Bitdefender®
MOBILE SECURITY

ANVÄNDARMAN
UAL

Bitdefender Mobile Security

Användarmanual

Publiceringsdatum 2022-11-22

Rättsligt meddelande

Bitdefender

Innehållsförteckning

OM DEN HÄR GUIDEN

Syfte och avsedd målgrupp

Den här guiden är avsedd för alla Android-användare som har valt Bitdefender Mobile Security 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 med Android-enheter.

Du kommer att få reda på hur du konfigurerar och använder Bitdefender Mobile Security 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 och dess användargränssnitt.

Funktioner och funktioner (sida 9)

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

Få hjälp (sida 46)

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

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 låter dig:

- Få det bästa skyddet för din Android-smarttelefon och surfplatta med minimal påverkan på batteritiden
- Skydda dig själv från att falla offer för länkbaserade mobilbedrägerier
- Ha tillgång till vårt säkra VPN för en snabb, anonym och säker upplevelse när du surfar på webben
- Hitta, lås och torka din Android-enhet på distans i händelse av förlust eller stöld
- Kontrollera om ditt e-postkonto har varit inblandat i databrott eller dataläckor

2. KOMMA IGÅNG

2.1. Enhetskrav

Bitdefender Mobile Security fungerar på alla enheter som kör Android 5.0 eller senare versioner av operativsystemet. En aktiv internetanslutning krävs för genomsökning av hot i molnet.

2.2. Installera Bitdefender Mobile Security

- **Från Bitdefender Central**
  - På Android
    1. Gå till: https://central.bitdefender.com.
    2. Logga in på ditt Bitdefender-konto.
    3. Välj **Mina enheter** panel.
    4. Knacka **INSTALLATIONSSKYDD**och tryck sedan på **Skydda den här enheten**.
    5. Välj enhetens ägare. Om enheten tillhör någon annan trycker du på motsvarande knapp.
    6. Du omdirigeras till **Google Play** app. På Google Play-skärmen trycker du på installationsalternativet.
  - På Windows, macOS och iOS
    1. Gå till: https://central.bitdefender.com.
    2. Logga in på ditt Bitdefender-konto.
    3. Välj **Mina enheter** panel.
    4. Tryck **INSTALLATIONSSKYDD**, och tryck sedan på **Skydda andra enheter**.
    5. Välj enhetens ägare. Om enheten tillhör någon annan, tryck på motsvarande knapp.
    6. Tryck **SKICKA NEDLADDNINGSLÄNK**.
    7. 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.

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

- **Från Google Play**
  Sök efter Bitdefender Mobile Security för att hitta och installera appen. Alternativt, skanna QR-koden:

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

2.3. Logga in på ditt Bitdefender-konto

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

Om du installerade Bitdefender Mobile Security från ditt Bitdefender-konto kommer appen att försöka logga in på det kontot automatiskt.

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

1. Ange e-postadressen och lösenordet för ditt Bitdefender-konto i motsvarande fält. Om du inte har ett Bitdefender-konto och vill skapa ett, välj motsvarande länk.
2. Knacka **LOGGA IN**.

För att logga in med ett Facebook-, Google- eller Microsoft-konto trycker du på tjänsten du vill använda i området ELLER LOGGA

MED. Du omdirigeras till inloggningssidan för den valda tjänsten. Följ instruktionerna för att länka ditt konto till Bitdefender Mobile Security.

> **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.

2.4. Konfigurera skydd

När du har loggat in på appen visas fönstret Konfigurera skydd. För att säkra din enhet rekommenderar vi att du går igenom dessa steg:

- **Prenumerationsstatus**. För att skyddas av Bitdefender Mobile Security måste du aktivera din produkt med ett abonnemang, som anger hur länge du får använda produkten. Så snart den löper ut slutar appen att utföra sina funktioner och skydda din enhet.
  Om du har en aktiveringskod trycker du på I **HAR EN KOD**och tryck sedan på **AKTIVERA**.
  Om du har loggat in med ett nytt Bitdefender-konto och inte har någon aktiveringskod kan du använda produkten i 14 dagar utan kostnad.
- **Nätskydd**. Om din enhet kräver tillgänglighet för att aktivera webbskydd trycker du på **AKTIVERA**. Du omdirigeras till tillgänglighetsmenyn. Tryck på Bitdefender Mobile Security och slå sedan på motsvarande switch.
- **Skanner för skadlig programvara**. Kör en engångsskanning för att se till att din enhet är fri från hot. För att starta skanningsprocessen, tryck på **SKANNA NU**.
  Så snart skanningsprocessen börjar visas instrumentpanelen. Här kan du se säkerhetsstatusen för din enhet.

2.5. instrumentbräda

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

Instrumentpanelen ger information om din enhets säkerhetsstatus och genom Autopilot hjälper du dig att förbättra enhetens säkerhet genom att ge dig rekommendationer om funktioner.

Statuskortet högst upp i fönstret informerar dig om enhetens säkerhetsstatus med hjälp av explicita meddelanden och suggestiva

färger. Om Bitdefender Mobile Security inte har några varningar är statuskortet grönt. När ett säkerhetsproblem har upptäckts ändras statuskortets färg till rött.

För att erbjuda dig en effektiv operation och ökat skydd samtidigt som du utför olika aktiviteter, **Bitdefender autopilot** kommer att fungera som din personliga säkerhetsrådgivare. Beroende på aktiviteten du utför kommer Bitdefender Autopilot med kontextuella rekommendationer baserat på din enhetsanvändning och behov. Detta hjälper dig att upptäcka och dra nytta av fördelarna med funktionerna som ingår i Bitdefender Mobile Security-appen.

Närhelst det pågår en process eller en funktion kräver din input, visas ett kort med mer information och möjliga åtgärder i instrumentpanelen.

Du kan komma åt Bitdefender Mobile Security-funktionerna och enkelt navigera från det nedre navigeringsfältet:

Skanner för skadlig programvara

Gör att du kan starta en genomsökning på begäran och aktivera skanningslagring. För mer information, se Skanner för skadlig programvara (sida 9).

