ANVÄNDARGUIDE

Bitdefender CONSUMER SOLUTIONS

Parental Control

Bitdefender Parental Control

Användarmanual

Publication date 04/29/2024

Juridisk notering

Bitdefender

Innehållsförteckning

OM DEN HÄR GUIDEN

Syfte och avsedd målgrupp

Denna guide är avsedd för alla Bitdefender-användare som har valt Bitdefender Föräldrakontroll som sin lösning för säkerhet, övervakning och kontinuerligt skydd av sina barns enheter och närvaro på nätet.

Du kommer att få reda på hur du installerar, konfigurerar och får ut det mesta av Bitdefender Föräldrakontroll, för förbättrade funktioner och bättre kontroll över ditt barns aktiviteter online.

Vi önskar dig en trevlig och användbar föreläsning.

Så här använder du den här guiden

Den här guiden är ordnad runt flera större ämnesområden:

Komma igång (sida 3)

Kom igång med att konfigurera din Bitdefender Föräldrakontroll.

Funktioner och funktionaliteter (sida 8)

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

Få hjälp (sida 19)

Var du ska leta och var du ska be om hjälp om något oväntat inträffar.

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. KOMMA IGÅNG

Vi börjar med en djupgående, steg-för-steg-guide om hur du konfigurerar Bitdefender Föräldrakontroll-prenumerationen på ditt Bitdefender Central-konto. Det här är det första steget i den enkla process som krävs för att du ska kunna hantera och övervaka dina barns aktiviteter på nätet på ett effektivt sätt.

1.1. Konfigurera föräldrakontroll

När du aktiverar din prenumeration för att påbörja konfigurationen av Bitdefender Föräldrakontroll på ditt konto:

1. Gå till ditt Bitdefender Central-konto och öppna fliken **Föräldrakontroll** på vänster sida av skärmen.
2. Klicka på **Kom igång**.
3. Ange program-PIN-kod

   > **Obs**
   > Denna pinkod hjälper till att förhindra att dina barn avaktiverar föräldrakontrollfunktioner på egen hand genom att logga ut från sin barnapplikation.
   >
   > Se till att komma ihåg den här PIN-koden.

4. Klicka på **Nästa**.
5. Fortsätt genom att skapa en barnprofil. Skriv in barnets namn och välj en profilbild. Klicka sedan på **Nästa**.
6. Välj den ålder som motsvarar ditt barns ålder. När du har gjort det klickar du på **Nästa**.
7. Ange om Föräldrakontroll-appen ska installeras på den aktuella enheten du använder eller på en annan enhet.

Obs

Om du väljer **Andra enheter** får du tre installationsalternativ. Välj önskad metod:

- Genom att skanna QR-koden.
- Genom att kopiera den medföljande länken och öppna den i webbläsaren på barnets enhet.
- Genom att skicka installationslänken via e-post.

8. Vänta tills hämtningen är klar och kör sedan installationsprogrammet på enheten i fråga.

Därefter påbörjas installationsprocessen. De steg som måste tas härifrån varierar beroende på vilken typ av enhet och operativsystem som installationen utförs på.

1.2. Installera Bitdefender Föräldrakontroll på ditt barns enheter

1.2.1. På Windows-enheter:

När du kör det nyligen hämtade installationsprogrammet:

1. Klicka på **Ja** om en dialogruta för användarkontokontroll uppmanar dig att tillåta att installationsfilen gör ändringar i enheten.
2. Logga in med dina inloggningsuppgifter för Bitdefender Central-kontot om du uppmanas till det.

1.2.2. På macOS-enheter:

När hämtningen av installationsprogrammet är klar dubbelklickar du på Bitdefender-filen för att starta installationsprocessen:

1. Du kommer att vägledas genom de steg som krävs för att installera Bitdefender Föräldrakontroll för macOS. Klicka på **Tillåt** om du blir tillfrågad.
2. Klicka på de två efterföljande **Fortsätt**-knapparna.
3. För att fortsätta installationen måste du godkänna villkoren i prenumerationsavtalet för programvaran.
4. Klicka på **Fortsätt**. Därefter klickar du på **Installera**.

