GHIDUL UTILIZATORULUI

Bitdefender CONSUMER SOLUTIONS

Mobile Security for iOS

Bitdefender Mobile Security for iOS

Ghidul utilizatorului

Data publicării 02.10.2023

Aviz juridic

Bitdefender

Cuprins

Despre acest ghid 1
Scopul și publicul țintă 1
Cum să folosiți acest ghid 1
Convenții utilizate în acest ghid 1
Convenții tipografice 1
Atenționări 2
Comentarii 2
1. Ce este Bitdefender Mobile Security for iOS 4
2. Introducere 5
2.1. Cerințe dispozitiv 5
2.2. Instalare Bitdefender Mobile Security for iOS 5
2.3. Accesează contul tău Bitdefender 6
2.4. Panou de bord 7
3. Caracteristici și funcții 9
3.1. Scanare 9
3.2. Scam Alert 9
3.2.1. Cum se configurează Scam Alert 10
3.3. Protecție web 11
3.3.1. Alerte Bitdefender 12
3.4. VPN 13
3.4.1. Abonamente 15
3.5. Confidențialitate cont 16
4. Despre Bitdefender CENTRAL 18
4.1. Accesează Bitdefender Central 18
4.2. Autentificare în doi pași 19
4.2.1. Activați autentificarea de tip „two-factor” 19
4.3. Adăugarea dispozitivelor sigure 21
4.4. Dispozitivele mele 21
4.4.1. Adăugarea unui dispozitiv nou 21
4.4.2. Personalizează-ți dispozitivul 22
4.4.3. Acțiuni de la distanță 23
4.5. Activitate 24
4.6. Abonamentele mele 25
4.6.1. Verifică abonamentele disponibile 25
4.6.2. Activare abonament 25
4.6.3. Reînnoire abonament 26
4.7. Notificări 27
5. Întrebări frecvente 28
6. Obține ajutor 29

6.1. Solicitarea ajutorului 29
6.2. Resurse online 29
6.2.1. Centrul de asistență Bitdefender 29
6.2.2. Comunitatea de experți Bitdefender 30
6.2.3. Bitdefender Cyberpedia 30
6.3. Informații de contact 31
6.3.1. Distribuitori locali 31
Glosar 32

DESPRE ACEST GHID

Scopul și publicul țintă

Acest ghid este destinat tuturor utilizatorilor iOS care au ales Bitdefender Mobile Security for iOS 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 mobile Apple.

Vei afla cum să configurezi și să utilizezi Bitdefender Mobile Security for iOS 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 (pagina 5)

Fă cunoștință cu produsul Bitdefender Mobile Security for iOS și interfața sa pentru utilizatori.

Caracteristici și funcții (pagina 9)

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

Obține ajutor (pagina 29)

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 (pagina 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 FOR IOS

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?

Bitdefender Mobile Security for iOS îți permite:

- Cea mai eficientă protecție împotriva amenințărilor cu cel mai mic impact asupra bateriei
- Protejezi datele cu caracter personal: parolele, adresa și informațiile financiare
- Verifică ușor securitatea telefonului pentru a detecta și a remedia configurațiile greșite care l-ar putea expune la riscuri
- Eviți expunerea accidentală a datelor și utilizarea necorespunzătoare a tuturor aplicațiilor instalate
- Scanează-ți dispozitivul pentru a obține setări optime de securitate și confidențialitate
- Obții informații cu privire la activitatea ta online și istoricul incidentelor prevenite
- Verifică-ți conturile online pentru a detecta breșe de securitate a datelor sau scurgeri de date
- Criptezi traficul de pe internet cu VPN-ul inclus

Bitdefender Mobile Security for iOS este un produs gratuit care trebuie activat prin intermediul unui cont Bitdefender. Însă, anumite funcționalități importante ale Bitdefender, precum modulul Protecție web, pot fi accesate de către utilizatori doar prin plata unui abonament.

