitdefender Mobile Security pentru a accesa caracteristica Blocare aplicații.

> **Notă**
> Această caracteristică este disponibilă numai pentru telefoanele prevăzute cu cameră frontală.

Pentru a configura Fotografia instant pentru Blocare aplicații:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Activează butonul corespunzător din zona Fotografie instant.

Instantaneele făcute atunci când este introdus codul PIN incorect sunt afișate în fereastra Blocare aplicații și pot fi vizualizate pe întregul ecran.

Alternativ, acestea pot fi vizualizate în contul Bitdefender:

1. Mergi la: https://central.bitdefender.com.

2. Conectați-vă la contul dvs.
3. Selectează secțiunea **Dispozitivele mele**.
4. Selectați dispozitivul dvs. Android, apoi **Anti furt** fila.
5. Atingeți ⋮ chiar lângă **Verificați-vă instantaneele** pentru a vedea cele mai recente fotografii care au fost făcute.

Sunt salvate doar cele mai recente două fotografii.

Pentru a opri încărcarea instantaneelor în contul tău Bitdefender:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Dezactivează opțiunea **Încărcare fotografii** din secțiunea Fotografie instant.

3.7.5. Deblocare Inteligentă

O metodă ușoară de a evita ca funcția Blocare aplicații să îți solicite să introduci codul PIN sau amprenta de confirmare pentru aplicațiile protejate de fiecare dată când le accesezi este de a activa opțiunea Deblocare inteligentă.

Cu funcția Deblocare inteligentă poți seta ca fiind sigure rețelele Wi-Fi la care te conectezi de obicei și, atunci când ești conectat la acestea, setările funcției Blocare aplicații vor fi dezactivate pentru aplicațiile protejate.

Pentru a configura funcția Deblocare inteligentă:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Blocare aplicație**.
3. Apasă pe butonul .
4. Apasă butonul de lângă **Deblocare inteligentă** în cazul în care această caracteristică nu este activată.
   Validează folosind amprenta sau codul PIN.
   Prima dată când activezi această caracteristică, va trebui să permiți utilizarea locației. Apasă butonul **PERMITE** și apasă încă o dată **PERMITE**.
5. Atinge **ADAUGĂ** pentru a configura conexiunea Wi-Fi pe care o utilizezi la momentul actual ca fiind sigură.

Dacă te răzgândești, poți dezactiva funcția și rețelele Wi-Fi pe care le-ai setat ca fiind sigure vor fi tratate că fiind nesigure.

3.8. Rapoarte

Funcția Rapoarte păstrează un jurnal detaliat al evenimentelor asociate activității de scanare de pe dispozitivul tău.

La fiecare eveniment relevant pentru securitatea dispozitivului tău un nou mesaj este inclus in Reports.

Pentru a accesa secțiunea Rapoarte:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atinge **Rapoarte**.

În fereastra Rapoarte, sunt disponibile următoarele secțiuni:

- **RAPOARTE SĂPTĂMÂNALE** - aici, ai acces la starea de securitate și la sarcinile efectuate în săptămâna curentă și anterioară. Raportul săptămânii curente este generat în fiecare duminică și vei primi o notificare prin care esti informat cu privire la disponibilitatea acestuia.
  Săptămânal va fi afișată o nouă recomandare în această secțiune, astfel, asigura-te ca revii în mod regulat pentru a exploata la maxim aplicația.
  Pentru a opri primirea notificărilor de fiecare dată când se generează un raport:
  1. Atingeți **Mai mult** pe bara de navigare de jos.
  2. Atingeți **Setări**.
  3. Dezactivează opțiunea **Notificare raport nou** din zona de Rapoarte.
- **JURNAL ACTIVITATE** - de aici, poți verifica informațiile referitoare la activitatea aplicației Bitdefender Mobile Security, de la instalarea acesteia pe dispozitivul tău Android.
  Pentru a șterge jurnalul de activitate disponibil:
  1. Atingeți **Mai mult** pe bara de navigare de jos.
  2. Atingeți **Setări**.
  3. Atinge **Șterge Jurnal de activitate** și apoi apasă pe **ȘTERGE**.

3.9. WearON

Cu funcția Bitdefender WearON, îți poți găsi cu ușurință smartphone-ul, indiferent dacă l-ai lăsat la birou într-o sală de conferințe sau sub o pernă de canapea. Dispozitivul poate fi găsit chiar dacă ai activat modul silențios.

Menține această funcție activată pentru a te asigura că ai întotdeauna smartphone-ul la îndemână.

> **Notă**
> Funcția este compatibilă cu Android 4.3 și Android Wear.

3.9.1. Activarea WearON

Pentru a folosi WearON, nu trebuie decât să te conectezi smartwatch-ul la aplicația Bitdefender Mobile Security și să activezi funcția cu următoarea comandă vocală:

Inițiere:<Unde e telefonul meu>

Bitdefender WearON pune la dispoziție două comenzi:

1. **Alertă telefon**
   Cu funcția Phone Alert îți poți găsi rapid smartphone-ul, ori de câte ori ești prea departe de el.
   Dacă ai smartwatch-ul la tine, acesta detectează automat aplicația de pe telefonul tău și vibrează atunci când ești prea departe de telefon și conexiunea Bluetooth este pierdută.
   Pentru a activa această funcție, deschide Bitdefender Mobile Security, atinge **Global Settings** în meniu și selectează butonul corespunzător în secțiunea WearON.
2. **Scream**
   Găsirea telefonului nu a fost niciodată mai ușoară. Ori de câte ori uitați unde v-ați lăsat telefonul, atingeți comanda Scream de pe ceas pentru a face telefonul să "țipe".

3.10. Despre

Pentru a găsi informații despre versiunea Bitdefender Mobile Security pe care ai instalat-o, pentru a accesa și citi Contractul de abonament și Politica de confidențialitate, precum și pentru a vizualiza Licențele cu sursă deschisă:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Atinge opțiunea dorită în secțiunea Despre.

4. DESPRE BITDEFENDER CENTRAL

Bitdefender Central este platforma din care ai acces la caracteristicile și serviciile online ale produsului și de unde poți efectua de la distanță sarcini importante pe dispozitivele pe care este instalat Bitdefender. Te poți conecta la contul tău Bitdefender de pe orice calculator sau dispozitiv mobil conectat la internet accesând https://central.bitdefender.com sau direct din aplicația Bitdefender Central pe dispozitivele Android sau iOS.

Pentru a instala aplicația Bitdefender Central pe dispozitivele tale:

- **Pe Android** - caută Bitdefender Central în Google Play și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.
- **Pe iOS** - caută Bitdefender Central în App Store și apoi descarcă și instalează aplicația. Urmează pașii necesari pentru finalizarea instalării.

