ANVÄNDARMANUAL

Bitdefender CONSUMER SOLUTIONS

SecurePass

Bitdefender SecurePass

Användarmanual

Publication date 20/11/2024

Rättsligt meddelande

Bitdefender

Innehållsförteckning

OM DEN HÄR GUIDEN

Syfte och avsedd målgrupp

Den här guiden är avsedd för alla Bitdefender-användare på alla operativsystem som stöds (Windows, MacOS, Android, iOS) som har valt Bitdefender SecurePass som deras go-to lösenordshanteringsverktyg. Informationen som presenteras i den här boken är inte bara lämplig för datorvana, utan den fungerar som en tillgänglig och vänlig guide för alla.

Den här guiden hjälper dig att ta reda på hur du får ut det bästa av vår ultrasäkra och funktionsrika lösenordshanterare genom att diskutera alla dess funktioner och funktioner i detalj.

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 SecurePass och installationsprocessen.

Importera och exportera dina lösenord (sida 9)

Förstå hur du kan importera eller exportera lösenord in och ut ur SecurePass.

Funktioner och funktioner (sida 12)

Lär dig hur du använder Bitdefender SecurePass och alla dess funktioner.

Få hjälp (sida 24)

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 SECUREPASS

Bitdefender SecurePass är en multiplattformstjänst utformad för att hjälpa användare att lagra och organisera alla sina onlinelösenord. Den är byggd med de starkaste kända kryptografiska algoritmerna för högsta nivå av säkerhet och digital säkerhet. Det fungerar som en webbläsartillägg och mobilappslösning för identitets- och lösenordshantering, banktjänster och all annan typ av känslig information över enheter.

Bitdefender SecurePass kan automatiskt spara, autofyll, automatiskt generera och hantera dina lösenord för alla webbplatser och onlinetjänster med hjälp av ett enda huvudlösenord, vilket gör din övergripande digitala identitet mycket lättare att hantera.

1.1. Lösenordshanteraren testversion och betalversioner

Testversionen av Bitdefender Password Manager fungerar av alla konton som är identiska med den betalda versionen av produkten, men dess tillgänglighet kommer att upphöra efter 90 dagar efter aktiveringen.

Notera

Observera att den betalda versionen av produkten, även om den kan köpas som en helt fristående produkt, är obegränsad tillgång till Password Manager inkluderad i prenumerationerna 'Bitdefender Premium Security och Bitdefender Ultimate Security.

2. KOMMA IGÅNG

2.1. Systemkrav

Du kan använda den senaste versionen av Bitdefender SecurePass endast på enheter som kör följande operativsystem:

- **För PC-användare:**
  - Windows 7 med Service Pack 1
  - Windows 8.1
  - Windows 10
  - Windows 11
- **För macOS-användare:**
  - macOS 10.14 (Mojave) och senare macOS-operativsystem

  Notera
  Observera att systemprestanda kan påverkas på enheter som har gamla generationens processorer.
- **För iOS-användare:**
  - iOS 11.0 eller senare iOS operativsystem
- **För Android-användare:**
  - Android 5.1 och senare Android-operativsystem

  Notera
  - Funktionen för upplåsning av fingeravtryck stöds på **Android 6.0** och senare.
  - Autofyll-funktionen stöds på **Android 8.0** och senare, kompatibel med iPhone, iPad och iPod touch.

2.1.1. Programvarukrav

För att kunna använda Bitdefender SecurePass och alla dess funktioner måste dina Windows- eller macOS-enheter uppfylla följande programvarukrav:

- **Microsoft Edge** (baserat på Chromium 80 och senare)
- **Mozilla Firefox** (version 65 eller senare)
- **Google Chrome** (version 72 eller senare)
- **Safari** (version 12 eller senare)

Notera
Programvarukraven gäller inte för Android och iOS.

Varning
Underlåtenhet att uppfylla systemkraven som presenteras ovan kommer att resultera i antingen oförmåga att installera Bitdefender SecurePass eller fel på produkten.

2.2. Installation

Det här kapitlet kommer att vägleda dig om hur du installerar Bitdefender SecurePass till både webbläsarna på din Windows-dator och macOS, såväl som på dina mobila Android- eller iOS-enheter.