Nätskydd

Säkerställer en säker surfupplevelse genom att varna dig om potentiella skadliga webbsidor. För mer information, se Nätskydd (sida 11).

VPN

Krypterar internetkommunikation, vilket hjälper dig att behålla din integritet oavsett vilket nätverk du är ansluten till. För mer information, se VPN (sida 12).

Scam Alert

Håller dig säker genom att varna dig om skadliga länkar som kommer via SMS, meddelandeprogram och alla typer av meddelanden. För mer information, se Scam Alert (sida 15).

Anti-stöld

Låter dig aktivera eller inaktivera stöldskyddsfunktionerna och konfigurera stöldskyddsinställningar. För mer information, se Stöldskyddsfunktioner (sida 17).

Kontosekretess

Kontrollerar om något dataintrång har inträffat i dina onlinekonton. För mer information, se Kontosekretess (sida 21).

Applås

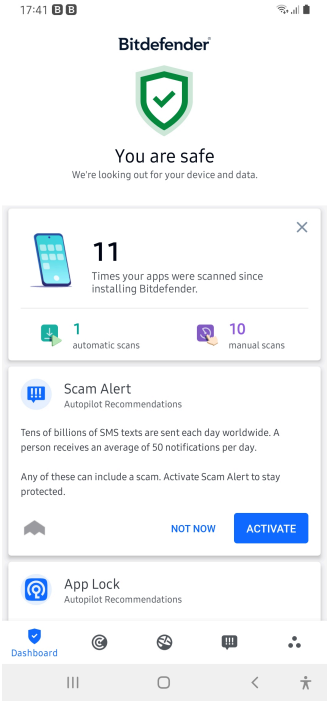
Låter dig skydda dina installerade appar genom att ställa in en PIN-kod. För mer information, se Applås (sida 23).

Rapporter

Håller en logg över alla viktiga åtgärder, statusändringar och andra viktiga meddelanden relaterade till din enhets aktivitet. För mer information, se Rapporter (sida 27).

Bära PÅ

Kommunicerar med din smartklocka för att hjälpa dig hitta din telefon ifall du tappar bort eller glömmer var du lämnade den. För mer information, se Bära PÅ (sida 28).



3. FUNKTIONER OCH FUNKTIONER

3.1. Skanner för skadlig programvara

Bitdefender skyddar din enhet och data mot skadliga appar med hjälp av skanning på installation och skanning på begäran.

Malware Scanner-gränssnittet ger en lista över alla typer av hot Bitdefender letar efter, tillsammans med deras definitioner. Klicka bara på ett hot för att se dess definition.

> **Notera**
> Se till att din mobila enhet är ansluten till internet. Om din enhet inte är ansluten till internet kommer skanningsprocessen inte att starta.

- **Skanning på installation**
  När du installerar en app skannar Bitdefender Mobile Security den automatiskt med hjälp av in-the-cloud-teknik. Samma skanningsprocess startar varje gång de installerade apparna uppdateras.
  Om appen visar sig vara skadlig visas en varning som uppmanar dig att avinstallera den. Knacka **Avinstallera** för att gå till appens avinstallationsskärm.
- **Skanning på begäran**
  Närhelst du vill försäkra dig om att apparna som är installerade på din enhet är säkra att använda kan du initiera en genomsökning på begäran.
  Så här startar du en genomsökning på begäran:
  1. Knacka **Skanner för skadlig programvara** på det nedre navigeringsfältet.
  2. Knacka **STARTA SKANNING**.

> **Notera**
> Ytterligare behörigheter krävs på Android 6 för skannerfunktionen för skadlig programvara. Efter knackning **STARTA SKANNING**, Välj **Tillåta** för följande:
>
> - Tillåta **Antivirus** ringa och hantera telefonsamtal?
> - Tillåta **Antivirus** för att komma åt foton, media och filer på din enhet?

Skanningsförloppet visas och du kan stoppa processen när som helst.

Som standard kommer Bitdefender Mobile Security att skanna din enhets interna lagring, inklusive eventuellt monterat SD-kort. På så sätt kan alla farliga appar som kan finnas på kortet upptäckas innan de kan orsaka skada.

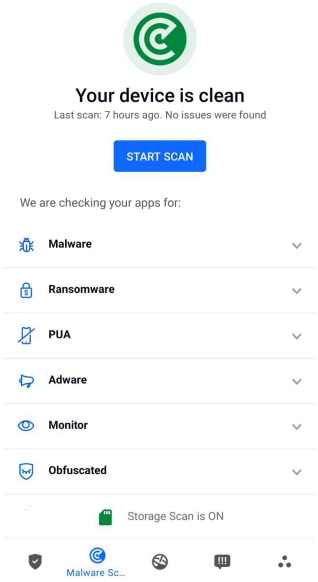
Så här inaktiverar du inställningen Scan Storage:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Inaktivera **Skanna lagring** i området Malware Scanner.

Om några skadliga appar upptäcks kommer information om dem att visas och du kan ta bort dem genom att trycka på **AVINSTALLERA**.

Malware Scanner-kortet visar statusen för din enhet. När din enhet är säker är kortet grönt. När enheten kräver en skanning, eller det finns någon åtgärd som kräver din input, blir kortet rött.

Om din Android-version är 7.1 eller senare kan du komma åt en genväg till Malware Scanner så att du kan köra skanningar snabbare utan att öppna Bitdefender Mobile Security-gränssnittet. För att göra detta, tryck och håll Bitdefender-ikonen på din hemskärm eller applåda och välj sedan ikon.