După autentificare, poți face următoarele:

- Descarcă și instalează Bitdefender pe sistemele de operare Windows, macOS, iOS și Android. Produsele disponibile pentru descărcare sunt:
  - Bitdefender Mobile Security for Android
  - Bitdefender Mobile Security for iOS
  - Gama de produse Bitdefender Windows
  - Bitdefender Antivirus for Mac
- Administrează și reînnoiește abonamentele Bitdefender.
- Adaugă dispozitive noi la rețeaua ta și administrează-le oriunde te-ai afla.
- Protejați-vă dispozitivele din rețea și datele de pe acestea împotriva furtului sau a pierderii cu ajutorul funcției Anti-Theft.

4.1. Accesează Bitdefender Central

Există două metode pentru a accesa Bitdefender Central

- Din browser-ul web:
  1. Deschide un browser web pe orice dispozitiv cu acces la internet.

2. Mergi la: https://central.bitdefender.com.
3. Conectează-te la contul tău cu ajutorul adresei de e-mail și parolei.

- De pe dispozitivul tău Android sau iOS:
  Deschide aplicația Bitdefender Central pe care ai instalat-o.

  Notă
  În acest material prezentăm opțiunile pe care le poți găsi în interfața web.

4.2. Autentificare în doi pași

Metoda de autentificare în doi pași adaugă un strat suplimentar de securitate contului tău Bitdefender, solicitând un cod de autentificare suplimentar pe lângă datele tale de conectare. În acest fel, vei evita ca altcineva să preia controlul asupra contului tău și veți ține la distanță atacuri cibernetice precum keyloggere, atacuri de tip „brute-force” sau pe bază de dicționar.

4.2.1. Activați autentificarea de tip „two-factor”

Prin activarea autentificării în doi pași, contul tău Bitdefender devine mult mai sigur. Identitatea ta va fi verificată de fiecare dată când te vei conecta de la diferite dispozitive pentru a instala unul dintre produsele Bitdefender, pentru a verifica starea abonamentului tău sau pentru a executa sarcini de la distanță pe dispozitivele tale.

Pentru a activa autentificarea de tip „two-factor”:

1. Acces Bitdefender Central.
2. Apasă pe pictograma din partea dreaptă sus a ecranului.
3. Apasă pe **Contul Bitdefender** din meniul vertical.
4. Selectează fila **Parolă și securitate**.
5. Atingeți **INCEPE**.
   Selectează una dintre următoarele metode:

   - **Aplicație de autentificare** - folosește o aplicație de autentificare pentru a genera un cod de fiecare dată când dorești să te conectezi la contul tău Bitdefender.

Dacă dorești să utilizezi o aplicație de autentificare, dar nu ești sigur ce să alegi, îți punem la dispoziție o listă cu aplicațiile de autentificare pe care le recomandăm.

a. Selectează **UTILIZEAZĂ O APLICAȚIE DE AUTENTIFICARE** pentru a începe.

b. Pentru a te autentifica pe un dispozitiv cu sistem de operare Android sau iOS, folosește dispozitivul tău pentru a scana codul QR.
Pentru a te autentifica pe un laptop sau computer, poți adăuga manual codul afișat.
Apasă **CONTINUĂ**.

c. Introdu codul furnizat de aplicație sau cel afișat la pasul anterior, apoi apasă **ACTIVARE**.

- **E-mail** - de fiecare dată când te conectezi la contul tău Bitdefender, se va trimite un cod de verificare către căsuța ta de e-mail. Verifică contul de e-mail și introdu codul primit.

a. Selectează **UTILIZEAZĂ ADRESA DE E-MAIL** pentru a începe.

b. Verifică-ți contul de e-mail și introdu codul furnizat.
Reține că ai cinci minute la dispoziție pentru a-ți verifica contul de e-mail și pentru a introduce codul generat. Dacă timpul expiră, va trebui să generezi un nou cod urmând aceiași pași.

c. Apasă **ACTIVARE**.

d. Ai la dispoziție zece coduri de activare. Poți copia, descărca sau tipări lista pentru a o utiliza ulterior în cazul în care îți pierzi adresa de e-mail sau nu te poți conecta. Fiecare cod poate fi utilizat o singură dată.

e. Atinge **EFECTUAT**.

Dacă nu mai dorești să folosești Autentificarea în doi pași:

1. Selectează opțiunea **DEZACTIVEAZĂ AUTENTIFICAREA ÎN DOI PAȘI**.
2. Verifică aplicația sau contul de e-mail și introdu codul primit.
Dacă ai optat pentru a primi codul de autentificare prin e-mail, ai cinci minute la dispoziție pentru a-ți verifica contul de e-mail și pentru a

introduce codul generat. Dacă timpul expiră, va trebui să generezi un nou cod urmând aceiași pași.

3. Confirmă alegerea.

4.3. Adăugarea dispozitivelor sigure

Pentru a ne asigura că tu ești singura persoană care poate accesa contul tău Bitdefender, este posibil să îți solicităm mai întâi un cod de securitate. Dacă dorești să omiți acest pas de fiecare dată când te conectezi de pe același dispozitiv, îți recomandăm să îl setezi ca dispozitiv sigur.

Pentru a adăuga dispozitive marcate ca fiind sigure:

1. Acces Bitdefender Central.
2. Apasă pe pictograma din partea dreaptă sus a ecranului.
3. Atingeți **Contul Bitdefender** în meniul slide.
4. Selectează **Parolă și securitate** fila.
5. Apasă **Dispozitive de încredere**.
6. Se afișează lista cu dispozitivele pe care este instalat Bitdefender. Selectează dispozitivul dorit.

Poți adăuga oricât de multe dispozitive dorești, cu condiția ca pe acestea să fie instalat Bitdefender și abonamentul tău să fie valid.

4.4. Dispozitivele mele

Zona **Dispozitivele mele** din contul Bitdefender îți oferă posibilitatea de a instala, administra și efectua operațiuni de la distanță pe produsul Bitdefender de pe orice dispozitiv pornit și conectat la internet. Filele dispozitivelor afișează numele dispozitivului, starea protecției și dacă există riscuri de securitate ce afectează protecția dispozitivelor tale.