2. INTRODUCERE

2.1. Cerințe dispozitiv

Bitdefender Mobile Security for iOS este compatibil cu orice dispozitiv care rulează iOS 12 sau o versiune ulterioară a sistemului de operare și necesită o conexiune activă la internet pentru a fi activat și pentru a detecta dacă la nivelul conturilor tale online s-a produs o scurgere de date.

2.2. Instalare Bitdefender Mobile Security for iOS

- **Din Bitdefender Central**
  - Pe iOS
    1. Accesează **Bitdefender Central**.
    2. Selectați secțiunea **Dispozitivele mele**.
    3. Atinge **INSTALARE PROTECȚIE** și apoi **Protejează acest dispozitiv**.
    4. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, atinge butonul corespunzător.
    5. Vei fi redirecționat către aplicația **App Store**. În ecranul App Store, selectează opțiunea de instalare.
  - Pe Windows, macOS, Android
    1. Acces Bitdefender Central.
    2. Selectează **Dispozitivele mele** panou.
    3. Apasă pe **INSTALARE PROTECȚIE** și apoi pe **Protejează alte dispozitive**.
    4. Selectează deținătorul dispozitivului. Dacă dispozitivul aparține altei persoane, apasă pe butonul corespunzător.
    5. Apasă pe **TRIMITE LINK DE DESCĂRCARE**.
    6. 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.

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

- **Din App Store**
  Caută Bitdefender Mobile Security pentru iOS pentru a localiza și instala aplicația.

Când deschizi pentru prima dată aplicația, se va afișa o fereastră ce conține detalii despre caracteristicile produsului. Accesează opțiunea Înainte de a începe pentru a continua cu următoarea fereastră.

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 pentru iOS.

Selectează **Continuă** pentru a trece la fereastra următoare.

2.3. Accesează contul tău Bitdefender

Pentru a utiliza Bitdefender Mobile Security for iOS, 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.

Pentru a-ți asocia dispozitivul unui cont Bitdefender:

1. Introdu în câmpul corespunzător adresa de e-mail asociată contului tău Bitdefender, apoi selectează opțiunea **ÎNAINTE**. Dacă nu ai încă un cont Bitdefender și dorești să-ți creezi unul, accesează linkul corespunzător și apoi urmează instrucțiunile de pe ecran până când contul este activat.
   Pentru a te conecta cu un cont de Facebook, Google, Apple 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 for iOS.

> **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. Introdu parola și apoi selectează **AUTENTIFICARE**.

De aici poți accesa și Politica de confidențialitate a Bitdefender.

2.4. Panou de bord

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

Prima dată când accesezi aplicația, ți se va solicita să permiți Bitdefender să-ți trimită notificări. Selectează opțiunea **Permite** pentru a rămâne informat de fiecare dată când Bitdefender trebuie să-ți comunice ceva care are legătură cu aplicația ta. Pentru administrarea notificărilor Bitdefender, accesează Setări > Notificări > Mobile Security.

Pentru a avea acces la secțiunea de care ai nevoie, accesează pictograma corespunzătoare din partea de jos a ecranului.

Protecție web

Rămâi în siguranță în timp ce navighezi pe internet și oricând aplicațiile mai puțin securizate încearcă să acceseze domenii nesigure. pentru informații suplimentare, accesează Protecție web (pagina 11).

VPN

Protejează-ți confidențialitatea indiferent de rețeaua la care te conectezi menținând criptată conexiunea la internet. Pentru informații suplimentare, accesează VPN (pagina 13).

Confidențialitate cont

Află dacă au fost sau nu accesate neautorizat conturile tale de e-mail. Pentru mai multe informații, consultați capitolul Confidențialitate cont (pagina 16).

