ANVÄNDARMANUAL

Bitdefender CONSUMER SOLUTIONS

Mobile Security for iOS

Bitdefender Mobile Security för iOS

Användarmanual

Publiceringsdatum 2023-10-02

Rättsligt meddelande

Bitdefender

Innehållsförteckning

OM DEN HÄR GUIDEN

Syfte och avsedd målgrupp

Den här guiden är avsedd för alla iOS-användare som har valt Bitdefender Mobile Security för iOS som en säkerhetslösning för sina mobila enheter. Informationen som presenteras i den här boken är inte bara lämplig för dem med teknisk bakgrund, den är tillgänglig för alla som kan arbeta under Apples mobila enheter.

Du kommer att få reda på hur du konfigurerar och använder Bitdefender Mobile Security för iOS för att skydda dig mot hot och andra skadliga applikationer. Du kommer att lära dig hur du blir bäst av Bitdefender.

Vi önskar dig en trevlig och användbar föreläsning.

Hur man använder den här guiden

Den här guiden är organiserad kring flera viktiga ämnen:

Komma igång (sida 4)

Kom igång med Bitdefender Mobile Security för iOS och dess användargränssnitt.

Funktioner och funktioner (sida 8)

Lär dig hur du använder Bitdefender Mobile Security för iOS för att skydda dig mot hot och skadliga applikationer genom att lära dig om dess funktioner och deras funktionalitet.

Få hjälp (sida 28)

Var man ska leta och var man kan be om hjälp om något oväntat dyker upp.

Konventioner som används i denna guide

Typografiska konventioner

Flera textstilar används i den här guiden för att förbättra läsbarheten. Deras aspekt och betydelse presenteras i tabellen nedan.

Utseende	Beskrivning
sample syntax	Syntaxexempel skrivs ut med monospaced tecken.
https://www.bitdefender.com	URL-länken pekar på någon extern plats, på http- eller ftp-servrar.
documentation@bitdefender.com	E-postadresser infogas i texten för kontaktinformation.
Om den här guiden (sida 1)	Detta är en intern länk till någon plats i dokumentet.
filename	Filer och kataloger skrivs ut med monospaced font.
alternativ	Alla produktalternativ skrivs ut med hjälp av **djärv** tecken.
nyckelord	Viktiga sökord eller fraser markeras med hjälp av **djärv** tecken.

Förmaningar

Förmaningarna är anteckningar i texten, grafiskt markerade, som uppmärksammar dig på ytterligare information relaterad till det aktuella stycket.

Notera

Anteckningen är bara en kort observation. Även om du kan utelämna det, kan anteckningarna ge värdefull information, som specifik funktion eller en länk till något relaterat ämne.

Viktig

Detta kräver din uppmärksamhet och rekommenderas inte att hoppa över det. Vanligtvis ger den icke-kritisk men betydande information.

Varning

Detta är viktig information som du bör behandla med ökad försiktighet. Inget dåligt kommer att hända om du följer anvisningarna. Du bör läsa och förstå den, för den beskriver något extremt riskabelt.

Begäran om kommentarer

Vi inbjuder dig att hjälpa oss att förbättra boken. Vi har testat och verifierat all information efter bästa förmåga. Skriv för att berätta för oss om eventuella brister du hittar i den här boken eller hur du tror att den kan förbättras, för att hjälpa oss att förse dig med bästa möjliga dokumentation.

Meddela oss genom att skicka ett mejl till documentation@bitdefender.com. Skriv alla dina dokumentationsrelaterade e-postmeddelanden på engelska så att vi kan behandla dem effektivt.

1. VAD ÄR BITDEFENDER MOBILE SECURITY FÖR IOS

Onlineaktiviteter som att betala räkningar, göra semesterbokningar eller köpa varor och tjänster är bekväma och problemfria. Men eftersom många aktiviteter har utvecklats på internet, kommer dessa med höga risker och, om säkerhetsdetaljer ignoreras, kan personuppgifter hackas. Och vad är viktigare än att skydda data som lagras på onlinekonton och på den personliga smartphonen?

Bitdefender Mobile Security för iOS låter dig:

- Få det mest kraftfulla skyddet mot hot med minsta möjliga påverkan på batteriet
- Skydda dina personuppgifter: lösenord, adress, social och ekonomisk information
- Kontrollera enkelt telefonens säkerhet för att upptäcka och åtgärda felkonfigurationer som kan avslöja den
- Undvik oavsiktlig dataexponering och missbruk för alla installerade appar
- Skanna din enhet för att uppnå optimala säkerhets- och sekretessinställningar
- Få användningsinsikter om din onlineaktivitet och historik över förhindrade incidenter
- Kontrollera dina onlinekonton mot dataintrång eller dataläckor
- Kryptera internettrafik med det medföljande VPN

Bitdefender Mobile Security för iOS levereras gratis och kräver aktivering med en Bitdefender-konto. Vissa viktiga funktioner i Bitdefender, såsom vår "Web Protection"-modul, kräver dock en betald prenumeration för att vara tillgängliga för våra användare.

2. KOMMA IGÅNG

2.1. Enhetskrav

Bitdefender Mobile Security för iOS fungerar på alla enheter som kör iOS 12 eller senare versioner av operativsystemet och behöver en aktiv internetanslutning för att aktiveras och för att upptäcka om något dataläckage har inträffat i dina onlinekonton.

2.2. Installera Bitdefender Mobile Security för iOS

- **Från Bitdefender Central**
  - På iOS
    1. Tillgång Bitdefender Central.
    2. Välj **Mina enheter** panel.
    3. Knacka **INSTALLATIONSSKYDD**och tryck sedan på **Skydda den här enheten**.
    4. Välj enhetens ägare. Om enheten tillhör någon annan trycker du på motsvarande knapp.
    5. Du omdirigeras till **App Store** app. På App Store-skärmen trycker du på installationsalternativet.
  - På Windows, macOS, Android
    1. Tillgång Bitdefender Central.
    2. Välj **Mina enheter** panel.
    3. Tryck **INSTALLATIONSSKYDD**, och tryck sedan på **Skydda andra enheter**.
    4. Välj enhetens ägare. Om enheten tillhör någon annan, tryck på motsvarande knapp.
    5. Tryck **SKICKA NEDLADDNINGSLÄNK**.
    6. Skriv en e-postadress i motsvarande fält och tryck på **SKICKA EPOST**. Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.

7. På enheten du vill installera Bitdefender kontrollera e-postkontot som du skrev in och tryck sedan på motsvarande nedladdningsknapp.

- **Från App Store**
  Sök efter Bitdefender Mobile Security för iOS för att hitta och installera appen.

Ett introduktionsfönster med information om produktens funktioner visas första gången du öppnar appen. Tryck på Kom igång för att fortsätta till nästa fönster.

Innan du går igenom valideringsstegen måste du godkänna prenumerationsavtalet. Ta dig tid att läsa prenumerationsavtalet eftersom det innehåller villkoren under vilka du får använda Bitdefender Mobile Security för iOS.

Knacka **Fortsätta** för att gå vidare till nästa fönster.

2.3. Logga in på ditt Bitdefender-konto

För att använda Bitdefender Mobile Security för iOS måste du länka din enhet till ett Bitdefender-, Facebook-, Google-, Apple- eller Microsoft-konto genom att logga in på kontot från appen. Första gången du öppnar appen uppmanas du att logga in på ett konto.

Så här länkar du din enhet till ett Bitdefender-konto:

1. Skriv in e-postadressen för ditt Bitdefender-konto i motsvarande fält och tryck sedan på **NÄSTA**. Om du inte har ett Bitdefender-konto och vill skapa ett, välj motsvarande länk och följ sedan instruktionerna på skärmen tills kontot är aktiverat.
   För att logga in med ett Facebook-, Google-, Apple- eller Microsoft-konto, tryck på tjänsten du vill använda från **Eller logga in** med område. Du omdirigeras till inloggningssidan för den valda tjänsten. Följ instruktionerna för att länka ditt konto till Bitdefender Mobile Security för iOS.