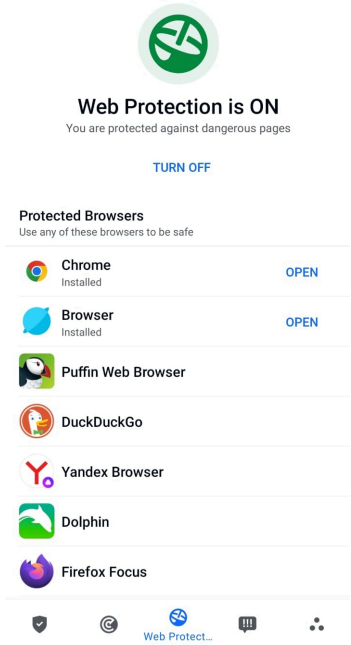
3.2. Nätskydd

Webbskydd kontrollerar med Bitdefender molntjänster webbsidor som du kommer åt med standardwebbläsaren Android, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Yandex Browser, Huawei Browser och Dolphin.

Notera

Ytterligare behörigheter krävs på Android 6 för webbskyddsfunktionen.

Tillåt behörighet att registrera dig som tillgänglighetstjänst och tryck på **SÄTTA PÅ** när det efterfrågas. Knacka **Antivirus** och aktivera omkopplaren, bekräfta sedan att du godkänner åtkomsten till din enhets behörighet.



Varje gång du går in på en bankwebbplats är Bitdefender Web Protection inställt på att meddela dig att du ska använda Bitdefender VPN. Meddelandet visas i statusfältet. Vi rekommenderar att du använder Bitdefender VPN medan du är inloggad på ditt bankkonto så att dina data kan förbli säkra från potentiella säkerhetsintrång.

Så här inaktiverar du webbskyddsmeddelandet:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Stäng av motsvarande strömbrytare i området Webbskydd.

3.3. 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 bankklassad kryptering och dölja din IP-adress var du än är. Din trafik omdirigeras via en separat server; vilket gör din enhet nästan omöjlig att identifieras genom de otaliga andra enheter som använder våra tjänster. Dessutom, medan du är ansluten till internet via VPN, 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.

Det finns två sätt att slå på eller stänga av Bitdefender VPN:

- Knacka **ANSLUTA** i VPN-kortet från Dashboard.
  Status för Bitdefender VPN visas.
- Knacka **VPN** på det nedre navigeringsfältet och tryck sedan på **ANSLUTA**.
  Knacka **ANSLUTA** varje gång du vill vara skyddad medan du är ansluten till osäkra trådlösa nätverk.
  Knacka **KOPPLA IFRÅN** när du vill inaktivera anslutningen.

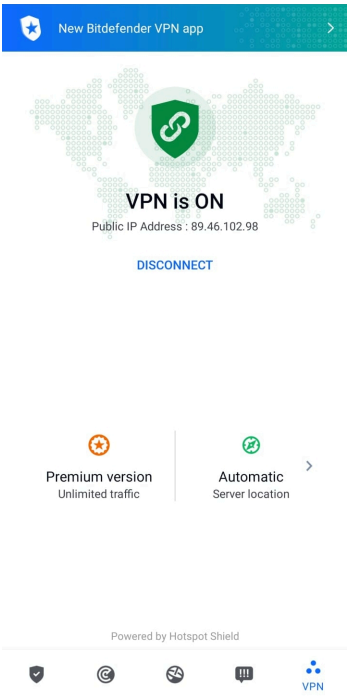
> **Notera**
> Första gången du slår på VPN ombeds du att tillåta Bitdefender att konfigurera en VPN-anslutning som övervakar nätverkstrafik. Knacka **OK** att fortsätta.

Om din Android-version är 7.1 eller senare kan du komma åt en genväg till Bitdefender VPN utan att öppna Bitdefender Mobile Security-gränssnittet.

För att göra detta, tryck och håll Bitdefender-ikonen på din hemskärm eller applåda och välj sedan ikon.

För att spara batteri, rekommenderar vi att du stänger av VPN-funktionen när du inte behöver den.

Om du har ett premiumabonnemang och vill ansluta till en server som du vill, tryck på Serverplats i VPN-funktionen och välj sedan den plats du vill ha. Mer information om VPN-prenumerationer finns i



3.3.1. VPN-inställningar

För en avancerad konfiguration av ditt VPN:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.

I VPN-området kan du konfigurera följande alternativ:

- Snabb VPN-åtkomst – ett meddelande visas i statusfältet på din enhet så att du snabbt kan slå på VPN.
- Öppna Wi-Fi-varning - varje gång du ansluter till ett öppet Wi-Fi-nätverk meddelas du i statusfältet på din enhet om att använda VPN.

3.3.2. 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** i VPN-fönstret.

Bitdefender Premium VPN-prenumeration är oberoende av Bitdefender Mobile Security-prenumerationen, vilket innebär att du kommer att kunna använda den under hela dess tillgänglighet, oavsett tillståndet för ditt säkerhetsabonnemang. Om Bitdefender Premium VPN-prenumerationen går ut, men den för Bitdefender Mobile Security fortfarande är aktiv, kommer du att återgå till den kostnadsfria planen.

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.

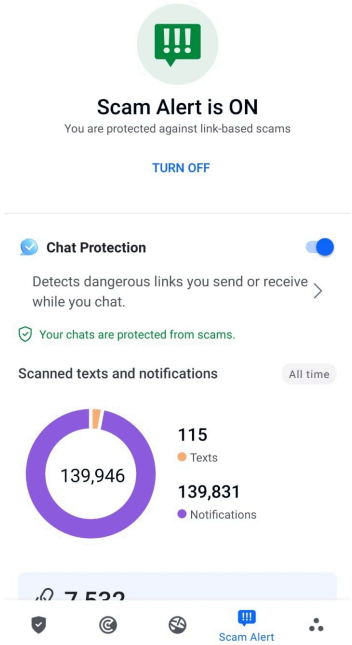
> **Notera**
> Bitdefender VPN fungerar också som en fristående applikation på alla operativsystem som stöds, nämligen Windows, macOS, Android och iOS.