Viktig
Innan installationen, se till att du har en giltig Password Manager-prenumeration i din Bitdefender Central konto så att det här webbläsartillägget kan hämta sin giltighet från ditt konto.

Aktiva prenumerationer listas i **mina prenumerationer** avsnitt inom Bitdefender Central.

2.2.1. Installerar på Windows- och macOS-enheter

Till skillnad från de flesta stationära applikationer och mjukvara som måste installeras och konfigureras på dessa enheter, kommer Bitdefender Password Manager som ett webbläsartillägg - även kallat ett tillägg - som snabbt kan läggas till och aktiveras i din föredragna webbläsare.

De webbläsare som för närvarande stöds för produkten är följande: **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge**, och **Safari**.

- **Google Chrome**
- **Mozilla Firefox**
- **Microsoft Edge**

Safari

Så här installerar du Bitdefender SecurePass:

1. När du har köpt Bitdefender SecurePass följer du stegen i bekräftelsemeddelandet för att aktivera din prenumeration.
2. Logga in på Bitdefender Central med dina inloggningsuppgifter.
   På menyn till vänster väljer du **SecurePass**.
3. Välj önskad webbläsare i SecurePass-panelen.
4. Installera webbläsartillägget:

   - **Google Chrome:**
     a. Klicka på **Lägg till i Chrome** knapp.
     b. Klicka på i bekräftelserutan **Lägg till tillägg**.

   - **Mozilla Firefox:**
     a. Klicka på **Lägg till i Firefox** knapp.
     b. Klicka på **Installera** knappen längst upp till höger på skärmen.

   - **Microsoft Edge:**
     a. Klicka på **Skaffa** knapp.
     b. Klick **Lägg till tillägg** i prompten som visas.

   - **Safari:**
     a. Installationsprogrammet för SecurePass laddas ner på din macOS-enhet. Dubbelklicka på den nedladdade filen och följ instruktionerna på skärmen därifrån.
     b. I slutet av installationsprocessen öppnar du **Safari** webbläsare och välj **Inställningar** i den övre menyraden.
     c. I fönstren Inställningar klickar du på **Fliken Tillägg**.
     d. Markera rutan bredvid **Bitdefender SecurePass** för att möjliggöra det.

När tillägget är installerat kan du gå vidare till Inställningsprocess (sida 7).

2.2.2. Installerar på Android-enheter

Den enklaste metoden för att installera Bitdefender Password Manager för Android-telefoner och surfplattor är att ladda ner applikationen direkt från Google Play.

1. Innan något annat, efter köpet, se till att öppna bekräftelsemeddelandet du fick för att följa instruktionerna där för att aktivera din SecurePass-prenumeration.
2. Öppna Google Play Store på din Android-enhet.
3. Skriv i Google Play Stores sökfält **Bitdefender SecurePass**, hitta och ladda ner programmet.
4. När nedladdningen är klar öppnar du appen och följer vid behov konfigurationsstegen på skärmen för att slutföra installationsprocessen.

Installationen på din Android-enhet är nu klar.

2.2.3. Installerar på iOS-enheter

Den enklaste metoden för att installera Bitdefender Password Manager för iOS- och iPadOS-enheter är att ladda ner programmet från Apple App Store.

1. Innan något annat, efter köpet, se till att öppna bekräftelsemeddelandet du fick för att följa instruktionerna där för att aktivera din SecurePass-prenumeration.
2. Öppna App Store på din iOS-enhet.
3. Skriv i App Stores sökfält **Bitdefender SecurePass**, hitta och ladda ner programmet.
4. När nedladdningen är klar öppnar du appen och följer vid behov konfigurationsstegen på skärmen för att slutföra installationsprocessen.

Installationen på din iOS / iPadOS-enhet är nu klar!

2.3. Inställningsprocess

Så här ställer du in Bitdefender SecurePass på din webbläsare/mobila enhet:

1. När du har slutfört installationsprocessen öppnar du SecurePass-tillägget/programmet och loggar in.
   Använd autentiseringsuppgifterna för Bitdefender-kontot som är kopplat till din SecurePass-prenumeration.
2. Du kommer att uppmanas att skapa en **Huvudlösenord**.