> **Notera**
> Bitdefender får inte tillgång till någon konfidentiell information som lösenordet för kontot du använder för att logga in eller personlig information om dina vänner och kontakter.

2. Skriv ditt lösenord och tryck sedan på **LOGGA IN**.

Härifrån kan du också komma åt Bitdefender sekretesspolicy.

2.4. instrumentbräda

Tryck på Bitdefender Mobile Security för iOS-ikonen i enhetens applåda för att öppna applikationsgränssnittet.

Första gången du öppnar appen uppmanas du att tillåta Bitdefender att skicka meddelanden till dig. Knacka **Tillåta** att hålla sig informerad varje gång Bitdefender måste kommunicera dig något som är relevant för din app. För att hantera Bitdefender-aviseringar, gå till Inställningar > Meddelanden > Mobilsäkerhet.

För att få tillgång till avsnittet du behöver, tryck på motsvarande ikon längst ned på skärmen.

Nätskydd

Var säker medan du surfar på webben och när mindre säkra appar försöker komma åt opålitliga domäner. För mer information, se Nätskydd (sida 10).

VPN

Behåll din integritet oavsett vilket nätverk du är ansluten till genom att hålla din internetkommunikation krypterad. För mer information, se VPN (sida 12).

Kontosekretess

Ta reda på om dina e-postkonton har läckt eller inte. För mer information, se Kontosekretess (sida 15).

För att se ytterligare alternativ, tryck på ••• ikonen på din enhet när du är på programmets startskärm. Följande alternativ visas:

- **Återställa köp** - härifrån kan du återställa de tidigare prenumerationer du har köpt via ditt iTunes-konto.
- **inställningar** - härifrån har du tillgång till:
  - **VPN-inställningar**
    - **Avtal** - du kan läsa villkoren under vilka du använder Bitdefender VPN-tjänsten. Om du trycker på **Jag håller inte**

med längre, kommer du inte att kunna använda Bitdefender VPN åtminstone förrän du trycker **Jag håller med**.

- **Öppna Wi-Fi-varning** - du kan aktivera eller inaktivera produktaviseringen som visas varje gång du ansluter till ett osäkrat Wi-Fi-nätverk.
  Syftet med detta meddelande är att hjälpa dig att hålla dina data privata och säkra genom att använda Bitdefender VPN.

- **Webbskyddsinställningar**
  - **Avtal** - du kan läsa villkoren under vilka du använder tjänsten Bitdefender Web Protection. Om du trycker på **Jag håller inte med längre**, kommer du inte att kunna använda Bitdefender VPN åtminstone förrän du trycker **Jag håller med**.
  - **Aktivera webbskyddsmeddelande** - Meddelar dig att webbskydd kan aktiveras efter avslutad VPN-session.
- **Produktrapporter**

- **Respons** - härifrån kan du starta standarde-postklienten för att skicka oss din feedback om appen.
- **App info** - härifrån har du tillgång till information om den installerade versionen och till prenumerationsavtal, integritetspolicy och överensstämmelse med öppen källkod.

3. FUNKTIONER OCH FUNKTIONER

3.1. Skanna

Bitdefender Mobile Security för iOS låter dig skanna din enhet efter eventuella säkerhetsbrister och potentiella hot på din enhet. Att köra skanningen kommer att söka efter:

- **OS-version:** Kontrollerar din iOS-version för de senaste uppdateringarna.
- **Lösenord/biometri:** Kontrollera säkerhetsnivån när det gäller åtkomst till din enhet.
- **Nätskydd:** Kontrollerar webbskyddsmodulens tillstånd
- **Kontosekretess:** Kontrollerar om det finns övervakade konton som anges i modulen Kontosekretess.
- **Skanna Wi-Fi:** Söker efter säkerhetsstatus för det för närvarande anslutna nätverket.

Skyddsstatusen bestäms efter att du kört en manuell skanning.

Efter att ha kört den första skanningen kommer du att mötas av Bitdefenders Autopilotrekommendationer. Det här är din personliga säkerhetsrådgivare som ger kontextuella rekommendationer baserat på din enhetsanvändning och behov. På så sätt kan du dra nytta av allt som din app har att erbjuda.

> **Notera**
> När du först går in i appen blir du ombedd att köra en skanning.

3.2. Scam Alert

Scam Alert-funktionen som är tillgänglig i Bitdefender Mobile Security för iOS skyddar proaktivt Apple-användare från nätfiske. Scam Alert för iOS inkluderar två lager av skydd som övervakar bedrägerier som levereras via SMS/MMS-meddelanden och kalenderinbjudningar:

- **Textmeddelandefilter (SMS, MMS)**
  Den här funktionen identifierar och filtrerar oönskade SMS- och MMS-meddelanden.

Ett skadligt SMS/MMS (Short Message Service/Multimedia Messaging Service) hänvisar till en typ av meddelande som skickas till mobila enheter med skadlig avsikt. Dessa meddelanden är utformade för att utnyttja sårbarheter, lura mottagare eller orsaka skada på målets enhet, personliga information eller säkerhet.

- **Calendar Invite Link Scanner**
  Den här funktionen upptäcker skräppostkalendrar och händelser som innehåller farliga länkar. Kalenderviruset är en typ av spam som påverkar kalenderappen på din iPhone, vilket kan vara irriterande och potentiellt farligt:
  - Du får oönskade kalenderinbjudningar eller händelseaviseringar när du av misstag accepterar en falsk kalenderinbjudan som skickas till din e-postadress av hackare eller spammare.
  - När du klickar på länken i inbjudan prenumererar du omedvetet på avsändarens kalender, vilket gör att de kan skicka fler spamhändelser till dig.
  - Spamhändelserna kan innehålla länkar eller bilagor som kan leda dig till nätfiskesidor eller andra cyberhot om du öppnar dem.

3.2.1. Hur man ställer in Scam Alert

För att aktivera Scam Alert måste du ge Bitdefender Mobile Security-appen åtkomst till kalenderaviseringar och SMS-meddelanden:

Så här aktiverar du SMS-filtrering:

För att Bitdefender ska börja filtrera meddelanden måste du manuellt aktivera alternativet Filtrera okända avsändare i inställningarna för appen Meddelanden:

1. Öppna **inställningar** app på din iPhone eller iPad.
2. Rulla ned och välj **Meddelanden** i listan.
3. Tryck på **Okänd & Spam** sektion.
4. Växla **Filtrera okända avsändare** till på-läget.
5. Välj **Mobil säkerhet** i avsnittet SMS-filtrering och välj sedan **Gör det möjligt**.

Bitdefender kommer nu att kunna filtrera skräpmeddelanden på din iPhone/iPad.

Notera

På grund av iOS-begränsningar kan Bitdefender SMS-filtrering endast användas för SMS- och MMS-meddelanden som kommer från personer som du inte har sparat i dina kontakter. Det betyder att det inte kommer att filtrera meddelanden från personer som redan finns i din kontaktlista eller iMessage-meddelanden från någon.

Så här aktiverar du kalenderskanning:

1. Öppna **Bitdefender Mobile Security** app installerad på din iPhone eller iPad.
2. Gå till **Scam Alert** alternativet i det nedre navigeringsfältet och tryck på **Ställ in nu**.
3. Knacka **Fortsätta** och tryck sedan på **Gör det möjligt**.
4. Välja **OK** för att ge Bitdefender åtkomst till din kalender. En kalenderskanning påbörjas omedelbart.

3.3. Nätskydd

Bitdefender Web Protection säkerställer en säker surfupplevelse genom att varna dig om potentiella skadliga webbsidor och när mindre säkra installerade appar försöker få åtkomst till opålitliga domäner.

När en URL pekar på en känd nätfiske eller bedräglig webbplats, eller till skadligt innehåll som spionprogram eller virus, blockeras webbsidan och en varning visas. Samma sak händer när installerade appar försöker komma åt skadliga domäner.

Viktig

Om du befinner dig i ett område där användningen av en VPN-tjänst är begränsad enligt lag, kommer funktionaliteten för webbskydd inte att vara tillgänglig.