3.4. Scam Alert

Scam Alert-funktionen tar förebyggande åtgärder i förgrunden och hanterar potentiellt farliga situationer innan de ens har en chans att bli ett problem, inklusive hot mot skadlig programvara. Scam Alert övervakar alla inkommande SMS-meddelanden och Android-aviseringar i realtid.

När en farlig länk kommer i ett meddelande på din telefon kommer en varning att dyka upp på din skärm. Bitdefender kommer att erbjuda två alternativ. Det första alternativet är att avvisa informationen. Det andra alternativet är att **VISA DETALJER**. Detta ger dig mer information om händelsen, samt viktiga råd, såsom:

- Öppna eller vidarebefordra inte den upptäckta länken.
- För sms, radera meddelandet om möjligt.
- Blockera avsändaren om de inte är en betrodd kontakt.
- Avinstallera appen som skickar farliga länkar i aviseringar.



Notera

På grund av Android-operativsystemets begränsningar kan Bitdefender inte radera textmeddelanden, vidta några direkta åtgärder relaterade till SMS-meddelanden eller någon annan källa till skadliga meddelanden. Om du ignorerar Scam Alert-varningen och försöker öppna den farliga länken, kommer Bitdefenders webbskyddsfunktion automatiskt att fånga den, vilket förhindrar din enhet från att bli infekterad.

3.4.1. Aktiverar Scam Alert

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

1. Öppna Bitdefender Mobile Security-appen installerad på din Android-telefon eller surfplatta.
2. På Bitdefender-appens huvudskärm, tryck på **Scam Alert** alternativet i det nedre navigeringsfältet och tryck sedan på **SÄTTA PÅ**.
3. Tryck på **TILLÅTA** knapp.

4. I listan Notification Access, växla Bitdefender Security till **PÅ** placera.
5. Bekräfta åtgärden genom att trycka på **TILLÅTA**.
6. Återgå till skärmen Scam Alert och tryck **TILLÅTA** för att ge Bitdefender möjligheten att skanna inkommande SMS-meddelanden.

3.4.2. Chattskydd i realtid

Chattmeddelanden är vårt bekvämaste sätt att hålla kontakten, men de är också ett enkelt sätt för farliga länkar att nå dig.

Med chattskyddsfunktionen aktiverad utökas Scam Alert-modulen från att skydda dina texter och aviseringar till att skydda dina chattar även mot länkbaserade attacker, genom att upptäcka farliga länkar som du antingen skickar eller tar emot medan du chattar.

Så här aktiverar du chattskydd:

1. Öppna Bitdefender Mobile Security-appen installerad på din Android-telefon eller surfplatta.
2. På Bitdefender-appens huvudskärm, tryck på **Scam Alert** alternativet i det nedre navigeringsfältet.
3. Du kommer att mötas av chattskyddsfunktionen överst på fliken Scam Alert. Växla dess motsvarande omkopplare till **PÅ** placera.

> **Notera**
> För närvarande är Chat Protection kompatibelt med följande applikationer:
>
> - WhatsApp
> - Facebook Messenger
> - Telegram
> - Disharmoni

3.5. Stöldskyddsfunktioner

Bitdefender kan hjälpa dig att hitta din enhet och förhindra att dina personuppgifter hamnar i fel händer.

Allt du behöver göra är att aktivera Stöldskydd från enheten och, när det behövs, komma åt **Bitdefender Central** från vilken webbläsare som helst, var som helst.

> **Notera**
> Stöldskyddsgränssnittet innehåller också en länk till vår Bitdefender Central-app på Google Play Butik. Du kan använda den här länken för att ladda ner appen, om du inte redan har gjort det.

Bitdefender Mobile Security erbjuder följande stöldskyddsfunktioner:

Fjärrlokalisera

Visa enhetens aktuella plats på Google Maps. Platsen uppdateras var 5:e sekund, så att du kan spåra den om den är på resande fot.

Platsens noggrannhet beror på hur Bitdefender kan bestämma den:

- Om GPS är aktiverat på enheten kan dess plats fastställas inom ett par meter så länge den är inom GPS-satelliternas räckvidd (dvs. inte inne i en byggnad).
- Om enheten är inomhus kan dess plats bestämmas inom tiotals meter om Wi-Fi är aktiverat och det finns trådlösa nätverk tillgängliga inom dess räckvidd.
- I annat fall kommer platsen att bestämmas med hjälp av endast information från mobilnätet, som kan erbjuda en noggrannhet som inte är bättre än flera hundra meter.

Fjärrlås

Lås enhetens skärm och ange en numerisk PIN-kod för att låsa upp den.

Fjärrtorka

Ta bort all personlig data från din främmande enhet.

Skicka varning till enheten (Scream)

Skicka ett meddelande på distans som ska visas på enhetens skärm, eller utlösa ett högt ljud som spelas upp på enhetens högtalare.

Om du tappar bort din enhet kan du låta den som hittar den veta hur de kan returnera den till dig genom att visa ett meddelande på enhetens skärm.

Om du har tappat bort din enhet och det finns en chans att den inte är långt ifrån dig (till exempel någonstans i huset eller på kontoret), vilket bättre sätt att hitta den än att få den att spela ett högt ljud? Ljudet spelas även om enheten är i tyst läge.

3.5.1. Aktivera stöldskydd

För att aktivera stöldskyddsfunktioner, slutför du helt enkelt konfigurationsprocessen från stöldskyddskortet som finns tillgängligt i instrumentpanelen.

Alternativt kan du aktivera Stöldskydd genom att följa dessa steg:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Anti-stöld**.
3. Knacka **SÄTTA PÅ**.
4. Följande procedur kommer att börja hjälpa dig att aktivera den här funktionen:

   Notera
   Ytterligare behörigheter krävs på Android 6 för stöldskyddsfunktionen.