Pentru a vizualiza opțiuni suplimentare, accesează pictograma ••• de pe dispozitivul tău când te afli pe pagina principală a aplicației. Vor apărea următoarele opțiuni:

- **Restabilire achiziții** - din această secțiune poți restabili abonamentele anterioare achiziționate folosind contul tău iTunes.
- **Setări** - din această secțiune ai acces la:
  - **Setări VPN**
    - **Contract** - aici poți citi condițiile conform cărora poți utiliza serviciul Bitdefender VPN. Dacă selectezi **Nu mai sunt de acord**, nu vei putea utiliza Bitdefender VPN cel puțin până când nu apeși **Sunt de acord**.
    - **Avertisment rețea Wi-Fi deschisă** - poți activa sau dezactiva notificarea produsului care se afișează de fiecare dată când te conectezi la o rețea Wi-Fi nesecurizată.
      Scopul acestei notificări este de a te ajuta să-ți menții confidențialitatea și securitatea datelor tale folosind Bitdefender VPN.
  - **Setări Protecție web**
    - **Contract** - aici poți citi condițiile conform cărora poți utiliza serviciul Bitdefender Protecție web. Dacă selectezi **Nu mai sunt de acord**, nu vei putea utiliza Bitdefender VPN cel puțin până când nu apeși **Sunt de acord**.
    - **Activare notificări Protecție web** - Primești notificări care te anunță că serviciul Protecție web poate fi activat după finalizarea unei sesiuni VPN.
  - **Rapoarte produs**
- **Feedback** – de aici poți lansa clientul de e-mail implicit pentru a ne trimite feedback privind aplicația.
- **Detalii App** - de aici poți accesa informațiile privind versiunea instalată și Contractul de abonament, Politica de confidențialitate și conformitatea cu licențele open-source.

3. CARACTERISTICI ȘI FUNCȚII

3.1. Scanare

Cu ajutorul Bitdefender Mobile Security for iOS, îți poți scana dispozitivul pentru a identifica orice vulnerabilități în ceea ce privește securitatea și amenințări posibile de pe dispozitivul tău. Efectuarea scanării va verifica următoarele:

- **Versiunea sistemului de operare:** Se verifică versiunea iOS pentru cele mai recente actualizări.
- **Parola/Date biometrice:** verifică nivelul de securitate când vine vorba de accesarea dispozitivului tău.
- **Protecție web:** verifică starea modulului Protecție web
- **Confidențialitate cont:** verifică prezența conturilor monitorizate enumerate în modulul Confidențialitate cont.
- **Scanare Wi-Fi:** verifică nivelul de securitate al rețelei la care ești conectat.

Starea protecției este determinată după ce efectuezi o scanare manuală.

După ce efectuezi prima scanare, vei fi întâmpinat de recomandările Autopilotului Bitdefender. Acesta este consilierul tău de securitate, care îți oferă recomandări contextuale pe baza modului de utilizare și necesităților dispozitivului tău. Astfel, vei beneficia de tot ce îți poate oferi aplicația ta.

> **Notă**
> Atunci când accesezi prima dată aplicația, ți se va solicita să efectuezi o scanare.

3.2. Scam Alert

Funcția de Scam Alert disponibilă în Bitdefender Mobile Security pentru iOS protejează în mod proactiv utilizatorii Apple de escrocherii de tip phishing. Scam Alert pentru iOS include două straturi de protecție care monitorizează înșelăciunile livrate prin mesaje SMS/MMS și invitații din calendar:

- **Filtru de mesaje text (SMS, MMS)**
  Această caracteristică identifică și filtrează mesajele SMS și MMS nedorite.
  Un SMS/MMS rău intenționat (Short Message Service/Multimedia Messaging Service) se referă la un tip de mesaj trimis către dispozitive mobile cu intenții dăunătoare. Aceste mesaje sunt concepute pentru a exploata vulnerabilități, pentru a înșela destinatarii sau pentru a provoca daune dispozitivului, informațiilor personale sau securității țintei.