4.4.1. Adăugarea unui dispozitiv nou

Dacă abonamentul dvs. acoperă mai multe dispozitive, puteți adăuga un dispozitiv nou și puteți instala Bitdefender Mobile Security pe acesta, după cum urmează:

1. Accesează Bitdefender Central.

2. Selectează panoul **Dispozitivele mele**, apoi atingeți **INSTALATI PROTECTIA**.
3. Alegeți una dintre cele două opțiuni disponibile:
   - **Protejați acest dispozitiv**
     Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, atingeți butonul corespunzător.
   - **Protejați alte dispozitive**
     Selectați această opțiune, apoi selectați proprietarul dispozitivului. Dacă dispozitivul aparține altcuiva, atingeți butonul corespunzător.
     Apasă pe **TRIMITE LINK DE DESCĂRCARE**. Introdu o adresă de e-mail în câmpul corespunzător și apasă pe **TRIMITE E-MAIL**. Reține că linkul pentru descărcare generat este valabil doar timp de 24 de ore. Dacă linkul expiră, trebuie să generezi unul nou urmând aceiași pași.
     Pe dispozitivul pe care doriți să vă instalați produsul Bitdefender, verificați contul de e-mail pe care l-ați introdus, apoi atingeți butonul de descărcare corespunzător.
4. Așteaptă să se finalizeze descărcarea și apoi execută aplicația de instalare.

4.4.2. Personalizează-ți dispozitivul

Pentru a-ți identifica ușor dispozitivele, poți personaliza denumirile acestora:

1. Acces Bitdefender Central.
2. Selectați secțiunea **Dispozitivele mele**.
3. Efectuează clic pe fila dispozitivului dorit și apoi pe pictograma ⋮ din colțul din dreapta sus al ecranului.
4. Selectează **Setări**.
5. Introdu o denumire nouă în câmpul **Denumire dispozitiv** și apoi apasă pe **SALVARE**.

Poți crea și aloca un deținător al fiecăruia dintre dispozitivele tale pentru o mai bună administrare a acestora:

1. Acces Bitdefender Central.

2. Selectează **Dispozitivele mele** panou.
3. Atingeți cardul dispozitivului dorit, apoi butonul ⋮ pictograma din colțul din dreapta sus al ecranului.
4. Selectează **Profil**.
5. Efectuează clic pe **Adăugare deținător** și completează câmpurile corespunzătoare. Personalizează-ți profilul adăugând o fotografie, selectând data nașterii și adăugând o adresă de e-mail și un număr de telefon.
6. Faceți clic pe **ADAUGĂ** pentru a salva profilul.
7. Selectează deținătorul dorit din lista **Deținător dispozitiv**, apoi apasă pe **ATRIBUIRE**.

4.4.3. Acțiuni de la distanță

Pentru a actualiza Bitdefender de la distanță pe un dispozitiv:

1. Accesează Bitdefender Central.
2. Selectează **Dispozitivele mele** panou.
3. Atingeți cardul dispozitivului dorit, apoi butonul ⋮ pictograma din colțul din dreapta sus al ecranului.
4. Selectează **Actualizare**.

Pentru mai multe operațiuni ce pot fi efectuate de la distanță și informații referitoare la produsul Bitdefender instalat pe un anumit dispozitiv, efectuează clic pe fila dispozitivului dorit.

După ce ai efectuat clic pe cardul dispozitivului, sunt disponibile următoarele file:

- **Panou de control.** În această fereastră, poți vizualiza detalii despre dispozitivul selectat, poți verifica starea de protecție a acestuia, statusul aplicației Bitdefender VPN și câte amenințări au fost blocate în ultimele șapte zile. Starea de protecție poate fi verde, atunci când nu există probleme care îți afectează dispozitivul, galbenă, atunci când dispozitivul necesită o intervenție din partea ta, sau roșie, atunci când există un risc la adresa dispozitivului tău. Dacă există probleme care afectează dispozitivul tău, efectuează clic pe săgeata jos din zona de status din partea de sus pentru a afla mai multe detalii. De aici, poți

- **Protecție.** Din această fereastră poți rula de la distanță o operațiune de scanare rapidă sau scanare a sistemului pe dispozitivele tale. Fă clic pe butonul **SCANARE** pentru a iniția procesul. De asemenea, poți vedea când a avut loc ultima scanare a dispozitivului și poți accesa un raport al celei mai recente scanări efectuate, care conține cele mai importante informații.
- **Optimizare.** Această funcție îți permite să îmbunătățești de la distanță performanța unui dispozitiv, prin scanarea rapidă, detectarea și ștergerea fișierelor inutile. Apasă pe butonul **INIȚIERE**, apoi selectează zonele pe care dorești să le optimizezi. Apasă din nou pe **INIȚIERE** pentru a iniția procesul de optimizare. Fă clic pe **Mai multe detalii** pentru a accesa un raport detaliat despre problemele corectate.
- **Anti-furt.** Dacă nu mai știi unde ți-ai pus dispozitivul sau dacă a fost furat sau pierdut, funcția Anti-furt îți poate localiza dispozitivul și poate efectua acțiuni de la distanță. Fă clic pe **LOCALIZARE** pentru a afla poziția dispozitivului. Se afișează ultima poziție cunoscută, ora și data la care dispozitivul s-a aflat acolo.
- **Vulnerabilitate.** Apasă pe butonul **SCANARE** din fila Vulnerabilitate pentru a verifica dacă există vulnerabilități la nivelul unui dispozitiv, cum ar fi dacă îi lipsesc actualizări Windows sau dacă există aplicații neactualizate sau parole nesigure. Vulnerabilitățile nu pot fi corectate de la distanță. În cazul în care se detectează o vulnerabilitate, va trebui să inițiezi o scanare nouă a dispozitivului și apoi să iei măsurile recomandate. Apasă pe **Mai multe detalii** pentru a accesa un raport detaliat despre problemele identificate.

4.5. Activitate

În secțiunea Activitate, ai acces la informații despre dispozitivele pe care este instalat Bitdefender.

Când accesezi fereastra **Activitate**, vor deveni disponibile următoarele carduri:

- **Dispozitivele mele.** Accesând această secțiune, poți vizualiza numărul de dispozitive conectate și stările lor de protecție. Pentru a remedia de la distanță anumite probleme identificate pe dispozitivele detectate, selectează **Remediere probleme** și apoi **SCANARE ȘI REMEDIERE PROBLEME**.

Pentru a vizualiza detaliile referitoare la problemele detectate, selectează **Vizualizează problemele**.
Informațiile despre amenințările detectate nu pot fi extrase de pe dispozitivele cu iOS.

- **Amenințări blocate.** Aici poți vizualiza un grafic care prezintă statistici globale, ce includ informații despre amenințările blocate în ultimele 24 de ore și șapte zile. Informațiile afișate sunt preluate în funcție de comportamentul periculos detectat în cazul fișierelor, aplicațiilor și adreselor URL accesate.
- **Principalii utilizatori cu amenințări blocate.** Aici poți vedea un top al utilizatorilor la care au fost detectate cele mai multe amenințări.
- **Principalele dispozitive cu amenințări blocate.** Aici poți vedea un top al dispozitivelor pe care au fost detectate cele mai multe amenințări.