5. Ange administratörsnamn och lösenord när du uppmanas att göra det och tryck sedan på knappen **Installera programvara**.

Vänta tills du får ett popup-meddelande om att *en systemtillägg har blockerats*. Detta är en naturlig företeelse under denna procedur. Om du vill fortsätta måste du tillåta systemtillägget Föräldrakontroll enligt anvisningarna nedan:

1. Klicka på knappen **Öppna systeminställningar**.

> **Obs**
> På tidigare macOS-versioner kallas den här knappen för **Öppna säkerhetsinställningar**.

2. Klicka på knappen **Tillåt** i fönstret som visas på skärmen och ange sedan administratörsnamn och lösenord för att låsa upp inställningarna.

> **Obs**
> Innan du kan klicka på knappen **Tillåt** i macOS 11 (Big Sur) och macOS 12 (Monterey) måste du först klicka på hänglåsikonen i det nedre vänstra hörnet i fönstret **Säkerhet och sekretess** och sedan ange ett administratörsnamn och lösenord för att göra ändringar.

3. Popup-fönstret **Filtrera nätverksinnehåll** visas. Klicka på knappen **Tillåt** i det här fönstret.
4. Klicka på knappen **Öppna systeminställningar**.
5. Klicka på knappen **Tillåt** ytterligare en gång.

1.2.3. På Android-enheter:

Du hittar Bitdefenders Google Play Store-sida för föräldrakontrollprogrammet:

1. Tryck på knappen **Installera**. Appen börjar hämtas och installeras.
2. När installationen är klar kommer du att se en **Öppna**-knapp. Tryck på den för att starta programmet Bitdefender Föräldrakontroll.

När du har öppnat programmet följer du stegen på skärmen för att ställa in föräldrakontroll på ditt barns Android-enhet:

1. Tryck på **Fortsätt**.

2. Logga in i appen med dina inloggningsuppgifter till Bitdefender Central-kontot.
3. Välj den barnprofil som du vill tilldela Android-enheten.
4. Du måste bevilja nödvändiga behörigheter för appen för att den ska fungera korrekt. För att göra det, tryck på **Nästa** och sedan på:
   a. Tillåt VPN-åtkomst och välj sedan **Tillåt hela tiden** för att filtrera onlineinnehåll på ditt barns enhet.
   b. För att hjälpa till att hitta ditt barns Android-enhet trycker du på **Nästa**, därefter på **Tillåt** och väljer alternativet **Tillåt hela tiden**.
   c. Både VPN- och platsbehörigheter kommer att visa en grön bock. Tryck på **Slutför installation** och sedan på **Nästa**.
   d. I det här läget finns det ytterligare 3 behörigheter för att blockera internetåtkomst och appar på barnets enhet. Tryck på **Ange behörighet** i panelen **Rättigheter för enhetsadministratör**.
   e. Tryck på knappen **Slutför** när du är klar med att konfigurera Bitdefender Föräldrakontroll-appen.

1.2.4. På iOS-enheter:

Du hittar Bitdefenders App Store-sida för föräldrakontrollprogrammet:

1. Tryck på molnikonen med en pil som pekar nedåt. Appen börjar hämtas och installeras.
2. När installationen är klar kommer du att se en **Öppna**-knapp. Tryck på den för att starta appen Bitdefender Föräldrakontroll.
3. Om det finns några profiler för mobilenhetshantering på barnets iOS-enhet kommer du att bli ombedd att ta bort dem. Tryck på **Nästa** och välj **Ta bort profiler**.
4. I appens iOS-**inställningar** går du till **Allmänt**, rullar sedan nedåt och trycker på avsnittet **VPN och enhetshantering**.
5. Tryck på varje post i avsnittet **MOBILENHETSHANTERING** och välj **Ta bort hantering** för var och en.
   Upprepa denna process tills det inte finns några fler MOBILENHETSHANTERING-poster kvar.