Så här aktiverar du webbskydd:

1. Tryck på ikonen längst ned på skärmen.
2. Knacka **Jag håller med**.
3. Aktivera webbskyddsbrytaren.

Notera

Första gången du aktiverar webbskydd kan du bli ombedd att tillåta Bitdefender att ställa in VPN-konfigurationer som övervakar nätverkstrafik. Knacka **Tillåta**, att fortsätta. Om en autentiseringsmetod (fingeravtryck eller PIN-kod) har ställts in för att skydda din smartphone måste du använda den. För att kunna upptäcka åtkomst till opålitliga domäner arbetar Web Protection tillsammans med VPN-tjänsterna.

Viktig

Webbskyddsfunktionen och VPN kan inte fungera samtidigt. Närhelst en av dem är aktiverad, kommer den andra (om den är aktiv vid den tidpunkten) att inaktiveras.

3.3.1. Bitdefender-varningar

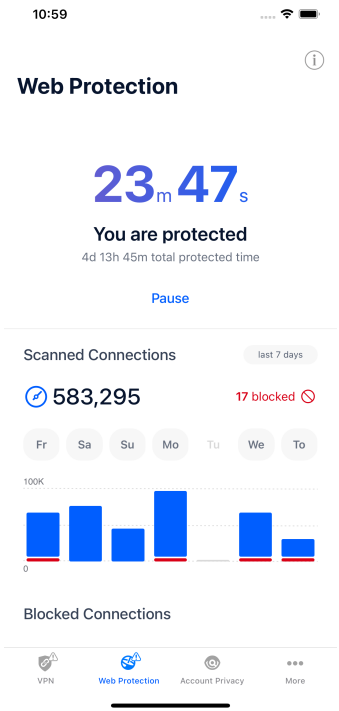
När du försöker besöka en webbplats som klassificeras som osäker blockeras webbplatsen. För att göra dig medveten om händelsen meddelas du av Bitdefender i meddelandecentret och i din webbläsare. Varningssidan innehåller information som webbadressen och det upptäckta hotet. Du måste bestämma dig för vad du ska göra härnäst.

Du får också ett meddelande i meddelandecentret när en mindre säker app försöker få åtkomst till opålitliga domäner. Tryck på det visade meddelandet för att omdirigeras till fönstret där du kan bestämma vad du ska göra härnäst.

Följande alternativ är tillgängliga för båda fallen:

- Navigera bort från webbplatsen genom att trycka på **TA MIG TILLBAKA TILL SÄKERHET**.
- Fortsätt till webbplatsen, trots varningen, genom att trycka på det visade meddelandet och sedan **Jag vill komma åt sidan**.

Bekräfta ditt val.



3.4. VPN

Med Bitdefender VPN kan du hålla din data privat varje gång du ansluter till osäkra trådlösa nätverk när du är på flygplatser, gallerior, kaféer eller hotell. På så sätt kan olyckliga situationer som stöld av personlig data eller försök att göra din enhets IP-adress tillgänglig för hackare undvikas.

VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter för att säkra din anslutning, kryptera data med kryptering av militär kvalitet och dölja din IP-adress var du än är. Din trafik omdirigeras via en separat server; vilket gör din enhet omöjlig att identifieras av din internetleverantör, genom de otaliga andra enheter som använder våra tjänster. Dessutom, medan du är ansluten till internet via Bitdefender Mobile Security for iOS, kan du komma åt innehåll som normalt är begränsat i specifika områden.

> **Notera**
> Vissa länder utövar internetcensur och därför har användningen av VPN på deras territorium förbjudits enligt lag. För att undvika juridiska konsekvenser kan ett varningsmeddelande visas när du försöker använda Bitdefender VPN-appen för första gången. Genom att fortsätta använda appen bekräftar du att du är medveten om tillämpliga landsbestämmelser och de risker som du kan utsättas för.

Så här aktiverar du Bitdefender VPN:

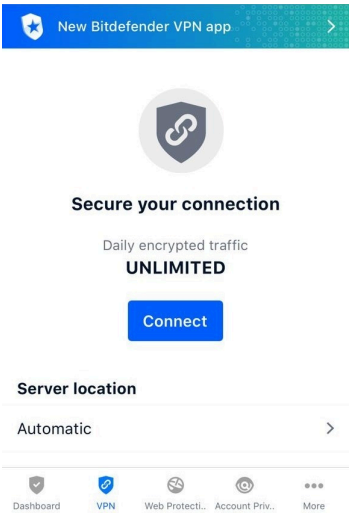
1. Tryck på ikonen längst ned på skärmen.
2. Knacka **Ansluta** varje gång du vill vara skyddad medan du är ansluten till osäkra trådlösa nätverk.
   Knacka **Koppla ifrån** när du vill inaktivera anslutningen.

> **Notera**
> Första gången du slår på VPN uppmanas du att tillåta Bitdefender att ställa in VPN-konfigurationer som övervakar nätverkstrafik. Knacka **Tillåta**, att fortsätta. Om en autentiseringsmetod (fingeravtryck eller PIN-kod) har ställts in för att skydda din smartphone måste du använda den.

De VPN ikonen visas i statusfältet när VPN är aktivt.

För att spara batteri, rekommenderar vi att du stänger av VPN när du inte behöver det.

Om du har ett premiumabonnemang och vill ansluta till en server som du vill, tryck på Automatisk i VPN-gränssnittet och välj sedan den plats du vill ha. Mer information om VPN-prenumerationer finns i Prenumerationer (sida 14).



3.4.1. Prenumerationer

Bitdefender VPN erbjuder gratis en daglig trafikkvot på 200 MB per enhet för att säkra din anslutning varje gång du behöver, och ansluter dig automatiskt till den optimala serverplatsen.

För att få obegränsad trafik och obegränsad tillgång till innehåll över hela världen genom att välja en serverplats efter din vilja, uppgradera till premiumversionen.

Du kan uppgradera till Bitdefender Premium VPN-version när som helst genom att trycka på **Aktivera Premium VPN** knappen tillgänglig i VPN-fönstret. Det finns två typer av prenumerationer att välja mellan: års- och månadsabonnemang.

Bitdefender Premium VPN-prenumeration är oberoende av Bitdefender Mobile Security för iOS gratisabonnemang, vilket innebär att du kommer att kunna använda den under hela dess tillgänglighet. Om Bitdefender Premium VPN-prenumeration går ut, kommer du automatiskt att återgå till gratisplanen.

Bitdefender VPN är en plattformsoberoende produkt, tillgänglig i Bitdefender-produkter som är kompatibla med Windows, macOS, Android och iOS. När du uppgraderar till premiumplanen kommer du att kunna använda ditt abonnemang på alla produkter, förutsatt att du loggar in med samma Bitdefender-konto.

Notera

Bitdefender VPN fungerar också som en fristående applikation på alla operativsystem som stöds, nämligen Windows, macOS, Android och iOS.

3.5. Kontosekretess

Bitdefender Account Privacy upptäcker om något dataläckage har inträffat på de konton du använder för att göra onlinebetalningar, handla eller logga in på olika appar eller webbplatser. De data som kan lagras på ett konto kan vara lösenord, kreditkortsinformation eller bankkontoinformation, och om den inte är ordentligt säkrad kan identitetsstöld eller intrång i integriteten förekomma.

Sekretessstatusen för ett konto visas direkt efter validering.

För att kontrollera om något av kontona har läckt, tryck på **Sök efter läckor**.

Så här börjar du hålla personlig information säker:

1. Tryck på ikonen längst ned på skärmen.
2. Knacka **Lägg till konto**.
3. Skriv din e-postadress i motsvarande fält och tryck sedan på **Nästa**.
   Bitdefender måste validera detta konto innan privat information visas. Därför skickas ett e-postmeddelande med en valideringskod till den angivna e-postadressen.
4. Kontrollera din inkorg och skriv sedan den mottagna koden i **Kontosekretess** område av din app. Om du inte kan hitta valideringse-postmeddelandet i mappen Inkorg, kontrollera även skräppostmappen.
   Sekretessstatusen för det validerade kontot visas.