- **Calendar Invite Link Scanner**
  Această funcție detectează calendarele spam și evenimentele care conțin linkuri periculoase. Virusul calendarului este un tip de spam care afectează aplicația Calendar a iPhone-ului tău, care poate fi enervant și potențial periculoasă:

  - Primești invitații de calendar sau notificări de evenimente nedorite atunci când accepți din greșeală o invitație de calendar falsă trimisă la adresa ta de e-mail de către hackeri sau spammeri.
  - Când faceți clic pe linkul din invitație, vă abonați fără să știți la calendarul expeditorului, ceea ce îi permite acestuia să vă trimită mai multe evenimente spam.
  - Evenimentele de spam pot conține link-uri sau atașamente care ar putea să vă conducă către pagini de phishing sau alte amenințări cibernetice dacă le deschideți.

3.2.1. Cum se configurează Scam Alert

Pentru a activa Scam Alert, trebuie să acordați aplicației Bitdefender Mobile Security acces la notificările din calendar și la mesajele SMS:

Cum să activați filtrarea SMS:

Pentru ca Bitdefender să înceapă să filtreze mesajele, trebuie să activați manual opțiunea Filtrați expeditorii necunoscuți din setările aplicației Mesaje:

1. Deschide **Setări** aplicația pe iPhone sau iPad.
2. Derulați în jos și selectați **Mesaje** dinn listă.
3. Apasă pe **Necunoscut sau spam** secțiune.

4. Comutati **Filtrați expeditorii necunoscuți** pe poziția pornit.
5. Selectați **Securitate mobilă** în secțiunea Filtrare SMS și apoi alegeți **Permite**.

Bitdefender va putea acum să filtreze mesajele nedorite de pe iPhone/iPad.

> **Notă**
> Din cauza restricțiilor iOS, filtrarea SMS-urilor Bitdefender poate fi utilizată numai pentru mesajele SMS și MMS care provin de la persoane pe care nu le-ați salvat în contacte. Aceasta înseamnă că nu va filtra mesajele de la persoane aflate deja în lista de contacte sau mesajele iMessage de la nimeni.

Cum să activați scanarea calendarului:

1. Deschide aplicația **Bitdefender Mobile Security** instalată pe iPhone sau iPad.
2. Du-te la opțiunea **Scam Alert** din bara de navigare de jos și apăsați pe **Configurați acum**.
3. Atingeți **Continua**, apoi atingeți **Permite**.
4. Alege **OK** pentru a acorda Bitdefender acces la calendarul dvs. O scanare a calendarului va începe imediat.

3.3. Protecție web

Modulul Protecție web Bitdefender asigură o experiență sigură de navigare trimițându-ți alerte cu privire la paginile web potențial periculoase și încercările de accesare de către aplicațiile instalate mai puțin securizate a unor domenii nesigure.

Atunci când o adresă URL face trimitere la un site web cunoscut pentru conținutul său de tip phishing sau fraudulos sau la conținut periculos, cum ar fi spyware sau viruși, pagina web respectivă este blocată și se afișează o alertă. Același lucru se întâmplă atunci când aplicațiile instalate încearcă să acceseze domenii periculoase.

> **Important**
> Dacă te afli într-o zonă în care utilizarea unui serviciu VPN este restricționată prin lege, funcționalitatea Protecție web nu va fi disponibilă.

Pentru a activa Protecția web:

1. Atinge pictograma din partea de jos a ecranului.
2. Apasă **Sunt de acord**.
3. Activează butonul Protecție web.

> **Notă**
> Prima dată când activezi modulul Protecție web, este posibil să ți se solicite să permiți Bitdefender să creeze configurații VPN care să monitorizeze traficul de rețea. Selectează **Permite** pentru a continua. Dacă a fost setată o metodă de autentificare (prin amprentă sau cod PIN) pentru a-ți proteja smartphone-ul, trebuie să o folosești. Pentru a putea detecta accesul la domeniile nesigure, modulul Protecție web funcționează împreună cu serviciile VPN.

> **Important**
> Caracteristica Protecție web și serviciul VPN nu pot funcționa simultan. Atunci când una dintre acestea este activată, cealaltă (dacă este activă în acel moment) va fi dezactivată.