4.6. Abonamentele mele

Platforma Bitdefender Central vă oferă posibilitatea de a administra cu ușurință abonamentele deținute pentru toate dispozitivele.

4.6.1. Verifică abonamentele disponibile

Pentru a verifica abonamentele disponibile:

1. Accesează Bitdefender Central.
2. Selectați fereastra **Abonamentele mele**.

Aici găsești informații referitoare la valabilitatea abonamentelor pe care le deții și la numărul de dispozitive care utilizează fiecare dintre aceste abonamente.

Poți adăuga un dispozitiv nou unui abonament sau poți îl reînnoi selectând un card de abonament.

> **Notă**
> Poți avea mai multe abonamente în contul tău cu condiția ca acestea să fie pentru platforme diferite (Windows, macOS, iOS sau Android).

4.6.2. Activare abonament

Un abonament poate fi activat în timpul procesului de instalare folosind contul Bitdefender. Concomitent cu procesul de activare, începe să curgă și perioada de valabilitate a abonamentului.

Dacă ați achiziționat un cod de activare de la unul dintre distribuitorii noștri sau l-ați primit cadou, puteți adăuga valabilitatea acestuia la abonamentul Bitdefender.

Pentru a activa un abonament folosind un cod de activare, urmează pașii de mai jos:

1. Accesează Bitdefender Central.
2. Selectează **Abonamentele mele** panou.
3. Apasă pe butonul **COD DE ACTIVARE**, apoi introdu codul în câmpul corespunzător.
4. Selectează **ACTIVARE** pentru a continua.

Abonamentul este acum activat.

4.6.3. Reînnoire abonament

Dacă ai dezactivat reînnoirea automată a abonamentului Bitdefender, îl poți reînnoi manual parcurgând pașii următori:

1. Accesează Bitdefender Central.
2. Selectează panoul **Abonamentele mele**.
3. Selectează cardul de abonament dorit.
4. Selectează **REÎNNOIRE** pentru a continua.

Se deschide o pagină web în browser-ul dvs., de unde puteți reînnoi abonamentul Bitdefender.

4.7. Notificări

Pentru a vă ajuta să fiți la curent cu ceea ce se întâmplă pe dispozitivele asociate contului dumneavoastră, aveți la dispoziție pictograma . Odată ce efectuați clic pe aceasta, veți avea o imagine de ansamblu ce constă în informații despre activitatea produselor Bitdefender instalate pe dispozitivele dumneavoastră.

5. ÎNTREBĂRI FRECVENTE

De ce este necesară o conexiune la internet pentru funcționarea Bitdefender Mobile Security?

Aplicația trebuie să comunice cu serverele Bitdefender pentru a determina starea de securitate a aplicațiilor scanate și a paginilor web pe care le vizitați, precum și pentru a primi comenzi de la contul tău Bitdefender, la folosirea funcțiilor Anti-Theft.

Pentru ce este nevoie de fiecare permisiune solicitată de Bitdefender Mobile Security?

- Acces la internet -> utilizat pentru comunicarea în cloud.
- Citire stare și identitate telefon > utilizată pentru a detecta dacă dispozitivul este conectat la internet și pentru a extrage anumite informații despre dispozitiv necesare pentru a crea o identitate unică pentru comunicarea cu cloud-ul Bitdefender.
- Citire și scriere marcaje în browser > modulul Protecție web șterge site-urile periculoase din istoricul tău de navigare.
- Citire date jurnal > Bitdefender Mobile Security identifică indicii ale activității periculoase din jurnalele Android.
- Locație > este necesară pentru localizarea de la distanță.
- Camera -> necesară pentru funcția Foto instant.
- Stocare > utilizată pentru a permite Scanerului malware să verifice cardul SD.

Cum pot opri trimiterea către Bitdefender a informațiilor despre aplicațiile suspecte?

Bitdefender Mobile Security trimite, în mod automat, rapoarte către serverele Bitdefender cu privire la aplicațiile suspecte pe care le instalezi. Aceste informații sunt esențiale pentru îmbunătățirea detectării amenințărilor și ne poate ajuta să îți oferim o experiență mai bună în viitor. Dacă nu mai dorești să ne transmiți informații despre aplicațiile suspecte:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.

3. Dezactivează opțiunea **Detectare în cloud** din zona Scaner programe periculoase.

Unde pot vedea detalii despre activitatea aplicației?

Bitdefender Mobile Security păstrează un jurnal al tuturor acțiunilor importante, modificărilor de stare și al altor mesaje critice legate de activitatea sa. Pentru accesare, vizualizați care este activitatea aplicației:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Rapoarte**.
   În fereastra RAPOARTE SĂPTĂMÂNALE poți accesa rapoartele care sunt generate în fiecare săptămână, iar în fereastra JURNAL ACTIVITATE poți vizualiza informații despre activitatea aplicației tale Bitdefender.

Am uitat codul PIN pe care l-am configurat pentru protejarea aplicației. Ce fac?

1. Acces Bitdefender Central.
2. Selectează **Dispozitivele mele** panou.
3. Atinge cardul dispozitivului dorit și apoi atinge ⋮ din colțul din dreapta sus al ecranului.
4. Selectați **Setări**.
5. Recuperați codul PIN din câmpul **PIN aplicație**.

Cum pot schimba codul PIN pe care l-am configurat pentru Blocare aplicații și Antifurt?

Dacă dorești să modifici codul PIN pe care l-ai configurat pentru Blocare aplicații și Antifurt:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Setări**.
3. Atinge **COD PIN** de Securitate în secțiunea Antifurt.
4. Tastează codul PIN actual.
5. Tastează noul cod PIN pe care dorești să îl configurezi.

Cum pot dezactiva funcția Blocare aplicații?

Nu există o opțiune de dezactivare a funcției Blocare aplicații, dar o poți opri cu ușurință prin debifarea casetelor de lângă aplicațiile selectate după introducerea codului PIN sau amprentei de validare configurate.

Cum pot configura o altă rețea wireless ca fiind de încredere?

Mai întâi, trebuie să îți conectezi dispozitivul la rețeaua wireless pe care dorești să o configurezi ca fiind sigură. Apoi urmează pașii de mai jos:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atingeți **Blocare aplicație**.
3. Atinge în colțul din dreapta sus.
4. Atinge **ADĂUGARE** de lângă rețeaua pe care dorești să o configurezi ca fiind sigură.

Cum pot renunța la afișarea fotografiilor realizate de dispozitivele mele?