Om läckor upptäcks på något av dina konton rekommenderar vi att du ändrar lösenordet så snart som möjligt. För att skapa ett starkt och säkert lösenord, ta hänsyn till dessa tips:

- Gör den minst åtta tecken lång.
- Inkludera gemener och versaler.
- Lägg till minst en siffra eller symbol, som #, @, % eller !.

När du väl har säkrat ett konto som var en del av ett integritetsintrång kan du bekräfta ändringarna genom att markera de identifierade läckorna som **Löst**. Att göra detta:

1. Knacka ··· bredvid intrånget du löste.
2. Knacka **Markera som löst**.

När alla upptäckta läckor är markerade som Lösta kommer kontot inte längre att visas som läckt, åtminstone tills ett nytt läckage upptäcks.

4. OM BITDEFENDER CENTRAL

Bitdefender Central är plattformen där du har tillgång till produktens onlinefunktioner och tjänster och kan utföra viktiga uppgifter på distans på enheter som Bitdefender är installerat på. Du kan logga in på ditt Bitdefender-konto från vilken dator eller mobil enhet som helst som är ansluten till internet genom att gå till https://central.bitdefender.com, eller direkt från Bitdefender Central-appen på Android- och iOS-enheter.

Så här installerar du Bitdefender Central-appen på dina enheter:

- **På Android** - sök Bitdefender Central på Google Play och ladda sedan ner och installera appen. Följ de nödvändiga stegen för att slutföra installationen.
- **På iOS** - sök Bitdefender Central på App Store och ladda sedan ner och installera appen. Följ de nödvändiga stegen för att slutföra installationen.

När du har loggat in kan du börja göra följande:

- Ladda ner och installera Bitdefender på Windows, macOS, iOS och Android operativsystem. Produkterna som är tillgängliga för nedladdning är:
  - Bitdefender Mobile Security för iOS
  - Bitdefender Mobile Security för Android
  - Bitdefender Antivirus för Mac
  - Bitdefender Windows produktlinje
- Hantera och förnya dina Bitdefender-prenumerationer.
- Lägg till nya enheter i ditt nätverk och hantera dem var du än är.

4.1. Åtkomst till Bitdefender Central

Det finns två sätt att komma åt Bitdefender Central

- Från din webbläsare:
  1. Öppna en webbläsare på valfri enhet med internetåtkomst.
  2. Gå till: https://central.bitdefender.com.

3. Logga in på ditt konto med din e-postadress och ditt lösenord.

❍ Från din Android- eller iOS-enhet:
Öppna Bitdefender Central-appen som du har installerat.

> **Notera**
> I detta material har vi tagit med alternativen som du kan hitta på webbgränssnittet.

4.2. 2-faktorsautentisering

Metoden för 2-faktorautentisering lägger till ett extra säkerhetslager till ditt Bitdefender-konto genom att kräva en autentiseringskod utöver dina inloggningsuppgifter. På så sätt kommer du att förhindra kontoövertagande och hålla borta typer av cyberattacker, såsom keyloggers, brute-force eller ordbokattacker.

4.2.1. Aktiverar 2-faktorsautentisering

Genom att aktivera 2-faktorsautentisering kommer du att göra ditt Bitdefender-konto mycket säkrare. Din identitet kommer att verifieras varje gång du loggar in från olika enheter, antingen för att installera en av Bitdefender-produkterna, kontrollera statusen för din prenumeration eller köra uppgifter på distans på dina enheter.

Så här aktiverar du tvåfaktorsautentisering:

1. Tillgång Bitdefender Central.
2. Tryck på ikonen i den övre högra sidan av skärmen.
3. Knacka **Bitdefender-konto** i bildmenyn.
4. Välj **Lösenord och säkerhet** flik.
5. Knacka **KOMMA IGÅNG**.
Välj en av följande metoder:

❍ **Autentiseringsapp** - använd en autentiseringsapp för att generera en kod varje gång du vill logga in på ditt Bitdefender-konto.
Om du vill använda en autentiseringsapp, men du är osäker på vad du ska välja, finns en lista med de autentiseringsappar som vi rekommenderar.

a. Knacka **ANVÄND AUTENTICATOR-APPEN** att börja.

b. Om du vill logga in på en Android- eller iOS-baserad enhet använder du din enhet för att skanna QR-koden.
   För att logga in på en bärbar dator eller dator kan du lägga till den visade koden manuellt.
   Knacka **FORTSÄTTA**.

c. Infoga koden från appen, eller den som visades i föregående steg och tryck sedan på **AKTIVERA**.

- **E-post** - varje gång du loggar in på ditt Bitdefender-konto kommer en verifieringskod att skickas till din e-postinkorg. Kontrollera mejlet och använd sedan koden du fick.

  a. Knacka **ANVÄND E-POST** att börja.

  b. Kontrollera din e-post och skriv in den medföljande koden.
     Observera att du har fem minuter på dig att kontrollera ditt e-postkonto och skriva in den genererade koden. Om tiden går ut måste du generera en ny kod genom att följa samma steg.

  c. Knacka **AKTIVERA**.

  d. Du får tio aktiveringskoder. Du kan antingen kopiera, ladda ner eller skriva ut listan och använda den om du tappar din e-postadress eller inte kommer att kunna logga in. Varje kod kan bara användas en gång.

  e. Knacka **GJORT**.

Om du vill sluta använda tvåfaktorsautentisering:

1. Knacka **STÄNG AV 2-FAKTORS AUTENTISERING**.
2. Kontrollera din app eller e-postkonto och skriv in koden du har fått.
   Om du har valt att ta emot autentiseringskoden via e-post har du fem minuter på dig att kontrollera ditt e-postkonto och skriva in den genererade koden. Om tiden går ut måste du generera en ny kod genom att följa samma steg.
3. Bekräfta ditt val.

4.3. Lägger till betrodda enheter

För att vara säker på att bara du kan komma åt ditt Bitdefender-konto kan vi behöva en säkerhetskod först. Om du vill hoppa över det här

steget varje gång du ansluter från samma enhet rekommenderar vi att du nominerar den som en betrodd enhet.

Så här lägger du till enheter som betrodda enheter:

1. Tillgång Bitdefender Central.
2. Tryck på ikonen i den övre högra sidan av skärmen.
3. Knacka **Bitdefender-konto** i bildmenyn.
4. Välj **Lösenord och säkerhet** flik.
5. Knacka **Betrodda enheter**.
6. Listan med enheterna som Bitdefender är installerade på visas. Tryck på önskad enhet.

Du kan lägga till så många enheter du vill, förutsatt att de har Bitdefender installerat och ditt abonnemang är giltigt.

4.4. Mina enheter

De **Mina enheter** område i ditt Bitdefender-konto ger dig möjlighet att installera, hantera och vidta fjärråtgärder på din Bitdefender-produkt på vilken enhet som helst, förutsatt att den är påslagen och ansluten till internet. Enhetskorten visar enhetens namn, skyddsstatus och om det finns säkerhetsrisker som påverkar skyddet av dina enheter.

4.4.1. Lägger till en ny enhet

Om ditt abonnemang omfattar mer än en enhet kan du lägga till en ny enhet och installera din Bitdefender Mobile Security for iOS på den, enligt följande:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panelen och tryck sedan på **INSTALLATIONSSKYDD**.
3. Välj ett av de två tillgängliga alternativen:
   - **Skydda den här enheten**
     Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan trycker du på motsvarande knapp.
   - **Skydda andra enheter**

Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan trycker du på motsvarande knapp.

Knacka **SKICKA NEDLADDNINGSLÄNK**. Skriv en e-postadress i motsvarande fält och tryck på **SKICKA EPOST**. Observera att den genererade nedladdningslänken endast är giltig under de kommande 24 timmarna. Om länken går ut måste du skapa en ny genom att följa samma steg.