3.3.1. Alerte Bitdefender

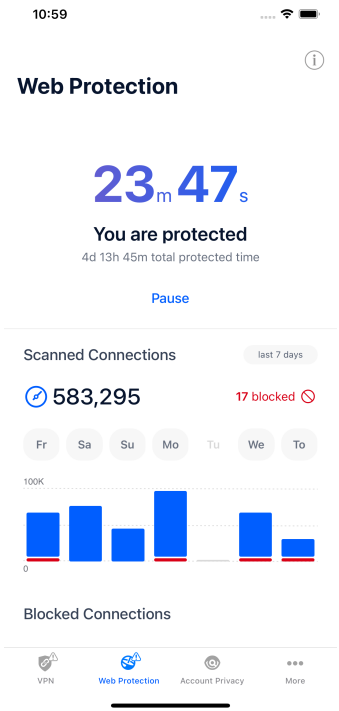
Ori de câte ori încerci să accesezi un site clasificat ca fiind nesigur, site-ul respectiv este blocat. Pentru a te informa despre acest eveniment, vei primi o notificare din partea Bitdefender în Centrul de notificări, precum și în browser. Pagina de avertizare conține informații precum adresa URL a site-ului și amenințarea detectată. Trebuie să decizi cum dorești să se procedeze în continuare.

De asemenea, vei primi o notificare în Centrul de notificări ori de câte ori o aplicație mai puțin sigură încearcă să acceseze domenii care nu sunt de încredere. Accesează notificarea respectivă pentru a fi redirecționat către fereastra în care poți decide cum dorești să procedezi în continuare.

Următoarele opțiuni sunt disponibile pentru ambele situații:

- Părăsește site-ul web respectiv selectând **REVENIRE LA O PAGINĂ SIGURĂ**.
- Accesează site-ul, în ciuda avertizării, selectând notificarea respectivă și apoi **Vreau să accesez pagina**.

Confirmă alegerea.



3.4. VPN

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

VPN acţionează ca tunel între dispozitivul tău şi reţeaua la care te conectezi, securizându-ţi conexiunea, criptându-ţi datele prin criptare de talie militară şi ascunzându-ţi adresa IP oriunde te-ai afla. Traficul tău este redirecţionat prin intermediul unui server separat, ceea ce face ca dispozitivul tău să fie imposibil de identificat de către ISP între multitudinea de alte dispozitive care folosesc serviciile noastre. Mai mult decât atât, în timp ce eşti conectat la internet prin intermediul Bitdefender Mobile Security for iOS, poţi accesa conţinut care în mod normal este restricţionat 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.

Activează Bitdefender VPN:

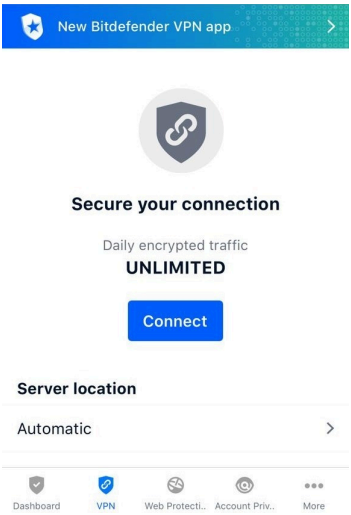
1. Apasă pe pictograma din partea de jos a ecranului.
2. Selectează **Conectare** de fiecare dată când dorești să fii protejat atunci când te conectezi la rețele wireless nesecurizate.
   Selectează **Deconectare** atunci când vrei să dezactivezi conexiunea.

> **Notă**
> Prima dată când activezi modulul VPN, ți se va solicita să permiți Bitdefender să creeze configurații VPN care să monitorizeze traficul de rețea. Selectează **Permite**, pentru a continua. Dacă a fost setată o metodă de autentificare (prin amprentă sau cod PIN) pentru a-ți proteja smartphone-ul, trebuie să o folosești.

Când VPN este activat, pictograma VPN apare pe bara de stare.

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, selectează Automat în interfața VPN și alege locația dorită. Pentru informații suplimentare privind abonamentele VPN, consultă Abonamente (pagina 15).