   För att aktivera det, följ dessa steg:

   a. Knacka **Aktivera stöldskydd**, tryck sedan på **SÄTTA PÅ**.

   b. Tillåt behörigheter för **Antivirus** för att komma åt enhetens plats.

   a. **Ge administratörsrättigheter**
   Dessa privilegier är väsentliga för driften av Anti-Theft och måste därför beviljas för att fortsätta.

   b. **Ställ in program-PIN**
   För att förhindra obehörig åtkomst till din enhet måste en PIN-kod ställas in. Varje gång ett försök görs att komma åt din enhet måste PIN-koden anges först. Alternativt, på enheter som stöder fingeravtrycksautentisering, kan en fingeravtrycksbekräftelse användas istället för den konfigurerade PIN-koden.
   Samma PIN-kod används av App Lock för att skydda dina installerade appar.

   c. **Aktivera Snap Photo**
   Varje gång någon försöker låsa upp din enhet utan framgång medan Snap Photo är på, kommer Bitdefender att ta ett foto av honom.
   Mer exakt, varje gång PIN-koden, lösenordet eller fingeravtrycksbekräftelsen du ställt in för att skydda din enhet

skrivs in fel tre gånger i rad, tas ett foto med den främre kameran. Fotot sparas tillsammans med tidsstämpeln och anledningen och kan ses när du öppnar Bitdefender Mobile Security och kommer åt fönstret Stöldskydd.
Alternativt kan du se det tagna fotot i ditt Bitdefender-konto:

i. Gå till: https://central.bitdefender.com.

ii. Logga in på ditt konto.

iii. Välj **Mina enheter** panel.

iv. Välj din Android-enhet och sedan **Anti-stöld** flik.

v. Knacka ⋮ bredvid **Kontrollera dina ögonblicksbilder** för att se de senaste bilderna som togs.
Endast de två senaste fotona sparas.

När stöldskyddsfunktionen är aktiverad kan du aktivera eller inaktivera webbkontrollkommandon individuellt från stöldskyddsfönstret genom att trycka på motsvarande alternativ.

3.5.2. Använda stöldskyddsfunktioner från Bitdefender Central

> **Notera**
> Alla stöldskyddsfunktioner kräver **Bakgrundsdata** alternativet för att aktiveras i enhetens inställningar för dataanvändning.

För att komma åt stöldskyddsfunktionerna från ditt Bitdefender-konto:

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. I den **MINA ENHETER** fönstret, välj önskat enhetskort genom att trycka på motsvarande **Visa detaljer** knapp.
4. Välj **Anti-stöld** flik.
5. Tryck på knappen som motsvarar den funktion du vill använda:
Lokalisera - visa enhetens plats på Google Maps.
VISA IP - visar den senaste IP-adressen för den valda enheten.
Varna - skriv ett meddelande som ska visas på enhetens skärm och/eller få din enhet att spela ett ljudlarm.

Låsa - lås din enhet och ställ in en PIN-kod för att låsa upp den.
Torka - radera all data från din enhet.

> **Viktig**
> När du har torkat en enhet upphör alla stöldskyddsfunktioner att fungera.

3.5.3. Stöldskyddsinställningar

Om du vill aktivera eller inaktivera fjärrkommandona:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Anti-stöld**.
3. Aktivera eller inaktivera önskade alternativ.

3.6. Kontosekretess

Bitdefender-kontosekretess upptäcker om något dataintrång 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.

Automatiska omkontroller är inställda på att köras i bakgrunden, men manuella skanningar kan också köras dagligen.

Meddelanden kommer att visas varje gång nya intrång som inkluderar något av de validerade e-postkontona upptäcks.

Så här börjar du hålla personlig information säker:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Kontosekretess**.
3. Knacka **KOMMA IGÅNG**.
4. E-postadressen som används för att skapa ditt Bitdefender-konto visas och läggs automatiskt till i listan över övervakade konton.
5. För att lägga till ett annat konto, tryck på **LÄGG TILL KONTO** i fönstret Kontosekretess och skriv sedan in e-postadressen.

Knacka **LÄGG TILL** att fortsätta.
Bitdefender måste validera detta konto innan privat information visas. Därför skickas ett e-postmeddelande med en valideringskod till den angivna e-postadressen.
Kontrollera din inkorg och skriv sedan den mottagna koden i **Kontosekretess** område av din app. Om du inte hittar valideringse-postmeddelandet i mappen Inkorg, kontrollera skräppostmappen.
Sekretessstatusen för det validerade kontot visas.

Om intrång 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 brotten som Lösta. Att göra detta:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Kontosekretess**.
3. Tryck på kontot du just säkrade.
4. Tryck på intrånget du säkrade kontot för.
5. Knacka **LÖST** för att bekräfta att kontot är säkert.

När alla upptäckta överträdelser är markerade som **Löst**, kommer kontot inte längre att visas som intrång, åtminstone tills ett nytt intrång upptäcks.

Så här slutar du att meddelas varje gång automatiska skanningar görs:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Stäng av motsvarande strömbrytare i området Kontosekretess.

3.7. Applås

Installerade appar som e-post, foton eller meddelanden kan innehålla personuppgifter som du vill förbli privata genom att selektivt begränsa åtkomsten till dem.

Applås hjälper dig att blockera oönskad åtkomst till appar genom att ställa in en säkerhets-PIN-åtkomstkod. PIN-koden du anger måste vara minst 4 siffror lång, men inte mer än 8, och krävs varje gång du vill komma åt de valda begränsade apparna.

Biometrisk autentisering (som fingeravtrycksbekräftelse eller ansiktsigenkänning) kan användas istället för den konfigurerade PIN-koden.

3.7.1. Aktiverar applås

För att begränsa åtkomsten till utvalda appar, konfigurera App Lock från kortet som visas i instrumentpanelen efter aktivering av Anti-Theft.

Alternativt kan du aktivera App Lock genom att följa dessa steg:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Applås**.
3. Knacka **SÄTTA PÅ**.
4. Tillåt åtkomst till användningsdata för Bitdefender Security.
5. Tillåta **rita över andra appar**.
6. Gå tillbaka till appen, konfigurera åtkomstkoden och tryck sedan på **STÄLL IN PIN**.