På enheten du vill installera din Bitdefender-produkt, kontrollera e-postkontot som du skrev in och tryck sedan på motsvarande nedladdningsknapp.

4. Vänta tills nedladdningen är klar och kör sedan installationsprogrammet.

4.4.2. Anpassa din enhet

För att enkelt identifiera dina enheter kan du anpassa enhetens namn:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. Tryck på önskat enhetskort och sedan på ⋮ ikonen i det övre högra hörnet av skärmen.
4. Välj **inställningar**.
5. Skriv in ett nytt namn i **Enhetsnamn** fältet och tryck sedan på **SPARA**.

Du kan skapa och tilldela en ägare till var och en av dina enheter för bättre hantering:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. Tryck på önskat enhetskort och sedan på ⋮ ikonen i det övre högra hörnet av skärmen.
4. Välj **Profil**.
5. Knacka **Lägg till ägare**, fyll sedan i motsvarande fält. Anpassa profilen genom att lägga till ett foto, välja ett födelsedatum och lägga till en e-postadress och ett telefonnummer.
6. Knacka **LÄGG TILL** för att spara profilen.

7. Välj önskad ägare från **Enhetsägare** lista och tryck sedan på **TILLDELA**.

4.4.3. Fjärråtgärder

För att fjärruppdatera Bitdefender på en enhet:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. Tryck på önskat enhetskort och sedan på ⋮ ikonen i det övre högra hörnet av skärmen.
4. Välj **Uppdatering**.

För fler fjärråtgärder och information om din Bitdefender-produkt på en specifik enhet, tryck på önskat enhetskort.

När du trycker på ett enhetskort är följande flikar tillgängliga:

- **Instrumentbräda.** I det här fönstret kan du se detaljer om den valda enheten, kontrollera dess skyddsstatus, status för Bitdefender VPN och hur många hot som har blockerats under de senaste sju dagarna. Skyddsstatusen kan vara grön, när det inte finns några problem som påverkar din enhet, gul när enheten behöver din uppmärksamhet eller röd när enheten är i fara. När det finns problem som påverkar din enhet, tryck på rullgardinspilen i det övre statusområdet för att få mer information.
- **Skydd.** Från det här fönstret kan du fjärrköra en snabb- eller systemsökning på dina enheter. Tryck på **SKANNA** knappen för att starta processen. Du kan också kontrollera när den senaste skanningen utfördes på enheten och en rapport över den senaste skanningen med den viktigaste informationen finns tillgänglig.
- **Optimizer.** Här kan du förbättra en enhets prestanda på distans genom att snabbt skanna, upptäcka och rensa värdelösa filer. Tryck på **START** och välj sedan de områden du vill optimera. Tryck igen på **START** för att starta optimeringsprocessen. Knacka **Fler detaljer** för att få tillgång till en detaljerad rapport om de åtgärdade problemen.
- **Anti-stöld.** I händelse av felplacering, stöld eller förlust, med stöldskyddsfunktionen kan du lokalisera din enhet och vidta fjärråtgärder. Knacka **LOKALISERA** för att ta reda på enhetens

position. Den senast kända positionen kommer att visas tillsammans med tid och datum.

- **Sårbarhet.** För att kontrollera en enhet för eventuella sårbarheter som saknade Windows-uppdateringar, föråldrade appar eller svaga lösenord tryck på **SKANNA** på fliken Sårbarhet. Sårbarheter kan inte fixas på distans. Om någon sårbarhet hittas måste du köra en ny skanning på enheten och sedan vidta de rekommenderade åtgärderna. Knacka **Fler detaljer** för att få tillgång till en detaljerad rapport om de hittade problemen.

4.5. Aktivitet

I aktivitetsområdet har du tillgång till information om enheterna som har Bitdefender installerat.

När du väl kommer åt **Aktivitet** fönster finns följande kort tillgängliga:

- **Mina enheter**. Här kan du se antalet anslutna enheter tillsammans med deras skyddsstatus. För att åtgärda problem på distans på de upptäckta enheterna, tryck på **Fixa problem**och tryck sedan på **SKANNA OCH ÅTGÄRDA PROBLEM**.

  För att se detaljer om de upptäckta problemen, tryck på **Visa problem**.

  Information om upptäckta hot kan inte hämtas från iOS-baserade enheter.

- **Hot blockerade**. Här kan du se en graf som visar en övergripande statistik inklusive information om de hot som blockerats under de senaste 24 timmarna och sju dagarna. Den visade informationen hämtas beroende på det skadliga beteende som upptäcks på åtkomst till filer, appar och webbadresser.

- **Toppanvändare med hot blockerade**. Här kan du se en topp med användarna där de flesta hoten har hittats.

- **Toppenheter med hot blockerade**. Här kan du se en topp med enheterna där de flesta hoten har hittats.

4.6. mina prenumerationer

Bitdefender Central-plattformen ger dig möjligheten att enkelt hantera de prenumerationer du har för alla dina enheter.

4.6.1. Kontrollera tillgängliga abonnemang

Så här kontrollerar du dina tillgängliga prenumerationer:

1. Tillgång Bitdefender Central.
2. Välj **mina prenumerationer** panel.

Här har du information om tillgängligheten för de prenumerationer du äger och antalet enheter som använder var och en av dem.

Du kan lägga till en ny enhet i ett abonnemang eller förnya den genom att välja ett abonnemangskort.

> **Notera**
> Du kan ha ett eller flera abonnemang på ditt konto förutsatt att de är för olika plattformar (Windows, macOS, iOS eller Android).

4.6.2. Aktivera prenumeration

En prenumeration kan aktiveras under installationsprocessen genom att använda ditt Bitdefender-konto. Tillsammans med aktiveringsprocessen börjar prenumerationens giltighet räknas ned.

Om du har köpt en aktiveringskod från en av våra återförsäljare eller fått den i present, kan du lägga till dess tillgänglighet till ditt Bitdefender-abonnemang.

För att aktivera ett abonnemang med en aktiveringskod, följ dessa steg:

1. Tillgång Bitdefender Central.
2. Välj **mina prenumerationer** panel.
3. Tryck på **AKTIVERINGSKOD** knappen och skriv sedan koden i motsvarande fält.
4. Knacka **AKTIVERA** att fortsätta.

Abonnemanget är nu aktiverat.

4.6.3. Förnya prenumeration

Om du inaktiverade den automatiska förnyelsen av din Bitdefender-prenumeration kan du förnya den manuellt genom att följa dessa steg:

1. Tillgång Bitdefender Central.

2. Välj **mina prenumerationer** panel.
3. Välj önskat abonnemangskort.
4. Knacka **FÖRNYA** att fortsätta.

En webbsida öppnas i din webbläsare där du kan förnya ditt Bitdefender-abonnemang.

4.7. Aviseringar

För att hjälpa dig att hålla dig informerad om vad som händer på enheterna som är kopplade till ditt konto ikonen är till hands. När du väl trycker på den har du en övergripande bild som består av information om aktiviteten hos Bitdefender-produkterna installerade på dina enheter.

5. VANLIGA FRÅGOR

Hur skyddar Bitdefender Mobile Security för iOS mig mot virus och cyberhot?

Bitdefender Mobile Security för iOS ger absolut skydd mot alla cyberhot och är speciellt utformad för att skydda din känsliga data från nyfikna ögon.

Du får en mängd avancerade säkerhets- och sekretessfunktioner för din iPhone och iPad – plus många bonusfunktioner, inklusive VPN och webbskydd.

Bitdefender Mobile Security för iOS reagerar omedelbart på virus och skadlig programvara utan att kompromissa med ditt systems prestanda.

Vilken typ av enheter och operativsystem täcker Bitdefender Mobile Security för iOS?

Bitdefender Mobile Security för iOS kommer att skydda dina smartphones och surfplattor som kör iOS mot alla cyberhot.

Varför behöver jag Bitdefender Mobile Security för iOS på Apple OS?