   Viktigt
   Observera att du behöver detta huvudlösenord för att låsa upp alla lösenord, kreditkortsinformation och anteckningar som sparats i Bitdefender SecurePass. Detta är i huvudsak nyckeln som gör det möjligt för ägaren att använda den här produkten.

   Se till att ange ett starkt huvudlösenord utan risk för att du lätt glömmer det.
   När du har bestämt dig för ett starkt och unikt huvudlösenord klickar du på **Spara och fortsätt**.
3. Därefter kommer du att förses med en **Återställningsnyckel**.

   Varning
   När du skapar huvudlösenordet får du en **24-siffrig återställningsnyckel**. Anteckna din återställningsnyckel på ett säkert ställe och tappa inte bort den. Den här nyckeln är det enda sättet att komma åt dina lösenord som sparats i Password Manager om du råkar **glöm huvudlösenordet** tidigare konfigurerat för ditt konto.

   - Spara återställningsnyckeln genom att kopiera den till ditt urklipp eller ladda ner den som en PDF-fil.
     Du kan trycka **Stäng** när det är klart.
4. När du är klar väljer du **Åtkomst till ditt valv** knapp.

Nu när installationsprocessen är klar kan du börja använda Bitdefender SecurePass.

3. IMPORTERA OCH EXPORTERA DINA LÖSENORD

Bitdefender Password Manager är byggd på ett sådant sätt att det effektivt underlättar kommunikation och dataöverföring med externa källor, plattformar och mjukvaruverktyg. Detta är den centrala anledningen till att det mycket vanliga behovet av att importera eller exportera lösenord till eller ut ur Bitdefender Password Manager kan tillfredsställas med lätthet.

3.1. Kompatibilitet

Bitdefender Password Manager kan sömlöst överföra data från följande lista med applikationer:

- Bitdefender Lösenordshanterare
- Bitdefender Plånbok
- Bitdefender SecurePass
- Säkrare pass
- 1Lösenord
- Kaspersky
- Dashlane
- Chrome-webbläsare
- Firefox-webbläsare
- Microsoft Edge
- Bitwarden
- Lastpass
- KeePass
- RoboForm

Denna överföring av data mellan Bitdefender Password Manager och annan programvara för kontohantering kan göras genom följande dataformat:

CSV, **JSON**, **XML**, **Text**, **1pif** och **FSK**.

3.2. Importerar till lösenordshanteraren

Bitdefender Password Manager låter dig enkelt importera lösenord från andra lösenordshanterare och webbläsare. Om du för närvarande funderar på att byta till Bitdefender Password Manager från en annan lösenordshanteringstjänst, har du med största sannolikhet lagrat en stor mängd referenser som användarnamn, lösenord och annan inloggningsinformation som krävs för alla dina konton.

Nu när du har valt Bitdefender Password Manager kommer du att leta efter att importera den sparade informationen till den.

Så här importerar du din lagrade information från andra appar och webbläsare till Bitdefender Password Manager, **oavsett operativsystem** där du har valt att installera denna produkt:

1. Öppna Bitdefender SecurePass och gå till **Inställningar**.
   - I webbläsaren:
     Klicka på **Inställningar** längst upp till höger på sidan.
   - I appen:
     Tryck på **Mer** knappen längst ner till höger på skärmen och, högst upp i listan som visas efteråt, tryck på **Inställningar**.
2. I **Säkerhetskopiering och återställning** sektion, välj **Importera lösenord**. Importfönstret öppnas.
3. Välj namnet på lösenordshanteraren eller webbläsaren du har använt tidigare från rullgardinsmenyn som är tillgänglig via **Välj filtyp** fält.

   > **Anmärkning**
   > Om ett lösenord användes för att kryptera filen måste du ange det i **Lösenord** fält; annars kan du lämna det tomt.

4. Välj **Välj fil som ska importeras** arkiverad.
   Navigera till den plats där de exporterade data som tillhör din gamla lösenordshanterare har sparats. Välj filen när du hittar den och klicka sedan på **Öppna**.
5. När du har valt filen väljer du **Importera** i det nedre vänstra hörnet av importfönstret. Processen börjar inom kort, åtföljd av en förloppsindikator.