   > **Notera**
   > Det här steget är endast tillgängligt om du inte tidigare har konfigurerat PIN-koden i Anti-Theft.

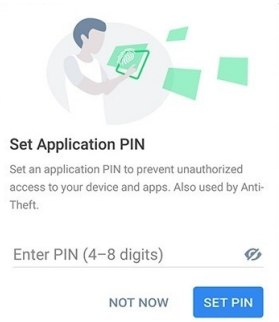
7. Aktivera alternativet Snap Photo för att fånga alla inkräktare som försöker komma åt dina privata data.

> **Notera**
> Ytterligare behörigheter krävs på Android 6 för Snap Photo-funktionen. Tillåt för att aktivera det **Antivirus** att ta bilder och spela in video.

8. Välj de appar du vill skydda.

Om du använder fel PIN-kod eller fingeravtryck fem gånger i rad, aktiveras en 30 sekunders timeout-session. På så sätt kommer alla försök att bryta sig in i de skyddade apparna att blockeras.

> **Notera**
> Samma PIN-kod används av Anti-Theft för att hjälpa dig att hitta din enhet.



3.7.2. Låsläge

Första gången du lägger till en app i App Lock visas skärmen för App Lock Mode. Härifrån kan du välja när applåsfunktionen ska skydda apparna som är installerade på din enhet.

Du kan välja mellan ett av följande alternativ:

- **Kräv upplåsning varje gång** - varje gång de låsta apparna öppnas måste PIN-koden eller fingeravtrycket som du har ställt in användas.
- **Håll olåst tills skärmen stängs av** - åtkomsten till dina appar kommer att vara giltig tills skärmen stängs av.
- **Lås efter 30 sekunder** - du kan avsluta och komma åt dina olåsta appar igen inom 30 sekunder.

Om du vill ändra den valda inställningen:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Knacka **Kräv upplåsning varje gång** i applåsområdet.
4. Välj önskat alternativ.

3.7.3. Applåsinställningar

För en avancerad konfiguration av App Lock:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.

I området för applås kan du konfigurera följande alternativ:

- **Känsligt appförslag** - få ett låsmeddelande varje gång du installerar en känslig app.
- **Kräv upplåsning varje gång** - välj ett av de tillgängliga lås- och upplåsningsalternativen.
- **Smart upplåsning** - håll appar olåsta medan du är ansluten till betrodda Wi-Fi-nätverk.
- **Slumpmässigt tangentbord** - förhindra PIN-läsning genom att slumpvisa nummerpositioner.

3.7.4. Snap Photo

Med Bitdefender Snap Photo kan du fånga dina vänner eller släktingar på hopp. På så sätt kan du utbilda deras nyfikna ögon att inte titta igenom dina personliga filer eller apparna du använder.

Funktionen fungerar enkelt: varje gång PIN-koden eller fingeravtrycksbekräftelsen du ställt in för att skydda dina appar matas in fel tre gånger i rad, tas ett foto med den främre kameran. Fotot sparas tillsammans med tidsstämpeln och anledningen, och kan ses när du öppnar Bitdefender Mobile Security och kommer åt funktionen App Lock.

> **Notera**
> Den här funktionen är endast tillgänglig för telefoner som har en främre kamera.

Så här konfigurerar du Snap Photo-funktionen för App Lock:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Aktivera motsvarande omkopplare i området Snap Photo.

Bilderna som togs när felaktig PIN-kod anges visas i App Lock-fönstret och kan visas i helskärmsläge.

Alternativt kan de ses i ditt Bitdefender-konto:

1. Gå till: https://central.bitdefender.com.
2. Logga in på ditt konto.
3. Välj **Min enhet** panel.
4. Välj din Android-enhet och sedan **Anti-stöld** flik.
5. Knacka bredvid **Kontrollera dina ögonblicksbilder** för att se de senaste bilderna som togs.

Endast de två senaste fotona sparas.

Så här slutar du ladda upp tagna foton på ditt Bitdefender-konto:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Inaktivera **Ladda upp foton** i området Snap Photo.

3.7.5. Smart upplåsning

En enkel metod för att sluta bli ombedd av App Lock-funktionen att ange PIN-koden eller fingeravtrycksbekräftelsen för de skyddade apparna varje gång du kommer åt dem är att aktivera Smart Unlock.

Med Smart Unlock kan du ställa in som betrodda Wi-Fi-nätverk du vanligtvis ansluter till, och när du är ansluten till dem kommer blockeringsinställningarna för applås att inaktiveras för de skyddade apparna.

Så här konfigurerar du Smart Unlock-funktionen:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Applås**.
3. Tryck på knapp.

4. Tryck på knappen bredvid **Smart upplåsning**, om funktionen ännu inte är aktiverad.
   Verifiera med ditt fingeravtryck eller din PIN-kod.
   Första gången du aktiverar funktionen måste du aktivera platsbehörigheten. Tryck på **TILLÅTA** knappen och tryck sedan på **TILLÅTA** igen.
5. Knacka **LÄGG TILL** för att ställa in den Wi-Fi-anslutning du använder som betrodd.

När du ändrar dig, inaktivera funktionen och de Wi-Fi-nätverk som du har angett som betrodda kommer att behandlas som opålitliga.

3.8. Rapporter

Rapportfunktionen för en detaljerad logg över händelser som rör skanningsaktiviteten på din enhet.

När något som är relevant för din enhets säkerhet händer läggs ett nytt meddelande till i rapporterna.

Så här kommer du till avsnittet Rapporter:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Rapporter**.