En del av dina mest personliga uppgifter lagras på din iPhone eller iPad – och du måste veta att den alltid är säker. Bitdefender Mobile Security för iOS ger absolut skydd mot cyberhot och tar hand om din integritet online och privat information utan att störa dina dagliga aktiviteter.

Får jag ett VPN med min Bitdefender Mobile Security för iOS-prenumeration?

Bitdefender Mobile Security för iOS kommer med en grundläggande version av Bitdefender VPN som inkluderar en generös mängd trafik (200 MB/dag, totalt 6GB/månad) gratis.

6. FÅ HJÄLP

6.1. Ber om hjälp

Bitdefender ger sina kunder en oöverträffad nivå av snabb och exakt support. Om du upplever några problem eller om du har några frågor om din Bitdefender-produkt, kan du använda flera onlineresurser för att hitta en lösning eller ett svar. Samtidigt kan du kontakta Bitdefender Customer Care-teamet. Våra supportrepresentanter kommer att svara på dina frågor i tid och ge dig den hjälp du behöver.

6.2. Onlineresurser

Flera onlineresurser finns tillgängliga för att hjälpa dig att lösa dina Bitdefender-relaterade problem och frågor.

- Bitdefender Support Center:
  https://www.bitdefender.se/consumer/support/
- Bitdefender Expert Community:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Du kan också använda din favoritsökmotor för att ta reda på mer information om datorsäkerhet, Bitdefender-produkterna och företaget.

6.2.1. Bitdefender Support Center

Bitdefender Support Center är ett onlineförråd med information om Bitdefender-produkterna. Den lagrar, i ett lättillgängligt format, rapporter om resultaten av den pågående tekniska supporten och buggfixningsaktiviteterna för Bitdefender-support- och utvecklingsteamen, tillsammans med mer allmänna artiklar om hotförebyggande, hantering av Bitdefender-lösningar med detaljerade förklaringar och många andra artiklar.

Bitdefender Support Center är öppet för allmänheten och fritt sökbart. Den omfattande informationen den innehåller är ytterligare ett sätt att förse Bitdefender-kunder med den tekniska kunskap och insikt de behöver. Alla giltiga förfrågningar om information eller buggrapporter

som kommer från Bitdefender-klienter hittar så småningom vägen till Bitdefender Support Center, som bugfixrapporter, fuskblad för lösningar eller informationsartiklar för att komplettera produkthjälpfiler.

Bitdefender Support Center är tillgängligt när som helst på följande adress: https://www.bitdefender.se/consumer/support/.

6.2.2. Bitdefender Expert Community

Expertgemenskapen är en miljö där Bitdefender-användare, entusiaster och fans kan engagera sig, utbyta idéer, stödja varandra och dela sina kunskaper och lösningar. Det är också en plats för idéer och ger värdefull feedback till våra utvecklingsteam. Community-medlemmarna är erfarna Bitdefender-användare som gärna hjälper andra kamrater på sin egen tid. Med deras enorma bidrag och genuina frivilliga insatser har vi skapat en kunskapsbas där användare kan hitta svar och vägledning, men med den mänskliga touchen.

Här hittar du meningsfulla konversationer med personer som använder Bitdefender på sina enheter. Gemenskapen erbjuder en sann kontakt med våra medlemmar och gör din röst hörd. Det är en plats där du uppmuntras att delta i vetskapen om att din åsikt och din input respekteras och omhuldas. Som en uppskattad leverantör strävar vi efter att erbjuda en oöverträffad nivå av snabb, exakt support och vi vill föra våra användare närmare oss. Vi har utformat vår community med detta syfte i åtanke.

Du hittar vår webbsida för expertgemenskapen här:

https://community.bitdefender.com/en/

6.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia har all information du behöver om de senaste cyberhoten. Det här är platsen där Bitdefender-experter delar med sig av tips och tricks om hur man kan hålla sig skyddad från hackare, dataintrång, identitetsstöld och sociala identitetsförsök.

Bitdefender Cyberpedias webbsida finns här:

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

6.3. Kontaktinformation

Effektiv kommunikation är nyckeln till ett framgångsrikt företag. Sedan 2001 har BITDEFENDER etablerat ett obestridligt rykte genom att

ständigt sträva efter bättre kommunikation för att överträffa våra kunders och partners förväntningar. Om du har några frågor, tveka inte att kontakta oss direkt via vår Bitdefender Support Center (sida 28).

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

6.3.1. Lokala distributörer

Bitdefender lokala distributörer är redo att svara på alla förfrågningar om deras verksamhetsområden, både i kommersiella och allmänna frågor.

Så här hittar du en Bitdefender-distributör i ditt land:

1. Gå till https://www.bitdefender.com/partners/partner-locator.html.
2. Välj ditt land och din stad med hjälp av motsvarande alternativ.

ORDLISTA

Aktiveringskod

Är en unik nyckel som kan köpas från detaljhandeln och användas för att aktivera en specifik produkt eller tjänst. En aktiveringskod möjliggör aktivering av ett giltigt abonnemang under en viss tidsperiod och antal enheter och kan även användas för att förlänga ett abonnemang med villkoret att genereras för samma produkt eller tjänst.

ActiveX

ActiveX är en modell för att skriva program så att andra program och operativsystemet kan anropa dem. ActiveX-teknik används med Microsoft Internet Explorer för att skapa interaktiva webbsidor som ser ut och beter sig som datorprogram, snarare än statiska sidor. Med ActiveX kan användare ställa eller svara på frågor, använda tryckknappar och interagera på andra sätt med webbsidan. ActiveX-kontroller skrivs ofta med Visual Basic. Active X är anmärkningsvärt för en fullständig brist på säkerhetskontroller; datorsäkerhetsexperter avråder från att använda det över internet.

Avancerat ihållande hot

Advanced persistent hot (APT) utnyttjar sårbarheter i system för att stjäla viktig information för att leverera den till källan. Stora grupper som organisationer, företag eller regeringar är föremål för detta hot. Målet med ett avancerat ihållande hot är att förbli oupptäckt under lång tid och kunna övervaka och samla in viktig information utan att skada de riktade maskinerna. Metoden som används för att injicera hotet i nätverket är genom en PDF-fil eller ett Office-dokument som ser ofarliga ut så att alla användare kan köra filerna.

Reklamprogram

Adware kombineras ofta med en värdapp som tillhandahålls utan kostnad så länge som användaren accepterar adware. Eftersom adware-appar vanligtvis installeras efter att användaren har godkänt ett licensavtal som anger syftet med appen, begås inget brott. Men popup-annonser kan bli irriterande och i vissa fall försämra systemets prestanda. Dessutom kan informationen som vissa av dessa appar samlar in orsaka integritetsproblem för användare som inte var fullt medvetna om villkoren i licensavtalet.

Arkiv

En disk, ett band eller en katalog som innehåller filer som har säkerhetskopierats.

En fil som innehåller en eller flera filer i ett komprimerat format.

Bakdörr

Ett hål i säkerheten i ett system som medvetet lämnats på plats av designers eller underhållare. Motivationen för sådana hål är inte alltid olycksbådande; vissa operativsystem, till exempel, kommer ur lådan med privilegierade konton avsedda att användas av fältservicetekniker eller säljarens underhållsprogrammerare.

Boot sektor

En sektor i början av varje disk som identifierar diskens arkitektur (sektorstorlek, klusterstorlek, och så vidare). För startdiskar innehåller bootsektorn även ett program som laddar operativsystemet.

Boot virus

Ett hot som infekterar startsektorn på en fast eller diskett. Ett försök att starta från en diskett som är infekterad med ett bootsektorvirus gör att hotet blir aktivt i minnet. Varje gång du startar ditt system från den tidpunkten kommer du att ha hotet aktivt i minnet.

Botnet

Termen "botnät" är sammansatt av orden "robot" och "nätverk". Botnät är internetanslutna enheter som är infekterade med hot och kan användas för att skicka skräppost, stjäla data, fjärrstyra sårbara enheter eller sprida spionprogram, ransomware och andra typer av hot. Deras mål är att infektera så många uppkopplade enheter som möjligt, såsom datorer, servrar, mobila eller IoT-enheter som tillhör stora företag eller industrier.