Öppna appen som är installerad på barnets enhet igen och följ stegen på skärmen för att konfigurera Bitdefender Föräldrakontroll:

1. Tryck på **Fortsätt**.
2. Logga in i appen med dina inloggningsuppgifter till Bitdefender Central-kontot.
3. Välj den barnprofil som du vill tilldela iOS-enheten.
4. Du måste sedan ge de nödvändiga behörigheterna för att applikationen ska fungera korrekt. Tryck på **Nästa**.
5. Tillåt VPN-åtkomst för att filtrera onlineinnehåll på ditt barns enhet. Tryck på **Tillåt** två gånger i rad för att lägga till VPN-konfigurationerna.
6. Tryck på **Nästa** och välj sedan **Tillåt** för att hjälpa till att hitta ditt barns iOS-enhet.
7. Gå sedan igenom processen med att ställa in Apple Family Control för att blockera internetåtkomst och appar på barnets enhet.

> **Obs**
> Du kan trycka på **Läs mer nu** för att få en steg-för-steg-guide om hur du gör det.

8. När du har konfigurerat Apple Family Control på din egen enhet och på ditt barns enhet väljer du Jag **har konfigurerat Apple Family Control** för att fortsätta.
9. Låt sedan Skärmtidsåtkomst filtrera onlineinnehåll på ditt barns iOS-enhet.
10. Tryck på **Slutför installation**.

.

När du har slutfört dessa steg på ditt barns enhet(er) är installationsprocessen klar. Som förälder kan du nu övervaka ditt barns onlineaktiviteter och visa användningsstatistik i ditt Bitdefender Central-konto, i instrumentpanelen för föräldrakontroll, som vi kommer att beskriva i följande kapitel.

2. FUNKTIONER OCH FUNKTIONALITETER

2.1. Profiler

En barnprofil är en anpassad uppsättning regler som gör det möjligt för appen Bitdefender Föräldrakontroll att hantera och övervaka ett barns aktiviteter på nätet. Den innehåller inställningar som är anpassade till barnets ålder, t.ex. innehållsfilter och tidsbegränsningar. Med hjälp av Bitdefender Central-kontot kan föräldrar skapa, redigera och radera dessa profiler, samt tilldela och ta bort enheter till dem, vilket säkerställer en säker och lämplig onlineupplevelse för deras barn.

Så här skapar du en barnprofil:

1. Gå till Bitdefender Central och logga in på ditt konto.
2. Klicka på fliken **Föräldrakontroll** i menyn på vänster sida.
3. Klicka på **Ny profil** för att skapa en ny barnprofil.
4. Ange barnets namn, profilbild och födelsedatum.

   > **Obs**
   > Baserat på barnets ålder blockerar Bitdefender automatiskt vissa kategorier som chatt, sociala nätverk, explicit innehåll med mera. Du kan justera blockerade kategorier senare.

5. Klicka på knappen **Spara**.

Den nya profilen är nu skapad och visas på sidan.

Så här redigerar du en barnprofil:

1. Klicka på knappen **Visa detaljer** i barnets profil.
2. Om du vill ändra ditt barns profil går du till **Redigera profil**.
3. Använd motsvarande fält för att ändra barnets namn, födelsedag och/eller profilbild.
4. Klicka på **Spara ändringar** när du har ändrat de nödvändiga uppgifterna.

Så här tar du bort en barnprofil:

1. Klicka på knappen **Visa detaljer** i barnets profil.

2. Gå till **Redigera profil**.
3. Klicka på knappen **Ta bort profil** och bekräfta borttagningen.

Så här tilldelar du enheter till en barnprofil:

Om ditt barn har flera enheter (Windows, macOS, Android eller iOS) kan du tilldela dem till samma barnprofil.

1. Klicka på knappen **Visa detaljer** i barnets profil.
2. Klicka på antalet enheter som listas under deras namn.
3. Klicka på knappen **Tilldela enheter**.
4. Välj enhetsnamnet och klicka sedan på knappen **Tilldela**.