Pentru a nu mai afișa fotografiile realizate de dispozitivele tale:

1. Acces Bitdefender Central.
2. Atinge în partea dreaptă de sus a ecranului.
3. Atinge **Setări** din meniul vertical.
4. Dezactivează opțiunea **Afișează/nu mai afișa instantanee realizate pe dispozitivele tale**.

Cum pot efectua cumpărături online în siguranță?

Cumpărăturile online prezintă riscuri mari atunci când sunt ignorate anumite detalii. Pentru a nu deveni victima unei fraude, îți recomandăm următoarele:

- Păstrează securitatea ta actualizată.
- Trimite plăți online numai dacă este asigurată protecția cumpărătorului.
- Folosește un VPN atunci când te conectezi la internet prin intermediul unor rețele wireless publice sau nesecurizate.
- Atenție la parolele atribuite conturilor tale online. Acestea trebuie să fie puternice și să includă litere mari și mici, numere și simboluri (@, !, %, #, etc.).
- Asigură-te că informațiile sunt trimise prin intermediul unor conexiuni sigure. Extensiile site-urilor online trebuie să fie HTTPS://, nu HTTP://.

Când ar trebui să utilizez Bitdefender VPN?

Trebuie să procedezi cu atenție atunci când accesezi, descarci sau încarci conținut pe internet. Ca să fii sigur că ești protejat atunci când navighezi pe web, îți recomandăm să folosești Bitdefender VPN când:

- când dorești să te conectezi la rețele wireless publice
- când dorești să accesezi conținut care în mod normal este restricționat în anumite zone, indiferent dacă ești acasă sau în străinătate
- când dorești să-ți păstrezi confidențialitatea datelor tale personale (nume de utilizator, parole, datele cardului de credit etc.)
- când dorești să-ți ascunzi adresa IP

Bitdefender VPN va avea un impact negativ asupra autonomiei bateriei dispozitivului meu?

Bitdefender VPN este conceput să îți protejeze datele personale, să îți ascundă adresa IP în timp ce ești conectat la rețele wireless nesecurizate și la conținutul cu acces restricționat din anumite țări. Pentru a evita consumarea inutilă a bateriei, îți recomandăm să folosești funcția VPN numai atunci când ai nevoie de ea și să te deconectezi atunci când ești offline.

De ce încetinește viteza de internet atunci când sunt conectat cu Bitdefender VPN?

Bitdefender VPN este conceput să îți ofere o navigare ușoară pe web; totuși, conexiunea ta la internet sau distanța față de serverul la care te conectezi pot cauza o încetinire. În acest caz, dacă nu trebuie neapărat să te conectezi din locația ta la un server îndepărtat (de ex. din SUA sau China), îți recomandăm să permiți Bitdefender VPN să te conecteze automat la cel mai apropriat server, sau să găsești un server mai apropiat de locația ta curentă.

Pot schimba contul Bitdefender asociat dispozitivului meu?

Da, puteți schimba cu ușurință contul Bitdefender asociat dispozitivului dvs. urmând pașii de mai jos:

1. Atingeți **Mai mult** pe bara de navigare de jos.
2. Atinge adresa ta de e-mail.
3. Atinge **Deconectează-te de la contul tău**. Dacă a fost configurat un cod PIN, ți se solicită să îl introduci.
4. Confirmați alegerea dvs.

5. Introdu adresa e-mail și parola contului tău în câmpurile corespunzătoare și selectează **AUTENTIFICARE**.

Ce impact va avea Bitdefender Mobile Security asupra dispozitivului meu în materie de performanțe și baterie?

Impactul este extrem de redus. Aplicația rulează numai atunci când este absolut necesar – inclusiv la instalare și în timpul utilizării interfeței – sau atunci când efectuezi o verificare de siguranță. Bitdefender Mobile Security nu rulează în fundal atunci când efectuați apeluri telefonice, când scrieți mesaje sau vă jucați.

Ce înseamnă Administratorul dispozitivului?

Administratorul dispozitivului este o funcție Android care oferă aplicației Bitdefender Mobile Security permisiunile necesare pentru a efectua anumite sarcini de la distanță. În lipsa acestor drepturi de acces, blocarea de la distanță nu ar funcționa, iar caracteristica de ștergere a datelor de pe dispozitiv nu ar putea elimina datele tale în totalitate. Dacă dorești să ștergi aplicația, asigură-te că retragi aceste drepturi de acces înainte de a încerca dezinstalarea accesând **Setări > Securitate > Selectare administratori dispozitiv**.

Cum să remediați eroarea "Lipsă Token Google" care apare la autentificarea din Bitdefender Mobile Security.

Această eroare apare atunci când dispozitivul dumneavoastră nu este asociat cu un cont Google sau este asociat cu un cont, dar o problemă temporară împiedică conectarea la Google. Încercați una dintre următoarele soluții:

- Accesează Setări > Aplicații > Gestionare aplicațiile > Bitdefender Mobile Security și apasă pe **Ștergere date**. Apoi încearcă din nou să te conectezi.
- Asigura-te că dispozitivul tău este asociat cu un cont Google.
  Pentru a verifica, accesează Setări > Conturi și sincronizare și vezi dacă apare vreun cont Google în secțiunea **Gestionare conturi**. Dacă nu apare niciun cont, adaugă contul tău, repornește dispozitivul și încearcă să te conectezi din nou în Bitdefender Mobile Security.
- Repornește dispozitivul și încearca să te autentifici din nou.

În ce limbi este disponibil Bitdefender Mobile Security?

Bitdefender Mobile Security este disponibil în prezent în următoarele limbi:

- Portugheză braziliană
- Cehă
- Olandeză
- Engleză
- Franceză
- Germană
- Greacă
- Maghiară
- Italiană
- Japoneză
- Coreană
- Poloneză
- Portugheză
- Română
- Rusă
- Spaniolă
- Suedeză
- Thailandeză
- Turcă
- Vietnameză

În versiunile ulterioare vor fi adăugate și alte limbi. Pentru a modifica limba în care se afișează interfața Bitdefender Mobile Security, accesează setările**Limbă și tastatură** ale dispozitivului tău și setează limba pe care dorești să o utilizezi.

6. OBȚINE AJUTOR

6.1. Solicitarea ajutorului

Bitdefender le oferă clienților săi un serviciu rapid și precis de asistență, la un nivel inegalabil. Dacă întâmpini probleme sau dacă ai întrebări legate de produsul tău Bitdefender, poți utiliza o serie de resurse online pentru a identifica o soluție sau un răspuns. De asemenea, poți contacta echipa Serviciului de asistență pentru clienți. Reprezentanții noștri îți vor răspunde la întrebări în timp util și îți vor oferi sprijinul de care ai nevoie.