Webbläsare

Förkortning för webbläsare, en programvaruapp som används för att hitta och visa webbsidor. Populära webbläsare inkluderar Microsoft Internet Explorer, Mozilla Firefox och Google Chrome. Dessa är grafiska webbläsare, vilket innebär att de kan visa grafik såväl som text. Dessutom kan de flesta moderna webbläsare presentera multimediainformation, inklusive ljud och video, även om de kräver plugin-program för vissa format.

Brute Force Attack

Lösenordsgissningsattack används för att bryta sig in i ett datorsystem genom att ange möjliga lösenordskombinationer, oftast med det enklast att gissa lösenordet.

Kommandorad

I ett kommandoradsgränssnitt skriver användaren kommandon i utrymmet som tillhandahålls direkt på skärmen med hjälp av kommandospråk.

Småkakor

Inom internetbranschen beskrivs cookies som små filer som innehåller information om enskilda datorer som kan analyseras och användas av annonsörer för att spåra dina intressen och smaker online. I det här området utvecklas fortfarande cookieteknologi och avsikten är att rikta annonser direkt till det du har sagt att dina intressen är. Det är ett tveeggat svärd för många människor eftersom det å ena sidan är effektivt och relevant eftersom du bara ser annonser om det du är intresserad av. Å andra sidan handlar det faktiskt om att "spåra" och "följa" vart du går och vad du klickar på. Det är förståeligt nog att det finns en debatt om integritet och många känner sig kränkta av uppfattningen att de ses som ett "SKU-nummer" (ni vet, streckkoden på baksidan av paketen som skannas vid utcheckningslinjen) . Även om denna synpunkt kan vara extrem, är den i vissa fall korrekt.

Cybermobbning

När kamrater eller främlingar begår kränkande handlingar mot barn med avsikt för att fysiskt skada dem. För att skada känslomässigt skickar angriparna elaka meddelanden eller föga smickrande bilder, vilket gör att deras offer isolerar sig från andra eller känner sig frustrerade.

Ordbok Attack

Lösenordsgissningsattacker används för att bryta sig in i ett datorsystem genom att ange en kombination av vanliga ord för att generera potentiella lösenord. Samma metod används för att gissa dekrypteringsnycklar för krypterade meddelanden eller dokument. Ordboksattacker lyckas eftersom många människor är benägna att välja korta och enstaka ordlösenord som är lätta att gissa.

Diskenhet

Det är en maskin som läser data från och skriver data till en disk. En hårddisk läser och skriver hårddiskar. En diskettenhet får åtkomst till disketter. Diskenheter kan antingen vara interna (inrymd i en dator) eller externa (inrymd i en separat låda som ansluts till datorn).

Ladda ner

Att kopiera data (vanligtvis en hel fil) från en huvudkälla till en kringutrustning. Termen används ofta för att beskriva processen att kopiera en fil från en onlinetjänst till sin egen dator. Nedladdning kan också syfta på att kopiera en fil från en nätverksfilserver till en dator i nätverket.

E-post

E-post. En tjänst som skickar meddelanden på datorer via lokala eller globala nätverk.

evenemang

En åtgärd eller händelse som upptäckts av ett program. Händelser kan vara användaråtgärder, som att klicka på en musknapp eller trycka på en tangent, eller systemhändelser, som att minnet blir slut.

Utnyttjar

Ett sätt att dra nytta av olika buggar eller sårbarheter som finns i en dator (mjukvara eller hårdvara). Således kan hackare få kontroll över datorer eller nätverk.

Falskt positivt

Uppstår när en skanner identifierar en fil som infekterad när den faktiskt inte är det.

Filnamnstillägg

Den del av ett filnamn, efter den sista punkten, som anger vilken typ av data som lagras i filen. Många operativsystem använder filnamnstillägg, t.ex. Unix, VMS och MS-DOS. De är vanligtvis från en till tre bokstäver (vissa tråkiga gamla operativsystem stöder inte mer än tre). Exempel inkluderar "c" för C-källkod, "ps" för PostScript, "txt" för godtycklig text.

Heuristisk

En regelbaserad metod för att identifiera nya hot. Denna metod för skanning är inte beroende av specifik databas med hotinformation. Fördelen med den heuristiska skanningen är att den inte luras av en ny

variant av ett befintligt hot. Det kan dock ibland rapportera misstänkt kod i vanliga program, vilket genererar den så kallade "falska positiva".

Honungsburk

Ett lockdatorsystem som lockar hackare att studera hur de agerar och identifiera de kätterska metoder de använder för att samla in systeminformation. Företag och företag är mer intresserade av att implementera och använda honeypots för att förbättra sin övergripande säkerhet.

IP

Internet Protocol - Ett routbart protokoll i TCP/IP-protokollsviten som ansvarar för IP-adressering, routing och fragmentering och återmontering av IP-paket.

Java applet

Ett Java-program som är designat för att endast köras på en webbsida. För att använda en applet på en webbsida skulle du ange namnet på appleten och storleken (längd och bredd, i pixlar) som appleten kan använda. När webbsidan nås laddar webbläsaren ner appleten från en server och kör den på användarens dator (klienten). Applets skiljer sig från appar genom att de styrs av ett strikt säkerhetsprotokoll.

Till exempel, även om appletar körs på klienten, kan de inte läsa eller skriva data på klientens dator. Dessutom är appletar ytterligare begränsade så att de bara kan läsa och skriva data från samma domän som de betjänas från.

Keylogger

En keylogger är en app som loggar allt du skriver. Keyloggers är inte skadliga till sin natur. De kan användas för legitima ändamål, som att övervaka anställda eller barnaktivitet. De används dock i allt högre grad av cyberbrottslingar i skadliga syften (till exempel för att samla in privata uppgifter, såsom inloggningsuppgifter och personnummer).

Makrovirus

En typ av datorhot som är kodat som ett makro inbäddat i ett dokument. Många appar, som Microsoft Word och Excel, stöder kraftfulla makrospråk. Dessa appar låter dig bädda in ett makro i ett dokument och få makrot att köras varje gång dokumentet öppnas.

E-postklient

En e-postklient är en app som gör att du kan skicka och ta emot e-post.

Minne

Interna lagringsutrymmen i datorn. Termen minne identifierar datalagring som kommer i form av chips, och ordet lagring används för minne som finns på band eller diskar. Varje dator kommer med en viss mängd fysiskt minne, vanligtvis kallat huvudminne eller RAM.

Icke-heuristisk

Denna metod för skanning bygger på specifik databas med hotinformation. Fördelen med den icke-heuristiska skanningen är att den inte luras av vad som kan tyckas vara ett hot och inte genererar falsklarm.

Rovdjur online

Individer som försöker locka minderåriga eller tonåringar till konversationer med avsikt att involvera dem i illegala sexuella aktiviteter. Sociala nätverk är den idealiska platsen där utsatta barn lätt kan jagas och förföras till att begå sexuella aktiviteter, online eller ansikte mot ansikte.

Packade program

En fil i ett komprimeringsformat. Många operativsystem och appar innehåller kommandon som gör att du kan packa en fil så att den tar mindre minne. Anta till exempel att du har en textfil som innehåller tio på varandra följande mellanslagstecken. Normalt skulle detta kräva tio byte lagring.

Ett program som packar filer skulle dock ersätta mellanslagstecken med ett speciellt mellanslagsserietecken följt av antalet mellanslag som ersätts. I detta fall skulle de tio utrymmena endast kräva två byte. Detta är bara en packningsteknik - det finns många fler.

Väg

Den exakta vägbeskrivningen till en fil på en dator. Dessa riktningar beskrivs vanligtvis med hjälp av det hierarkiska arkiveringssystemet uppifrån och ner.

Rutten mellan två valfria punkter, till exempel kommunikationskanalen mellan två datorer.