> **Obs**
> Om enheten inte syns i listan klickar du på **Installera en ny enhet** och följer sedan instruktionerna på skärmen för att installera och konfigurera Bitdefender Föräldrakontroll på den nya enheten.

Så här tar du bort enheter från en barnprofil:

När du tar bort en enhet från ett barns profil innebär det att enheten inte längre kommer att hanteras av Bitdefender Föräldrakontroll. De regler och inställningar som anges i barnets profil gäller inte längre för den enheten. Även om appen Föräldrakontroll fortfarande är installerad på enheten upphör den att fungera.

1. Klicka på knappen **Visa detaljer** i barnets profil.
2. Klicka på antalet enheter som listas under deras namn.
3. Leta reda på barnets enhet och klicka på alternativet **Ta bort tilldelning av enhet**.
4. Tryck på knappen **Ja, ta bort tilldelning av enhet** för att bekräfta åtgärden.

2.2. Statistik

Föräldrakontroll ger insikter i hur barn använder internet och sina enheter. I den här guiden går vi igenom de olika statistiska uppgifter som finns tillgängliga för föräldrar i Bitdefender Central, vilket ger dem möjlighet att fatta välgrundade beslut och säkerställa en säker och balanserad onlineupplevelse för sina barn.

För att visa statistiken:

1. Gå till Bitdefender Central och logga in på ditt konto.
2. När du är inloggad klickar du på fliken **Föräldrakontroll** i menyn på vänster sida.
3. Klicka på profilen för det barn vars statistik du vill se.

När du har valt ditt barns profil kommer du till en instrumentpanel som visar olika statistikpaneler. Alla hänvisar till de övriga funktioner som beskrivs längre ner i denna dokumentation.

2.3. PIN-kod för förälder

PIN-koden för föräldrakontroll är en säkerhetsfunktion i Bitdefender Central-plattformens instrumentpanel för föräldrakontroll. Det fungerar som ett sätt för föräldrar att behålla kontrollen över sina barns tillgång till Bitdefender Föräldrakontroll-appen som är installerad på deras enheter. Nedan följer en detaljerad guide om hur du ställer in, hittar och hanterar din föräldra-PIN.

PIN-koden för föräldrar förhindrar obehöriga utloggningar från Bitdefender Föräldrakontroll-appen på ditt barns enhet. När ditt barn försöker logga ut kommer hen att uppmanas att ange PIN-koden. Det säkerställer att endast du, som förälder med tillgång till Bitdefender Central-kontot, kan styra appens inställningar.

> **Obs**
> När du konfigurerar Föräldrakontroll-appen för första gången ombeds du att ange en 4-8 siffror lång PIN-kod för föräldrarna.

2.3.1. Har du glömt PIN-koden?

Om du glömmer din föräldra-PIN-kod kan du enkelt hämta den från ditt Bitdefender Central-konto:

1. Gå till Bitdefender Central och logga in på ditt konto.
2. När du är inloggad klickar du på fliken **Föräldrakontroll** i menyn på vänster sida.
3. Klicka på **Pin-kod** i det övre högra hörnet av sidan.
4. Klicka på den ögonformade ikonen för att hitta din PIN-kod för föräldrar.

2.3.2. Ändra din PIN-kod

Om du misstänker att din PIN-kod har äventyrats eller om du helt enkelt vill uppdatera den av säkerhetsskäl:

1. I avsnittet Föräldrakontroll i ditt Bitdefender Central-konto klickar du på alternativet **Pin-kod**.
2. Välj alternativet **Ändra PIN-kod** och följ anvisningarna på skärmen för att ange en ny PIN-kod.

2.4. Innehållsfiltrering

Innehållsfiltrering gör det möjligt för föräldrar att begränsa barnens tillgång till onlineinnehåll, så att de kan blockera hela kategorier av webbplatser eller göra undantag baserat på specifika webbadresser eller ämnen.