När de har importerats kommer dina lösenord att vara tillgängliga på alla enheter där Bitdefender Password Manager-applikationen eller webbläsartillägget är installerat.

> **Anmärkning**
> När du går tillbaka till ditt lösenordsvalv i SecurePass kommer du att märka en mapp som heter **Importera**, som innehåller all data från din tidigare lösenordshanterare eller webbläsare.

3.3. Exporterar från Password Manager

Bitdefender Password Manager låter dig enkelt exportera dina sparade lösenord (inklusive kontoinloggningsuppgifter, säkra anteckningar etc.) till en CSV-fil (kommaseparerade värden) eller en krypterad fil om du någonsin vill byta till en annan lösenordshanterartjänst, så att din avgång från Bitdefender Password Manager inte kommer att vara en svår process.

> **Viktig**
> En CSV-fil är **inte** krypterad och innehåller användarnamn och lösenord i vanlig textformat, vilket innebär att din privata information kan läsas av alla som har tillgång till din enhet. Vi rekommenderar därför att du följer instruktionerna nedan på en betrodd enhet.

Så här kan du exportera dina data från Bitdefender Password Manager:

1. Öppna Bitdefender SecurePass och gå till **Inställningar**.
   - I webbläsaren:
     Klicka på **Inställningar** längst upp till höger på sidan.
   - I appen:
     Tryck på **Mer** knappen längst ner till höger på skärmen och, högst upp i listan som visas efteråt, tryck på **Inställningar**.
2. I **Säkerhetskopiering och återställning** sektion, välj **Exportera lösenord**. Exportfönstret öppnas.
3. Klicka på **Välj filtyp**. Från rullgardinsmenyn väljer du att exportera dina data i antingen ett JSON-format eller ett CSV-format. Du kan också ange ett lösenord för att skydda den exporterade filen.
   Markera motsvarande ruta om du också vill inkludera delade objekt.
4. Klick **Exportera** i det nedre vänstra hörnet av exportfönstret och spara den exporterade filen på din enhet.

4. FUNKTIONER OCH FUNKTIONER

Det här kapitlet tar dig igenom alla funktioner och funktioner i Bitdefender Password Manager, förklarar deras användbarhet och hur du använder dem mest effektivt.

4.1. Spara lösenord manuellt

Du kan säkert lagra information som lösenord, referenser och andra, till exempel kreditkortsinformation eller anteckningar i Bitdefender SecurePass manuellt, på följande sätt:

1. Öppna Bitdefender SecurePass
2. I **Mitt valv** fliken, tryck på **+Lägg till objekt** knapp.
3. Välj den objekttyp du vill lägga till. (konto, kreditkort, identitet eller anteckning).
4. Fyll i de obligatoriska fälten beroende på det valda objektet.
5. När du har slutfört alla nödvändiga uppgifter, spara objektet för att lägga till det i ditt SecurePass-valv.

4.2. Lösenordsgenerator

Bitdefender SecurePass innehåller en lösenordsgenereringsfunktion som kan hjälpa till med skapandet av säkra lösenord.

För att komma åt och använda lösenordsgeneratorn:

1. Öppna Bitdefender SecurePass och få tillgång till **Skapa lösenord** fliken på vänster sida av skärmen. Detta tar dig till lösenordsgeneratorn integrerad i SecurePass
2. Anpassa lösenordet som du ska generera enligt dina egna behov och preferenser.
   - Lösenordslängd: Dra skjutreglaget för att bestämma vilken längd som helst mellan 8 och 32 tecken.
   - Stora och små bokstäver: Välj vilka - eller båda - typer av bokstäver du vill lägga till för komplexitetsnivån för ditt lösenord.
   - Siffror: Om du markerar den här rutan kommer siffror att inkluderas i teckensträngen som innehåller ditt lösenord.

- Specialtecken: Lägg till symboler i ditt lösenord för att förbättra lösenordets komplexitet.

> **Anmärkning**
> Tryck på **Spara inställningar** knappen för SecurePass för att komma ihåg dem och alltid generera lösenord baserat på de inställningar du sparat.