6.2. Resurse online

Sunt disponibile mai multe resurse online pentru a vă ajuta la soluționarea problemelor și întrebărilor referitoare la produsul Bitdefender.

- Centrul de asistență Bitdefender:
  https://www.bitdefender.ro/consumer/support/
- Comunitatea de experți Bitdefender:
  https://community.bitdefender.com/ro
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

De asemenea, puteți folosi motorul de căutare preferat pentru a afla informații suplimentare referitoare la securitatea informatică, produsele și compania Bitdefender.

6.2.1. Centrul de asistență Bitdefender

Centrul de Asistență Bitdefender este un depozit online ce conține informații despre produsele Bitdefender. Acesta stochează, într-un format ușor accesibil, rapoarte privind rezultatele unor activități continue de asistență tehnică și remediere ale echipelor de asistență și dezvoltare Bitdefender, alături de articole mai generale referitoare la prevenirea amenințărilor, gestionarea soluțiilor Bitdefender cu explicații detaliate și multe alte articole.

Bitdefender Support Center 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 bug-uri venind de la clienții BitDefender ajung în cele din urmă în Bitdefender Support Center, ca rapoarte asupra eliminării bug-urilor, fișe de lucru sau articole informative pentru a suplimenta fișierele de suport ale produsului.

Centrul de asistență Bitdefender este disponibil oricând la următoarea adresă: https://www.bitdefender.ro/consumer/support/.

6.2.2. Comunitatea de experți Bitdefender

Comunitatea de experți este un mediu în care utilizatorii, pasionații și fanii Bitdefender pot interacționa, face schimb de idei, se pot ajuta reciproc și își pot împărtăși cunoștințele și soluțiile. De asemenea, acesta este un loc în care se nasc idei și de unde echipele noastre de dezvoltare pot obține un feedback valoros. Membrii comunității sunt utilizatori Bitdefender cu experiență, dornici să-și ajute colegii, în timpul liber. Cu contribuția lor impresionantă și prin eforturi voluntare sincere, am creat o bază de cunoștințe unde utilizatorii pot găsi răspunsuri și îndrumări, prin interacțiune.

Aici veți găsi conversații relevante cu persoane care utilizează Bitdefender pe dispozitivele lor. Comunitatea oferă o legătură reală cu membrii noștri și îți permite să te faci auzit. Este un loc unde ești încurajat să participi, având siguranța că opinia și aportul tău sunt respectate și prețuite. Pentru că activitatea noastră este apreciată, depunem eforturi pentru a asigura o asistență rapidă și precisă, la un nivel incomparabil, și ne dorim să-i aducem pe utilizatorii noștri mai aproape de noi. Cu acest scop în minte, am creat această comunitate.

Accesează pagina Comunității noastre de experți aici:

https://community.bitdefender.com/ro

6.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia conține toate informațiile de care ai nevoie despre cele mai noi amenințări cibernetice. Acesta este locul unde experții Bitdefender își împărtășesc sfaturi și recomandări despre cum să se protejeze împotriva hackerilor, breșelor de securitate a datelor, furtului de identitate și încercărilor de asumare a identității.

Accesează pagina Bitdefender Cyberpedia aici:

https://www.bitdefender.com/cyberpedia/.

6.3. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. Din 2001, BITDEFENDER și-a stabilit o reputație incontestabilă prin străduința constantă pentru o mai bună comunicare, astfel încât să depășească așteptările clienților și partenerilor noștri. Dacă aveți întrebări, nu ezitați să ne contactați direct prin intermediul nostru Centrul de asistență Bitdefender (page 49).

https://www.bitdefender.ro/consumer/support/

6.3.1. 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. Mergi la https://www.bitdefender.com/partners/partner-locator.html.
2. Selectează țara și orașul folosind opțiunile corespunzătoare.

GLOSAR

Cod de activare

Este o cheie unică care poate fi cumpărată de la retail și utilizată pentru a activa un anumit produs sau serviciu. Un cod de activare permite activarea unui abonament valabil pentru o anumită perioadă de timp și număr de dispozitive și poate fi folosit și pentru a prelungi un abonament cu condiția să fie generat pentru același produs sau serviciu.

ActiveX

ActiveX este un model de scriere a programelor, astfel încât alte programe și sistemul de operare să le poată apela. Tehnologia ActiveX este utilizată cu Microsoft Internet Explorer pentru a crea pagini web interactive care arată și se comportă ca niște programe de calculator, mai degrabă decât ca pagini statice. Cu ActiveX, utilizatorii pot pune sau răspunde la întrebări, pot folosi butoane și pot interacționa în alte moduri cu pagina web. Controalele ActiveX sunt adesea scrise folosind Visual Basic. Active X se remarcă prin lipsa completă a controalelor de securitate; experții în securitatea computerelor descurajează utilizarea acestuia pe internet.

Amenințare persistentă avansată

Amenințarea persistentă avansată (APT) exploatează vulnerabilitățile sistemelor pentru a fura informații importante pentru a le livra la sursă. Grupurile mari, cum ar fi organizațiile, companiile sau guvernele, sunt vizate de această amenințare. Obiectivul unei amenințări persistente avansate este de a rămâne nedetectat pentru o lungă perioadă de timp, putând monitoriza și aduna informații importante fără a deteriora mașinile vizate. Metoda folosită pentru a injecta amenințarea în rețea este printr-un fișier PDF sau un document Office care arată inofensiv, astfel încât fiecare utilizator să poată rula fișierele.

Adware

Adware-ul este adesea combinat cu o aplicație gazdă care este furnizată gratuit, atâta timp cât utilizatorul este de acord să accepte adware-ul. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord cu un acord de licență care precizează scopul aplicației, nu se comite nicio infracțiune. Cu toate acestea, reclamele pop-up pot deveni o supărare și, în unele cazuri, pot degrada performanța sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații

le colectează pot cauza probleme de confidențialitate pentru utilizatorii care nu cunoșteau pe deplin termenii din acordul de licență.

Arhiva

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.

Ușa din spate

O gaură în securitatea unui sistem lăsată în mod deliberat de proiectanți sau întreținători. Motivația pentru astfel de găuri nu este întotdeauna sinistră; unele sisteme de operare, de exemplu, ies din cutie cu conturi privilegiate destinate utilizării de către tehnicienii de service pe teren sau programatorii de întreținere ai furnizorului.

Sectorul de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (dimensiunea sectorului, dimensiunea clusterului și așa mai departe). Pentru discurile de pornire, sectorul de boot conține și un program care încarcă sistemul de operare.