> **Obs**
> Innehållsfiltreringsfunktionen i Bitdefender Föräldrakontroll hindrar inte ditt barn från att använda applikationer eller webbplatser offline, eftersom den bara hanterar internettrafiken online för de enheter som de använder.

För att komma åt innehållsfiltrering:

1. Logga in på ditt Bitdefender Central-konto.
2. Klicka på fliken **Föräldrakontroll** i menyn på vänster sida.
3. Gå till ditt barns profil och klicka på menyn **Mer** längst upp till höger. Välj sedan **Innehållsfiltrering**.

2.4.1. Säker sökning och YouTube-begränsningar

I avsnittet **Sekretess och säkerhet** på höger sida av skärmen kan du aktivera omkopplarna Säker sökning och YouTube-begränsad.

- **Säker sökning:** Vid användning av sökmotorer förhindrar Säker sökning att innehåll som Google bedömer som osäkert visas i sökresultaten.
- **YouTube-begränsad:** Ger barnet tillgång till åldersanpassade videor på YouTube.

> **Obs**
> **Säker sökning** och **YouTube-begränsad** omdirigerar alla DNS-förfrågningar från **google.com** till **safe**.google.com. Den faktiska innehållsfiltreringen görs av Google. Bitdefender Föräldrakontroll filtrerar inte innehåll inom Säker sökning eller Google. Det är inte heller säkert att YouTube effektivt kontrollerar taggar på videor, vilket kan leda till att barn utsätts för olämpligt innehåll.

2.4.2. Blockering och tillåtande av webbplatskategorier

> **Obs**
> I avsnittet **Kategorier** anges vilka typer av webbplatser som ditt barn kan se online och som tillåts eller blockeras som standard, beroende på den ålder som angavs när barnets profil skapades.

Du kan när som helst blockera eller tillåta olika typer av webbplatser:

1. Välj en kategori.
2. Om du vill blockera åtkomsten till den här kategorin väljer du **Blockerad** i rullgardinsmenyn. För att tillåta åtkomst väljer du **Tillåt**.

> **Viktigt**
> Om du blockerar kategorin **Fildelning** för ditt barns profil kommer macOS-uppdateringen inte att fungera. Vi rekommenderar att du tillfälligt tillåter fildelning när du uppdaterar macOS.

2.4.3. Undantag

På fliken **Undantag** kan du ange undantag för webbplatser och program:

- **Webbplatsundantag:**
  1. Klicka på knappen **Lägg till undantag**.
  2. Välj **Endast webbplats** och klicka sedan på knappen **Nästa**.
  3. Skriv in webbadressen och välj om du vill tillåta eller blockera den i rullgardinsmenyn.
  4. Klicka sedan på knappen **Lägg till**.
- **App- och webbplattformundantag:**
  1. Klicka på knappen **Lägg till undantag**.

2. Välj **App- och webbplattform** och klicka sedan på knappen **Nästa**.
3. Välj den plattform som du vill göra ett undantag för från den angivna listan. Alternativt kan du använda sökfältet för att hitta det du letar efter.
4. Klicka sedan på knappen **Lägg till**.

- **Ta bort undantag:**
  Alla undantag som du har ställt in kommer att visas i Innehållsfiltrering i den angivna listan längst ned.
  För att ta bort ett undantag klickar du på papperskorgsikonen till höger om posten.

2.5. Daglig internettid

I ditt Bitdefender Central-konto under avsnittet Föräldrakontroll visas ett kort för daglig internettid för varje barnprofil som skapats. Detta kort visar den totala tid som barnet har tillbringat online på alla tilldelade enheter. Om du vill begränsa ett barns tid på nätet:

1. Gå till barnets profil och klicka på knappen **Ange tidsgräns** i panelen **Daglig internettid**. Alternativt kan du klicka på menyn **Mer** i det övre högra hörnet och välja **Daglig internettid**.
2. Klicka på knappen **Aktivera tidsgräns** för att aktivera den här funktionen.