3. Skapa ett nytt lösenord genom att klicka på den cirkulära pilikonen som finns under det lösenord som visas för närvarande. Varje klick genererar en ny teckensträng.
4. När du är nöjd med det genererade lösenordet kan du antingen kopiera det till ditt urklipp eller klicka på **Spara konto** knappen för att lagra den i ditt valv (genom koppling till annan kontoinformation).

> **Anmärkning**
> Du kan också snabbt skapa ett lösenord **direkt från registreringsformulär** genom att klicka på Bitdefender SecurePass-ikonen som finns i lösenordsfältet på registreringssidan. Genom att klicka på den kan du sedan välja **Generera lösenord** alternativ.

4.3. Kontroll av lösenordsstyrka

Bitdefender SecurePass erbjuder möjligheten att utvärdera styrkan hos sparade lösenord och känsliga data. Detta är en viktig funktion för att utvärdera och bedöma eventuella sårbarheter för din datasekretess och säkerhet.

Så här kontrollerar du styrkorna hos lagrade lösenord:

1. Öppna Bitdefender SecurePass och välj i e-postmenyn **Säkerhetsrapport** flik.
   Fliken Säkerhetsrapport är uppdelad i fyra avsnitt: intrång, svag, gammal och dubblett.
2. Antalet lösenord som faller i var och en av de fyra kategorierna visas på skärmen.
   Dessutom, genom att gå igenom listan över lagrade lösenord, kommer varje lösenord att taggas med den kategori som det ligger under.

För att förstå innebörden bakom dessa säkerhetsnivåer följer nedan några korta detaljer om var och en av dem:

- Brottna lösenord: Om någon av dina inloggningsuppgifter har varit en del av ett dataintrång kommer de att listas under **kränkt** sektion.

> **Anmärkning**
> För att kontrollera om något av dina lösenord har äventyrats och läckt ut genom dataintrång, klicka på **Kör säkerhetsgenomsökning** knapp.

- Svaga lösenord: SecurePass identifierar och flaggar **svag** lösenord lagrade i ditt valv baserat på en intern, lokalt körande algoritm som tittar på olika kriterier som lösenordslängd, olika tecken och inkludering av siffror eller versaler bland andra faktorer.
- Gamla lösenord: Lösenord som har sparats och omodifierats under en längre period än sex månader kommer att flaggas som **gammal**.
- Duplicerade lösenord: Med tanke på att användning av samma lösenord på flera plattformar och konton utgör en stor säkerhetsrisk, kommer SecurePass att flagga lösenord som används på mer än ett ställe som **dubblera**.

4.4. Dataorganisation

Inom Bitdefender SecurePass kan du organisera och därmed lättare hantera alla dina sparade objekt.

Du kan kategorisera dina objekt i specifika mappar för enkel åtkomst genom att följa dessa steg:

1. Öppna Bitdefender SecurePass och gå till **Mitt valv**. Klicka här på **Lägg till mapp** knapp.
2. Namnge mappen och tryck på **Skapa** knapp.
   Den nya mappen visas nu i ditt valv.

Så här flyttar du objekt till den skapade mappen:

1. Klicka på ett konto du vill flytta och tryck på **Redigera** knapp.
2. Tryck på den plats som visas bredvid **Spara objekt i** och välj mappnamnet från rullgardinsmenyn.
3. Tryck på **Spara konto** knapp.

Kontot lagras nu i den valda mappen.

4.5. Intelligent autofyllning

Bitdefender SecurePass låter dig fylla i kontouppgifter och information automatiskt på alla Sing-In-formulär online.

> **Anmärkning**
> Som webbläsartillägg, på antingen Windows eller macOS, bör Autofyll-funktionen fungera sömlöst.

4.5.1. Autofyll på Android

Så här konfigurerar du SecurePass på Android för att använda Autofyll:

1. Öppna Bitdefender SecurePass-appen på din Android-enhet.
2. Tryck på **Mer** menyknapp.
3. Överst på skärmen trycker du på **Inställningar**.
4. Knacka på **Gör detta till din standardlösenordshanterare**
5. Aktivera Bitdefender SecurePass i listan Autofyll-tjänster.