Virus de pornire

O amenințare care infectează sectorul de pornire al unui disc fix sau al unei dischete. O încercare de pornire de pe o dischetă infectată cu un virus din sectorul de boot va face ca amenințarea să devină activă în memorie. De fiecare dată când porniți sistemul din acel moment, veți avea amenințarea activă în memorie.

botnet

Termenul „botnet” este compus din cuvintele „robot” și „rețea”. Rețelele bot sunt dispozitive conectate la internet infectate cu amenințări și pot fi folosite pentru a trimite e-mailuri spam, a fura date, a controla de la distanță dispozitive vulnerabile sau a răspândi programe spyware, ransomware și alte tipuri de amenințări. Obiectivul lor este de a infecta cât mai multe dispozitive conectate, precum PC-uri, servere, dispozitive mobile sau IoT aparținând marilor companii sau industrii.

Browser

Prescurtare pentru browser web, o aplicație software folosită pentru a localiza și afișa pagini web. Printre browserele populare se numără Microsoft Internet Explorer, Mozilla Firefox și Google Chrome. Acestea sunt browsere grafice, ceea ce înseamnă că pot afișa atât grafică, cât și text. În

plus, majoritatea browserelor moderne pot prezenta informații multimedia, inclusiv sunet și video, deși necesită plug-in-uri pentru unele formate.

Atac de forță brută

Atacul de ghicire a parolei folosit pentru a pătrunde într-un sistem computerizat prin introducerea de combinații posibile de parole, de cele mai multe ori începând cu parola cel mai ușor de ghicit.

Linie de comanda

Într-o interfață de linie de comandă, utilizatorul tastează comenzi în spațiul oferit direct pe ecran folosind limbajul de comandă.

Cookie-uri

În industria internetului, cookie-urile sunt descrise ca fișiere mici care conțin informații despre computere individuale care pot fi analizate și utilizate de agenții de publicitate pentru a urmări interesele și gusturile dvs. online. În acest domeniu, tehnologia cookie-urilor este încă în curs de dezvoltare și intenția este de a direcționa anunțurile direct către ceea ce ați spus că sunt interesele dvs. Este o sabie cu două tăișuri pentru mulți oameni, deoarece, pe de o parte, este eficientă și pertinentă, deoarece vedeți doar reclame despre ceea ce vă interesează. Pe de altă parte, implică de fapt „urmărirea” și „urmărirea” unde mergeți și pe ce dai click. De înțeles, există o dezbatere asupra confidențialității și mulți oameni se simt jigniți de ideea că sunt priviți ca un „număr SKU” (știți, codul de bare de pe spatele pachetelor care este scanat la linia de check-out de la băcănie) . Deși acest punct de vedere poate fi extrem, în unele cazuri este precis.

Hărțuirea cibernetică

Când colegii sau străinii comit acte abuzive împotriva copiilor intenționat pentru a-i răni fizic. Pentru a dăuna emoțional, agresorii trimit mesaje răutăcioase sau fotografii nemăgulitoare, făcând astfel victimele lor să se izoleze de ceilalți sau să se simtă frustrate.

Dicţionar Attack

Atacurile de ghicire a parolelor erau folosite pentru a pătrunde într-un sistem informatic prin introducerea unei combinații de cuvinte comune pentru a genera parole potențiale. Aceeași metodă este folosită pentru a ghici cheile de decriptare ale mesajelor sau documentelor criptate. Atacurile de dicționar reușesc, deoarece mulți oameni înclină să aleagă parole scurte și simple, care sunt ușor de ghicit.

Unitate disc

Este o mașină care citește și scrie date pe un disc. Un hard disk citește și scrie hard disk-uri. O unitate de dischetă accesează dischetele. Unitățile de disc pot fi fie interne (găzduite într-un computer), fie externe (găzduite într-o cutie separată care se conectează la computer).

Descarca

Pentru a copia date (de obicei un fișier întreg) de la o sursă principală pe un dispozitiv periferic. Termenul este adesea folosit pentru a descrie procesul de copiere a unui fișier dintr-un serviciu online pe propriul computer. Descărcarea se poate referi și la copierea unui fișier de pe un server de fișiere din rețea pe un computer din rețea.

E-mail

Poștă electronică. Un serviciu care trimite mesaje pe computere prin rețele locale sau globale.

Evenimente

O acțiune sau o apariție detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi clic pe un buton al mouse-ului sau apăsarea unei taste, sau apariții ale sistemului, cum ar fi epuizarea memoriei.

Exploatările

O modalitate de a profita de diferite erori sau vulnerabilități care sunt prezente într-un computer (software sau hardware). Astfel, hackerii pot obține controlul asupra computerelor sau rețelelor.

Fals pozitiv

Apare atunci când un scaner identifică un fișier ca fiind infectat, când de fapt nu este.

Extensie de nume de fișier

Porțiunea dintr-un nume de fișier, care urmează punctului final, care indică tipul de date stocate în fișier. Multe sisteme de operare folosesc extensii de nume de fișiere, de exemplu Unix, VMS și MS-DOS. Acestea sunt de obicei de la una la trei litere (unele sisteme de operare vechi triste nu acceptă mai mult de trei). Exemplele includ „c” pentru codul sursă C, „ps” pentru PostScript, „txt” pentru text arbitrar.

Euristică

O metodă bazată pe reguli de identificare a noilor amenințări. Această metodă de scanare nu se bazează pe baza de date cu informații despre amenințări specifice. Avantajul scanării euristice este că nu este păcălit de o nouă variantă a unei amenințări existente. Cu toate acestea, poate raporta ocazional cod suspect în programele normale, generând așa-numitul „fals pozitiv".

Borcan cu miere

Un sistem informatic momeală creat pentru a atrage hackerii să studieze modul în care acţionează și să identifice metodele eretice pe care le folosesc pentru a colecta informaţii despre sistem. Companiile și corporațiile sunt mai interesate de implementarea și utilizarea honeypot-urilor pentru a-și îmbunătăți starea generală de securitate.

IP

Internet Protocol - Un protocol rutabil din suita de protocoale TCP/IP care este responsabil pentru adresarea IP, rutarea și fragmentarea și reasamblarea pachetelor IP.

applet Java

Un program Java care este proiectat să ruleze numai pe o pagină web. Pentru a utiliza un applet pe o pagină web, trebuie să specificați numele applet-ului și dimensiunea (lungime și lățime, în pixeli) pe care le poate utiliza applet-ul. Când pagina web este accesată, browserul descarcă appletul de pe un server și îl rulează pe computerul utilizatorului (clientul). Appleturile diferă de aplicații prin faptul că sunt guvernate de un protocol de securitate strict.

De exemplu, chiar dacă aplicațiile rulează pe client, acestea nu pot citi sau scrie date pe computerul clientului. În plus, applet-urile sunt restricționate în continuare, astfel încât să poată citi și scrie numai date de pe același domeniu din care sunt servite.