Nätfiske

Handlingen att skicka ett e-postmeddelande till en användare som falskeligen påstår sig vara ett etablerat legitimt företag i ett

försök att lura användaren till att överlämna privat information som kommer att användas för identitetsstöld. E-postmeddelandet uppmanar användaren att besöka en webbplats där de ombeds att uppdatera personlig information, såsom lösenord och kreditkort, personnummer och bankkontonummer, som den legitima organisationen redan har. Webbplatsen är dock falsk och inrättad endast för att stjäla användarens information.

Foton

Photon är en innovativ, icke-påträngande Bitdefender-teknik, designad för att minimera prestandapåverkan från din säkerhetslösning. Genom att övervaka din dators aktivitet i bakgrunden skapar den användningsmönster som hjälper till att optimera uppstarts- och skanningsprocesser.

Polymorft virus

Ett hot som ändrar form för varje fil som den infekterar. Eftersom de inte har något konsekvent binärt mönster är sådana hot svåra att identifiera.

Hamn

Ett gränssnitt på en dator som du kan ansluta en enhet till. Persondatorer har olika typer av portar. Internt finns det flera portar för att ansluta diskenheter, bildskärmar och tangentbord. Externt har persondatorer portar för anslutning av modem, skrivare, möss och annan kringutrustning.

I TCP/IP- och UDP-nätverk, en slutpunkt till en logisk anslutning. Portnumret identifierar vilken typ av port det är. Till exempel används port 80 för HTTP-trafik.

Ransomware

Ransomware är ett skadligt program som försöker tjäna pengar på användare genom att låsa deras sårbara system. CryptoLocker, CryptoWall och TeslaWall, är bara några varianter som jagar användarnas personliga system.

Infektionen kan spridas genom att komma åt skräppostmeddelanden, ladda ner e-postbilagor eller installera appar, utan att låta användaren veta vad som händer på hans system. Dagliga användare och företag riktas mot ransomware-hackare.

Rapportfil

En fil som listar åtgärder som har inträffat. Bitdefender har en rapportfil som visar sökvägen som skannats, mapparna, antalet skannade arkiv och filer, hur många infekterade och misstänkta filer som hittades.

Rootkit

Ett rootkit är en uppsättning mjukvaruverktyg som ger åtkomst till ett system på administratörsnivå. Termen användes först för UNIX-operativsystemen och den hänvisade till omkompilerade verktyg som gav inkräktare administrativa rättigheter, så att de kunde dölja sin närvaro så att de inte syns av systemadministratörerna.

Den huvudsakliga rollen för rootkits är att dölja processer, filer, inloggningar och loggar. De kan också fånga upp data från terminaler, nätverksanslutningar eller kringutrustning, om de innehåller lämplig programvara.

Rootkits är inte skadliga till sin natur. Till exempel döljer system och till och med vissa appar viktiga filer med rootkits. Men de används mest för att dölja hot eller för att dölja närvaron av en inkräktare i systemet. I kombination med hot utgör rootkits ett stort hot mot integriteten och säkerheten i ett system. De kan övervaka trafik, skapa bakdörrar i systemet, ändra filer och loggar och undvika upptäckt.

Manus

En annan term för makro- eller batchfil, ett skript är en lista med kommandon som kan köras utan användarinteraktion.

Spam

Elektronisk skräppost eller skräpnyhetsgrupper. Allmänt känd som all oönskad e-post.

Spionprogram

All programvara som i hemlighet samlar in användarinformation via användarens internetanslutning utan hans eller hennes vetskap, vanligtvis i reklamsyfte. Spionprogram är vanligtvis paketerade som en dold komponent av gratisprogram eller shareware-program som kan laddas ner från internet; Det bör dock noteras att majoriteten av shareware och freeware-appar inte kommer med spionprogram. När det väl har installerats övervakar spionprogrammet användaraktivitet på internet och överför informationen i bakgrunden till någon annan. Spionprogram kan också samla information om e-postadresser och till och med lösenord och kreditkortsnummer.

Spionprograms likhet med ett trojansk hästhot är det faktum att användare omedvetet installerar produkten när de installerar något annat. Ett vanligt sätt att bli offer för spionprogram är att ladda ner vissa peer-to-peer filbytesprodukter som är tillgängliga idag.

Bortsett från frågorna om etik och integritet stjäl spionprogram från användaren genom att använda datorns minnesresurser och även genom att äta bandbredd då det skickar information tillbaka till spionprogrammets hembas via användarens internetanslutning. Eftersom spionprogram använder minne och systemresurser kan apparna som körs i bakgrunden leda till systemkrascher eller allmän systeminstabilitet.

Startobjekt

Alla filer som placeras i den här mappen öppnas när datorn startar. Till exempel kan en startskärm, en ljudfil som ska spelas upp när datorn startar, en påminnelseskalender eller appar vara startobjekt. Normalt placeras ett alias för en fil i den här mappen istället för själva filen.

Prenumeration

Köpeavtal som ger användaren rätt att använda en viss produkt eller tjänst på ett visst antal enheter och under en viss tid. Ett utgånget abonnemang kan förnyas automatiskt med den information som användaren lämnade vid första köpet.

Systemfältet

Systemfältet, som introducerades med Windows 95, finns i aktivitetsfältet i Windows (vanligtvis längst ner bredvid klockan) och innehåller miniatyrikoner för enkel åtkomst till systemfunktioner som fax, skrivare, modem, volym med mera. Dubbelklicka eller högerklicka på en ikon för att visa och komma åt detaljerna och kontrollerna.

TCP/IP

Transmission Control Protocol/Internet Protocol - En uppsättning nätverksprotokoll som ofta används på internet som tillhandahåller kommunikation över sammankopplade nätverk av datorer med olika hårdvaruarkitekturer och olika operativsystem. TCP/IP innehåller standarder för hur datorer kommunicerar och konventioner för att ansluta nätverk och dirigera trafik.

Hot

Ett program eller kod som läses in på din dator utan din vetskap och som körs mot din vilja. De flesta hot kan också replikera sig själva. Alla

datorhot är konstgjorda. Ett enkelt hot som kan kopiera sig själv om och om igen är relativt lätt att producera. Även ett så enkelt hot är farligt eftersom det snabbt kommer att använda allt tillgängligt minne och få systemet att stanna. En ännu farligare typ av hot är en som kan överföra sig själv över nätverk och kringgå säkerhetssystem.

Uppdatering av hotinformation

Det binära mönstret för ett hot, som används av säkerhetslösningen för att upptäcka och eliminera hotet.

Trojan

Ett destruktivt program som maskerar sig som en godartad app. Till skillnad från skadliga program och maskar replikerar trojaner inte sig själva men de kan vara lika destruktiva. En av de mest lömska typerna av trojanska hästhot är ett program som påstår sig befria din dator från hot men istället introducerar hot på din dator.

Termen kommer från en berättelse i Homeros Iliaden, där grekerna ger en gigantisk trähäst till sina fiender, trojanerna, skenbart som ett fredsoffer. Men efter att trojanerna släpat hästen innanför sina stadsmurar, smyger grekiska soldater ut ur hästens ihåliga mage och öppnar stadsportarna, så att deras landsmän kan strömma in och fånga Troja.

Uppdatering

En ny version av en mjuk- eller hårdvaruprodukt utformad för att ersätta en äldre version av samma produkt. Dessutom kontrollerar installationsrutinerna för uppdateringar ofta att en äldre version redan är installerad på din dator; Om inte kan du inte installera uppdateringen.

Bitdefender har sin egen uppdateringsfunktion som låter dig söka manuellt efter uppdateringar, eller låta den uppdatera produkten automatiskt.

Virtual Private Network (VPN)

Är en teknik som möjliggör en tillfällig och krypterad direktanslutning till ett visst nätverk över ett mindre säkert nätverk. På så sätt är det säkert och krypterat att skicka och ta emot data, svårt att fångas av snokare. Ett bevis på säkerhet är autentiseringen, som endast kan göras med ett användarnamn och lösenord.

Mask

Ett program som sprider sig över ett nätverk och reproducerar sig själv allt eftersom. Den kan inte koppla sig till andra program.