> **Anmärkning**
> Du kan också gå till inställningarna för din Android-enhet, i **Lösenord och konton** > **Autofylltjänst** > aktivera Bitdefender SecurePass.
>
> För Android 11 eller tidigare versioner av operativsystemet är inställningarna: **Systemet** > **Språk och inmatning** > **Avancerad**.

6. Knacka **OK**.

När denna konfiguration är klar, när du trycker på ett inloggningsfält, kommer ett alternativ som heter Bitdefender SecurePass att visas på din skärm. Du kan trycka på den för att öppna appen. Logga in på SecurePass och dina referenser kommer automatiskt att fyllas

4.5.2. Autofyll på iOS

Så här konfigurerar du SecurePass på din iOS-enhet för att använda Autofyll:

1. Öppna **Inställning** app på din iPhone eller iPad och välj **Allmänt**.

2. Knacka på **Autofyll och lösenord**. Säkerställ alternativet **Autofyll lösenord och lösennycklar** eller **Autofyll lösenord** - beroende på iOS-versionen - är påslagen.
3. I **Autofyllformulär** lista, aktivera **Bitdefender SecurePass** ansökan.

När denna konfiguration är klar, när du trycker på ett inloggningsfält, kommer ett alternativ som heter Bitdefender SecurePass att visas på din skärm. Du kan trycka på den för att öppna appen. Logga in på SecurePass och dina referenser kommer automatiskt att fyllas

4.5.3. Autofyllkortuppgifter

Medan SecurePass ger en lättillgänglig ikon för automatisk fyllning av inloggningsuppgifter och lösenord, fungerar funktionen Autofyll för kreditkortsinformation annorlunda:

1. Navigera till betalnings- eller kassasidan på webbplatsen där du vill använda din lagrade kreditkortsinformation.
2. Högerklicka på ett tomt område på betalningssidan. Detta kommer att uppmana den sammanhangsberoende menyn att visas på skärmen.
3. Välj Bitdefender SecurePass från menyn genom att hålla muspekaren över alternativet. Detta öppnar en undermeny med ytterligare alternativ
4. Välj **Fyll i kreditkortsinformation automatiskt**. Detta visar en lista över alla kreditkort som du har lagrat i SecurePass-
5. Välj önskat kort.

På detta sätt kommer SecurePass automatiskt att fylla i betalningsformuläret med uppgifterna om det kreditkort du valt.

5. ANVÄND SOM EN 2FA-APPLIKATION

Du kan alltid välja att använda Bitdefender SecurePass som en tvåfaktorsautentiseringsapp för vilken webbplats eller plattform du vill, och hantera dina 2FA-koder tillsammans med dina lösenord på följande sätt:

1. Gå till säkerhetsinställningarna på webbplatsen eller applikationen där du vill aktivera 2FA-funktionen. Vanligtvis kommer du att presenteras med en QR-kod eller en verifieringskod under processen.
2. Starta Bitdefender SecurePass och öppna motsvarande konto du vill konfigurera för 2FA-användning. Klicka på **Redigera** knapp.
3. Bläddra till botten av kontoinmatningssidan i SecurePass och tryck på **Tvåfaktorsautentisering** alternativ.
4. Skanna QR-koden eller ange koden manuellt.
   När detta är gjort kommer SecurePass att bekräfta den framgångsrika tvåfaktorsautentiseringsinställningen.
5. Därefter trycker du på den nya **Visa kod** knappen är nu synlig i gränssnittet. En tidskänslig kod visas där
6. Gå tillbaka till kontot där du aktiverade 2FA-funktionen och mata in koden från Bitdefender SecurePass för att verifiera din installation.

När du har slutfört denna installationsprocess trycker du på **Spara konto** knappen i SecurePass för att slutföra processen.

Från och med nu, när du sjunger in på plattformen som du har ställt in 2FA-funktionen för, kommer du att uppmanas att använda SecurePass 2FA-koder för respektive konto, vilket erbjuder ett nytt säkerhetslager för kontot i fråga.

6. DELA DATA

Bitdefender SecurePass kommer med möjligheten att dela känslig information säkert, till exempel referenser, lösenord eller kreditkortsuppgifter.