Keylogger

Un keylogger este o aplicație care înregistrează orice tastați. Keylogger-urile nu sunt rău intenționate în natură. Ele pot fi folosite în scopuri legitime, cum ar fi monitorizarea angajaților sau a activității copiilor. Cu toate acestea, acestea sunt din ce în ce mai folosite de infractorii cibernetici în scopuri rău intenționate (de exemplu, pentru a colecta date private, cum ar fi datele de conectare și numerele de securitate socială).

Virus macro

Un tip de amenințare informatică care este codificată ca macrocomandă încorporată într-un document. Multe aplicații, cum ar fi Microsoft Word și Excel, acceptă limbaje macro puternice. Aceste aplicații vă permit să încorporați o macrocomandă într-un document și să executați macrocomandă de fiecare dată când documentul este deschis.

Client de mail

Un client de e-mail este o aplicație care vă permite să trimiteți și să primiți e-mail.

Memorie

Zone de stocare internă în computer. Termenul de memorie identifică stocarea de date care vine sub formă de cipuri, iar cuvântul stocare este folosit pentru memoria care există pe benzi sau discuri. Fiecare computer vine cu o anumită cantitate de memorie fizică, denumită de obicei memorie principală sau RAM.

Non-euristic

Această metodă de scanare se bazează pe baza de date cu informații despre amenințări specifice. Avantajul scanării non-euristice este că nu este păcălit de ceea ce ar putea părea a fi o amenințare și nu generează alarme false.

Prădători online

Persoane care caută să atragă minori sau adolescenți în conversații cu scopul de a-i implica în activități sexuale ilegale. Rețelele de socializare sunt locul ideal în care copiii vulnerabili pot fi vânați cu ușurință și seduși să comită activități sexuale, online sau față în față.

Programe pline

Un fișier într-un format de compresie. Multe sisteme de operare și aplicații conțin comenzi care vă permit să împachetați un fișier astfel încât să ocupe mai puțină memorie. De exemplu, să presupunem că aveți un fișier text care conține zece caractere spațiale consecutive. În mod normal, acest lucru ar necesita zece octeți de stocare.

Cu toate acestea, un program care împachetează fișiere ar înlocui caracterele de spațiu cu un caracter special din seria spațială, urmat de numărul de spații înlocuite. În acest caz, cele zece spații ar necesita doar doi octeți. Aceasta este doar o tehnică de ambalare - sunt multe altele.

Cale

Indicațiile exacte către un fișier de pe un computer. Aceste direcții sunt de obicei descrise prin intermediul sistemului ierarhic de evidență de sus în jos.

Ruta dintre oricare două puncte, cum ar fi canalul de comunicații între două computere.

Phishing

Acțiunea de a trimite un e-mail unui utilizator care pretinde în mod fals că este o întreprindere legitimă stabilită în încercarea de a înșela utilizatorul pentru a renunța la informații private care vor fi folosite pentru furtul de identitate. E-mailul îl direcționează pe utilizator să viziteze un site web unde i se cere să actualizeze informații personale, cum ar fi parolele și numerele de card de credit, de securitate socială și de cont bancar, pe care organizația legitimă le are deja. Totuși, site-ul web este fals și creat doar pentru a fura informațiile utilizatorului.

Foton

Photon este o tehnologie Bitdefender inovatoare, neitruzivă, proiectată pentru minimizarea impactului soluției tale de securitate asupra performanțelor. Prin monitorizarea în fundal a activității PC-ului tău, creează modele de utilizare care vor ajuta la optimizarea pornirii și a proceselor de scanare.

Virus polimorf

O amenințare care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, astfel de amenințări 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 endpoint către o conexiune logică. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Ransomware

Ransomware este un program periculos care încearcă să obțină bani de la utilizatori prin blocarea sistemelor vulnerabile. CryptoLocker, CryptoWall și

TeslaWall sunt doar câteva variante care vânează sistemele personale ale utilizatorilor.

Infecția se poate extinde prin accesarea mesajelor spam, descărcarea atașamentelor e-mail sau instalarea de aplicații, fără ca utilizator să afle ce se întâmplă pe sistemul său. Utilizatorii și companiile sunt vizate zilnic de către hackerii ransomware.

Fișier 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 instrumente 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 instrumente 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, conectări și jurnale. Acestea pot, de asemenea, să intercepteze date de la terminale, conexiuni la rețea sau dispozitive periferice, 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 amenințări sau prezența intrușilor în sistem. În combinație cu amenințările, 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 întreaga gamă a mesajelor electronice nesolicitate (junk). În general, acestea sunt cunoscute sub numele de mesaje 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 o amenințare de tip cal troian este legată de 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 de pornire

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.

Abonament

Contractul de cumpărare care acordă utilizatorului dreptul de a folosi un anumit produs sau serviciu pe un anumit număr de dispozitive și o anumită perioadă de timp. Un abonament expirat poate fi reînnoit automat folosind informațiile furnizate de utilizator la prima achiziție.

Zona de notificare

Introdusă odată cu apariția sistemului Windows 95, bara de sistem se află 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 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.

Amenințare

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 amenințărilor se pot și înmulți. Toate amenințările informatice sunt create de om. O simplă amenințare care poate realiza copii ale sale este relativ simplu de produs. Chiar și o asemenea amenințare este periculoasă întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. O amenințare și mai periculoasă este cea care este capabilă să se răspândească în rețea și poate să treacă de sistemele de securitate.

Actualizare informații despre amenințări

Modelul binar al unei amenințări, utilizat de către soluția de securitate pentru detectarea și eliminarea amenințării.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de programele malițioase și viermi, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cele mai mascate tipuri de amenințări de tip cal troian este un program care pretinde că elimină amenințările de pe calculatorul tău, însă, în loc de aceasta, introduce amenințări pe calculatorul tău.

Termenul provine de la o poveste din opera „Iliada” a lui Homer, în care grecii le 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. Rutinele de instalare a actualizărilor verifică dacă pe calculatorul tău există instalată o altă versiune mai veche; dacă nu, nu vei putea instala actualizarea.

Bitdefender dispune de o funcție proprie de actualizare care îți permite să verifici manual actualizările sau să permiți actualizarea automată a produsului.

Rețea privată virtuală (VPN)

Este o tehnologie care permite o conexiune directă temporară și criptată la o anumită rețea prin intermediul unei rețele mai puțin sigure. Astfel, trimiterea și primirea de date este sigură și criptată, dificil de interceptat de către curioși. O dovadă de securitate este autentificarea, care se poate efectua numai folosind un nume de utilizator și o parolă.

Vierme

Reprezintă un program care se auto-propagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.