Följande flikar är tillgängliga i fönstret Rapporter:

- **VECKORAPPORTER** - här har du tillgång till säkerhetsstatus och utförda uppgifter från innevarande och föregående vecka. Den aktuella veckans rapport genereras varje söndag och du kommer att få ett meddelande om att den blir tillgänglig.
  Varje vecka kommer ett nytt tips att visas i det här avsnittet, så se till att du tittar in regelbundet för att få ut det bästa av appen.
  Så här slutar du ta emot aviseringar varje gång en rapport genereras:
  1. Knacka **Mer** på det nedre navigeringsfältet.
  2. Knacka **inställningar**.
  3. Inaktivera **Ny rapportavisering** växla i området Rapporter.
- **AKTIVITETS LOGG** - här kan du kontrollera detaljerad information om aktiviteten för din Bitdefender Mobile Security-app sedan den installerades på din Android-enhet.

Så här tar du bort den tillgängliga aktivitetsloggen:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Knacka **Rensa aktivitetsloggoch** tryck sedan på **KLAR**.

3.9. Bära PÅ

Med Bitdefender WearON kan du enkelt hitta din smartphone oavsett om du lämnade den på kontoret i ett konferensrum eller under en kudde i soffan. Enheten kan hittas även om det tysta läget är aktiverat.

Håll den här funktionen aktiverad för att se till att du alltid har din smartphone till hands.

Notera
Funktionen fungerar med Android 4.3 och Android Wear.

3.9.1. Aktiverar WearON

För att använda WearON behöver du bara ansluta din smartklocka till Bitdefender Mobile Security-appen och aktivera funktionen med följande röstkommando:

Start:<Var är min telefon>

Bitdefender WearON har två kommandon:

1. **Telefonvarning**
   Med funktionen Telefonvarning kan du snabbt hitta din smartphone när du går för långt bort från den.
   Om du har din smartklocka med dig känner den automatiskt av appen på din telefon och vibrerar när du går för långt från telefonen, mer exakt när Bluetooth-anslutningen tappas.
   För att aktivera den här funktionen, öppna Bitdefender Mobile Security, tryck på **Globala inställningar** i menyn och välj motsvarande omkopplare under WearON-sektionen.
2. **Skrika**
   Att hitta din telefon har aldrig varit enklare. När du glömmer var du lämnade telefonen trycker du på kommandot Scream på klockan för att få telefonen att skrika.

3.10. Handla om

För att hitta information om Bitdefender Mobile Security-versionen som du har installerat, för att komma åt och läsa prenumerationsavtalet och integritetspolicyn, och se Open-source-licenserna:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Tryck på önskat alternativ i området Om.

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 Android
  - Bitdefender Mobile Security för iOS
  - Bitdefender Windows produktlinje
  - Bitdefender Antivirus för Mac
- Hantera och förnya dina Bitdefender-prenumerationer.
- Lägg till nya enheter i ditt nätverk och hantera dem var du än är.
- Skydda nätverksenheterna och deras data mot stöld eller förlust med Anti-stöld.

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:

   - **Authenticator App** - 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 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

Varför kräver Bitdefender Mobile Security en internetanslutning?

Appen måste kommunicera med Bitdefender-servrar för att fastställa säkerhetsstatusen för apparna som den skannar och för webbsidorna du besöker, och även för att ta emot kommandon från ditt Bitdefender-konto när du använder stöldskyddsfunktionerna.

Vad behöver Bitdefender Mobile Security varje behörighet för?

- Internetåtkomst -> används för molnkommunikation.
- Läs telefonstatus och identitet -> används för att upptäcka om enheten är ansluten till internet och för att extrahera viss enhetsinformation som behövs för att skapa ett unikt ID när du kommunicerar med Bitdefender-molnet.
- Läs och skriv webbläsarbokmärken -> Webbskyddsmodulen tar bort skadliga webbplatser från din webbhistorik.
- Läs loggdata -> Bitdefender Mobile Security upptäcker spår av hotaktiviteter från Android-loggarna.
- Plats -> krävs för fjärrplats.
- Kamera -> krävs för Snap-foto.
- Lagring -> används för att tillåta skannern för skadlig programvara att kontrollera SD-kortet.

Hur kan jag sluta skicka information till Bitdefender om misstänkta appar?

Som standard skickar Bitdefender Mobile Security rapporter till Bitdefender-servrar om de misstänkta appar som du installerar. Denna information är viktig för att förbättra hotupptäckten och kan hjälpa oss att erbjuda dig en bättre upplevelse i framtiden. Om du vill sluta skicka information om misstänkta appar till oss:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Stäng av **Detektering i molnet** i området Malware Scanner.

Var kan jag se detaljer om appens aktivitet?

Bitdefender Mobile Security för en logg över alla viktiga åtgärder, statusändringar och andra viktiga meddelanden relaterade till dess aktivitet. För att komma åt se om appens aktivitet:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Rapporter**.
   I fönstret VECKRAPPORTER kan du komma åt rapporterna som genereras varje vecka och i fönstret AKTIVITETSLOGG kan du se information om aktiviteten i din Bitdefender-app.

Jag glömde PIN-koden som jag ställde in för att skydda min app. Vad gör jag?

1. Tillgång Bitdefender Central.
2. Välj **Mina enheter** panel.
3. Tryck på önskat enhetskort och tryck sedan på i det övre högra hörnet av skärmen.
4. Välj **inställningar**.
5. Hämta PIN-koden från **Applikations-PIN** fält.

Hur kan jag ändra PIN-koden jag ställer in för applås och stöldskydd?

Om du vill ändra PIN-koden du ställer in för applås och stöldskydd:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **inställningar**.
3. Tryck på Säkerhet **PINKOD** i stöldskyddsområdet.
4. Skriv in den aktuella PIN-koden.
5. Skriv in den nya PIN-koden du vill ställa in.

Hur kan jag stänga av applåsfunktionen?

Det finns inget avstängningsalternativ för applåsfunktionen, men du kan enkelt inaktivera den genom att avmarkera kryssrutorna bredvid de valda apparna efter att ha validerat PIN-koden eller fingeravtrycket du har angett.

Hur kan jag ställa in ett annat trådlöst nätverk som tillförlitligt?