Du kan använda delningsfunktionen via länkar:

1. Välj ett objekt som lagras i ditt valv.
   - I webbläsaren:
     Gå till ditt valv och klicka på objektet du vill dela. Klicka på menyn med tre punkter på höger sida och välj **Dela länk**.
   - I appen:
     Gå till ditt valv och tryck på objektet du vill dela. Klicka på länksikonen och välj **Skapa delningslänk** alternativ.
2. Skapa länken Dela genom att ange:
   - Länkens utgångsdatum.
   - Användningsgränsen.
   - Huruvida länken ska vara lösenordsskyddad eller inte.
3. När den har genererats kopierar du den genererade länken och skickar den till den avsedda mottagaren.

6.1. Dela med grupper

Grupper skapas för att göra datadelning ännu enklare. Du kan skapa olika grupper inom Bitdefender SecurePass med andra användare för att säkert dela

1. Skapa en grupp:
   - Gå till **Grupper** och tryck på **Skapa grupp** knappen på fliken Grupper.
   - Ange ett gruppnamn och tryck sedan på **Skapa grupp** knapp.
2. Lägg till objekt i grupper:
   - I webbläsaren:

Gå till ditt valv och klicka på objektet du vill dela. Klicka på menyn med tre punkter till höger om objektet och välj **Lägg till i grupp**.

- I appen:
  Gå till ditt valv och klicka på objektet du vill dela. **Dela med gruppen** alternativ.

Välj den grupp du vill dela objektet med.

3. Ställ in åtkomsträttigheterna (läs, skriva, bevilja) baserat på den kontrollnivå du vill ge gruppmedlemmar.
4. Tryck **Spara**, sedan **Utfört**.

Du och gruppmedlemmarna kan granska delade objekt i gruppens avsnitt.

6.2. Hantera grupper

I **Grupper** delen av Bitdefender SecurePass kan du granska alla skapade grupper och hantera dem baserat på dina behov:

- Byt namn på grupper.
- Redigera medlemmar. (bjuda in nya medlemmar, tilldela rättigheter till specifika medlemmar, bevilja admin- eller delningsrättigheter och ta bort befintliga medlemmar)
- Lämna grupper.
- Ta bort grupper.

7. LÅS KONTO

Bitdefender SecurePass levereras med en **Lås konto** funktion som omedelbart låser ditt konto och avslutar alla aktiva sessioner på alla enheter som har tillgång till det. Den här funktionen är särskilt praktisk när misstankar om obehörig åtkomst uppstår.

Så här låser du ditt SecurePass-konto:

1. Öppna Bitdefender SecurePass.
2. En gång i SecurePass:
   - I webbläsaren:
     Klicka på **Inställningar** längst upp till höger på sidan.
   - I mobilappen:
     Tryck på **Säkra mig** menyknapp.
3. Tryck på **Lås konto** knappen för att logga ut direkt från alla enheter och avsluta pågående sessioner.

8. VANLIGA FRÅGOR

Några vanliga frågor om Bitdefender Password Manager tenderar att återkomma. Vi har svaren! Här kan du lära dig mer om ditt Bitdefender-konto, import av lösenord, datasäkerhetsprotokoll och andra ämnen som är viktiga för våra kunder.

Allmänna frågor om Bitdefender Password Manager

Vad händer när Bitdefender Password Manager löper ut?

När din Password Manager-prenumeration löper ut och inte längre är aktiv har du högst 90 dagar på dig att exportera dina lösenord. Dina lösenord kommer att säkerhetskopieras i ytterligare 30 dagar. Under dessa 90 dagar kommer du bara att kunna exportera dina data. Du kan inte fortsätta använda lösenordshanteraren. Autofyll-funktionen slutar fungera, liksom möjligheten att generera lösenord.

I slutet av den 90-dagars respitperioden har du 30 extra dagar på dig att kontakta Bitdefender-supporten och begära att återställa dina lösenord till livedatabasen. Du kommer då att kunna exportera dina lösenord från Bitdefender Password Manager.