3.4.1. 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 face oricând upgrade la versiunea Bitdefender Premium VPN apăsând butonul **AActivare Premium VPN** disponibilă în fereastra VPN. Există două tipuri de abonamente disponibile: abonamente anuale și abonamente lunare.

Abonamentul Bitdefender Premium VPN este independent de abonamentul gratuit Bitdefender Mobile Security for iOS, ceea ce înseamnă că îl vei putea folosi pe toată durata de valabilitate. În cazul în care abonamentul Bitdefender Premium VPN expiră, vei reveni automat la planul gratuit.

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.

3.5. Confidențialitate cont

Funcția Confidențialitate cont Bitdefender detectează dacă s-au produs scurgeri de informații din conturile 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 privind cardurile de credit 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.

Pentru a verifica dacă un cont a fost accesat neautorizat, selectează opțiunea **Scanează pentru depistarea accesărilor neautorizate**.

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

1. Apasă pe pictograma din partea de jos a ecranului.
2. Atinge **Adăugare cont**.
3. Introdu adresa ta de e-mail în câmpul corespunzător și apoi selectează **Continuă**.
   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.
4. 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 și 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 căile de acces neautorizat ca fiind **Rezolvat(e)**. Pentru a face acest lucru:

1. Atinge ··· de lângă breșa pe care ai remediat-o.
2. Atinge **Marchează ca rezolvată**.

După ce toate căile de acces neautorizat sunt marcate ca fiind Rezolvate, contul nu va mai apărea ca fiind implicat într-o scurgere de informații, cel puțin până când nu se detectează o nouă scurgere de informații.

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 pentru iOS
  - Bitdefender Mobile Security for Android
  - Bitdefender Antivirus for Mac
  - Gama de produse Bitdefender Windows
- Administrează și reînnoiește abonamentele Bitdefender.
- Adaugă dispozitive noi la rețeaua ta și administrează-le oriunde te-ai afla.

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. Accesează: 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. Accesează 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. Selectează **ÎNCEPE UTILIZAREA**.
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. Confirmați alegerea dvs.

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 for iOS 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

Cum poate Bitdefender Mobile Security să mă protejeze împotriva virușilor și a amenințărilor cibernetice?

Bitdefender Mobile Security pentru iOS oferă protecție absolută împotriva tuturor atacurilor cibernetice și este conceput special pentru a-ți păstra datele sensibile departe de privirile indiscrete.

Vei obține o multitudine de caracteristici avansate de siguranță și confidențialitate pentru dispozitivele tale iPhone și iPad - plus multe funcții suplimentare, inclusiv VPN și Protecție Internet.

Bitdefender Mobile Security pentru iOS reacționează instantaneu la viruși și malware, fără a compromite performanța sistemului tău.

Ce tipuri de dispozitive și sisteme de operare acoperă Bitdefender Mobile Security pentru iOS?

Bitdefender Mobile Security pentru iOS îți va proteja telefoanele inteligente și tabletele care rulează cu sistem de operare iOS împotriva tuturor atacurilor cibernetice.

De ce am nevoie de Bitdefender Mobile Security pentru iOS pe sistemul de operare Apple OS?

Unele dintre cele mai importante date sunt stocate pe iPhone sau iPad - și trebuie să ai certitudinea că acestea sunt sigure în permanență. Bitdefender Mobile Security pentru iOS oferă o protecție absolută împotriva atacurilor cibernetice și are grijă de siguranța ta online și de informațiile tale personale, fără a interveni în activitățile tale de zi cu zi.

Primesc VPN odată cu abonamentul meu Bitdefender Mobile Security pentru iOS?

Bitdefender Mobile Security for iOS are integrată o versiune standard pentru Bitdefender VPN care include un volum generos de trafic (200 MB / zi, în total 6 GB lunar), gratuit.

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 (pagina 29).

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.

Dicționar 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 acționează şi să identifice metodele eretice pe care le folosesc pentru a colecta informații 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.