Först måste du ansluta din enhet till det trådlösa nätverk du vill ställa in som betrodd. Följ sedan dessa steg:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Knacka **Applås**.
3. Knacka i det övre högra hörnet.
4. Knacka **LÄGG TILL** bredvid nätverket du vill ställa in som tillförlitligt.

Hur kan jag sluta se tagna bilder tagna på mina enheter?

Så här slutar du göra synliga foton som tagits på dina enheter:

1. Tillgång Bitdefender Central.
2. Knacka i den övre högra sidan av skärmen.
3. Knacka **inställningar** i bildmenyn.
4. Inaktivera **Visa/visa inte snapbilder tagna på dina enheter** alternativ.

Hur kan jag hålla min onlineshopping säker?

Online shopping kommer med höga risker när vissa detaljer ignoreras. För att inte bli offer för bedrägeri rekommenderar vi följande:

- Håll din säkerhetsapp uppdaterad.
- Skicka onlinebetalningar endast med köparskydd.
- Använd ett VPN när du ansluter till internet från offentliga och osäkra trådlösa nätverk.
- Var uppmärksam på lösenorden du har tilldelat dina onlinekonton. De måste vara starka inklusive stora och små bokstäver, siffror och symboler (@, !, %, #, etc.).
- Se till att informationen du skickar är över säkra anslutningar. Webbplatstillägget online måste vara HTTPS:// och inte HTTP://.

När ska jag använda Bitdefender VPN?

Du måste vara försiktig när du använder, laddar ner eller laddar upp innehåll på internet. För att se till att du är säker när du surfar på webben rekommenderar vi att du använder Bitdefender VPN när du:

- vill ansluta till offentliga trådlösa nätverk
- vill komma åt innehåll som normalt är begränsat i specifika områden, oavsett om du är hemma eller utomlands

- vill hålla dina personuppgifter privata (användarnamn, lösenord, kreditkortsinformation, etc.)
- vill dölja din IP-adress

Kommer Bitdefender VPN att ha en negativ inverkan på batteritiden för min enhet?

Bitdefender VPN är utformad för att skydda dina personliga data, dölja din IP-adress när du är ansluten till osäkra trådlösa nätverk och komma åt begränsat innehåll i vissa länder. För att undvika onödig batteriförbrukning av din enhet rekommenderar vi att du bara använder VPN när du behöver det och kopplar bort när du är offline.

Varför stöter jag på internetnedgångar när jag är ansluten till Bitdefender VPN?

Bitdefender VPN är designad för att erbjuda dig en lätt upplevelse när du surfar på webben; din internetanslutning eller serveravståndet du ansluter till kan dock orsaka nedgången. I det här fallet, om det inte är ett måste att ansluta från din plats till en fjärransluten server (t.ex. från USA till Kina), rekommenderar vi att du tillåter Bitdefender VPN att automatiskt ansluta dig till närmaste server, eller hitta en server närmare din nuvarande plats.

Kan jag ändra Bitdefender-kontot som är länkat till min enhet?

Ja, du kan enkelt ändra Bitdefender-kontot som är länkat till din enhet genom att följa dessa steg:

1. Knacka **Mer** på det nedre navigeringsfältet.
2. Tryck på din e-postadress.
3. Knacka **Logga ut från ditt konto**. Om en PIN-kod har ställts in, uppmanas du att ange den.
4. Bekräfta ditt val.
5. Skriv in e-postadressen och lösenordet för ditt konto i motsvarande fält och tryck sedan på **LOGGA IN**.

Hur kommer Bitdefender Mobile Security att påverka min enhets prestanda och batteriautonomi?

Vi håller effekten väldigt låg. Appen körs bara när det är nödvändigt – efter att du installerat en app, när du surfar i appens gränssnitt eller när du vill ha en säkerhetskontroll. Bitdefender Mobile Security körs inte

i bakgrunden när du ringer dina kompisar, skriver ett meddelande eller spelar ett spel.

Vad är enhetsadministratör?

Enhetsadministratör är en Android-funktion som ger Bitdefender Mobile Security de behörigheter som behövs för att utföra vissa uppgifter på distans. Utan dessa privilegier skulle fjärrlås inte fungera och enhetsrensning skulle inte kunna ta bort dina data helt. Om du vill ta bort appen, se till att återkalla dessa privilegier innan du försöker avinstallera från **Inställningar > Säkerhet > Välj enhetsadministratörer**.

Så här fixar du felet "Inget Google Token" som visas när du loggar in på Bitdefender Mobile Security.

Det här felet uppstår när enheten inte är kopplad till ett Google-konto, eller när enheten är kopplad till ett konto men ett tillfälligt problem hindrar den från att ansluta till Google. Prova någon av följande lösningar:

- Gå till Android-inställningar > Applikationer > Hantera applikationer > Bitdefender Mobile Security och tryck på **Radera data**. Försök sedan logga in igen.
- Se till att din enhet är kopplad till ett Google-konto.
  För att kontrollera detta, gå till Inställningar > Konton och synkronisering och se om ett Google-konto är listat under **Hantera konton**. Lägg till ditt konto om ett inte finns med i listan, starta om din enhet och försök sedan logga in på Bitdefender Mobile Security.
- Starta om enheten och försök sedan logga in igen.

På vilka språk är Bitdefender Mobile Security tillgängligt?

Bitdefender Mobile Security är för närvarande tillgängligt på följande språk:

- brasiliansk
- tjeckiska
- holländska
- engelsk
- franska
- tysk
- grekisk

- ungerska
- italienska
- japanska
- koreanska
- putsa
- portugisiska
- rumänska
- ryska
- spanska
- svenska
- Thai
- turkiska
- vietnamesiska

Andra språk kommer att läggas till i framtida utgåvor. För att ändra språket för Bitdefender Mobile Security-gränssnittet, gå till din enhets **Språk & tangentbord** inställningar och ställ in enheten på det språk du vill använda.

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 46).

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.