Dina data kommer endast att lagras i livedatabasen till slutet av dagen då de återställdes på begäran. Vid midnatt raderas databasen – och om du ännu inte har överskridit den extra 30-dagarsperioden kan lösenord återställas från backup. Rådatabasdata från säkerhetskopian kan tillhandahållas på begäran till användaren, men databasen är krypterad och informationen kan inte nås.

Vad är ett huvudlösenord och varför måste jag komma ihåg det?

Huvudlösenordet är nyckeln som låser upp dörren till alla lösenord som är lagrade i ditt Bitdefender Password Manager-konto. Huvudlösenordet måste vara minst 8 tecken långt. Så skapa ett starkt huvudlösenord, memorera det och dela det aldrig med någon. För att skapa ett starkt huvudlösenord rekommenderar vi att du använder en kombination av stora och små bokstäver, siffror och specialtecken (som #, $ eller @).

Varför sparar du inte mitt huvudlösenord, och vad händer om jag glömmer det?

Anledningen till att vi inte lagrar ditt huvudlösenord på våra servrar är så att bara du kan komma åt ditt konto. Det är det säkraste sättet. Om

Bitdefender Password Manager inte känner igen ditt huvudlösenord, se till att du skriver det korrekt och att Caps Lock-tangenten inte är aktiv på tangentbordet.

Om du glömmer huvudlösenordet kan du alltid använda återställningsnyckeln för att låsa upp lösenordshanteraren. Under registreringsprocessen tillhandahåller Bitdefender Password Manager en **återställningsnyckel** som kan användas för att återfå åtkomst till kontot utan att förlora din data.

Vad är offline-läge?

Offline-läget aktiveras automatiskt när internetanslutningen avbryts när du använder Bitdefender SecurePass. Om du redan är inloggad och har angett ditt huvudlösenord låter offlineläget dig komma åt dina lösenord när en internetanslutning är utom räckhåll.

Hur avinstallerar jag Bitdefender Password Manager?

För att avinstallera Bitdefender Password Manager:

- På Windows och macOS:
  Ta bort tillägget Password Manager från din webbläsare. Högerklicka på Bitdefender-ikonen och välj "Ta bort".
- På Android:
  Knacka och håll appen Password Manager och dra den till toppen av skärmen där det står "Avinstallera".
- På iOS och iPadOS:
  Tryck och håll appen Lösenordshanteraren tills alla appar på skärmen börjar vicka, tryck sedan på X:et uppe till vänster om Bitdefender-ikonen.

Sekretess- och säkerhetsfrågor om Bitdefender Password Manager

Kan Bitdefender-anställda se mina lösenord?

Absolut inte. Din integritet är vår högsta prioritet. Detta är huvudorsaken till att vi inte lagrar ditt huvudlösenord på våra dataservrar: så att ingen har tillgång till ditt konto, inte ens företagets anställda. Varje lösenord och konto är mycket krypterade med den starkaste datasäkerhetsalgoritmen, och koden vi ser ser helt enkelt ut som en slumpmässig sträng av siffror och bokstäver som blandas ihop.

Vad skulle hända om lösenordshanterarens servrar hackades?

Varje lösenord krypteras lokalt på din enhet innan det kommer någonstans i närheten av våra servrar, så om hackare skulle bryta sig in i vårt system skulle de bara få sidor med slumpmässiga bokstäver och siffror utan din nyckel för att dekryptera dem. Det betyder att du och dina kontouppgifter alltid är säkra hos oss.

9. FÅ HJÄLP

9.1. 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.

9.2. 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.

9.2.1. 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/.

9.2.2. 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/

9.2.3. 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/.

9.3. 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 24).

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

9.3.1. 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

Det är en unik nyckel som kan köpas från återförsäljare och användas för att aktivera en specifik produkt eller tjänst. En aktiveringskod möjliggör aktivering av en giltig prenumeration för en viss tidsperiod och antal enheter och kan också användas för att förlänga en prenumeration 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.

Virtuellt privat nätverk (VPN)

Är en teknik som aktiverar en tillfällig och krypterad direktanslutning till ett visst nätverk över ett mindre säkert nätverk. På så sätt är det säkert och krypterat att skicka data och svårt för snokare att få tag på dem. Ett bevis på säkerheten 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.