> **Obs**
> Som standard får barnet 1 timme och 30 minuters tillgång till internet per dag. Om föräldern inte förlänger denna tidsgräns stoppas barnets tillgång till internet efter 1 timme och 30 minuter.

Ta bort daglig tidsgräns:

- Du stänger av funktionen Daglig internettid genom att gå till instrumentpanelen för ditt barns profil, klicka på knappen **Redigera tid** i panelen **Daglig internettid** och sedan på knappen **Paus** i panelen **Tidsgräns**.
- Om du vill ta bort tidsgränsen för en viss dag klickar du på knappen ⊗ som motsvarar den veckodagen i panelen **Schema**.

Ändring av tidsgräns:

- Om du vill ställa in en annan tidsgräns för en viss veckodag klickar du på dagens namn i panelen **Schema**, väljer önskad gräns i rullgardinsmenyn och klickar sedan på knappen **Spara ändringar**. Du kan välja mer än en dag åt gången.

2.5.1. Belöningssystem

Med funktionen **Belöning** kan du belöna eller förlänga skärmtiden för ditt barn och på så sätt främja sunda onlinevanor. Du kan använda belöningssystemet på två olika sätt:

- **Manuell belöning:**

  1. Navigera till avsnittet Föräldrakontroll i ditt Bitdefender Central-konto.
  2. Gå till barnets profil och klicka på knappen **Belöning** i panelen **Daglig internettid**.
  3. Välj hur mycket extra tid du vill lägga till och bekräfta genom att klicka på **Belöning**.

- **Barnbegäran:**
  När ditt barn når den dagliga gränsen kan de begära ytterligare tid via appen Föräldrakontroll som är installerad på deras mobila enhet. Som förälder får du ett meddelande i ditt Bitdefender Central-konto.

  1. När du är inloggad på ditt Bitdefender Central-konto, leta efter en röd prick på aviseringsklockan i det övre högra hörnet av skärmen, vilket indikerar en väntande begäran från ditt barn.
  2. Granska begäran och besluta hur mycket extra tid som ska beviljas.

> **Obs**
> Barn har möjlighet att begära förlängning av sin dagliga internettid endast på Android- och iOS-enheter.

2.6. Stänga av internet på ditt barns enhet

Som förälder kan det vara viktigt för ditt barns välbefinnande och produktivitet att du hanterar barnets internetanvändning. För att tillfälligt inaktivera internetåtkomst på ditt barns enhet med hjälp av Bitdefender Föräldrakontroll:

1. Gå till Bitdefender Central och logga in på ditt konto.
2. När du är inloggad klickar du på fliken **Föräldrakontroll** i menyn på vänster sida.
3. Välj **Visa detaljer** i profilen för det barn vars internet du vill inaktivera.
4. Klicka på knappen **Stoppa internet** i det övre högra hörnet av barnets instrumentpanel

   Obs
   Internet stängs av på alla ditt barns enheter. Denna åtgärd åsidosätter alla befintliga inställningar för föräldrakontroll, t.ex. rutiner, daglig tidsgräns eller tillåtna kategorier.

5. När tillgången till internet är avstängd ändras knappen **Stoppa internet** till **Återuppta internet**. För att återställa internetåtkomsten klickar du bara på knappen **Återuppta internet**.

2.7. Tillbaka till Rutiner

Inom Bitdefender Parental Control kan du ställa in upp till 3 olika rutiner för att schemalägga när ditt barns internetåtkomst ska stängas av. De ger en strukturerad metod för att hantera barnens onlineaktiviteter, främja sunda vanor och familjeengagemang samtidigt som de garanterar deras säkerhet. Dessa rutiner är oberoende av varandra, vilket innebär att du kan välja att aktivera bara en, två eller alla tre beroende på vad du föredrar:

- **Fokustid**
  Skapa ett schema som innehåller tid för läxor, studier och andra aktiviteter.
- **Läggdags**
  Använd rutinen Läggdags för att låsa in en viloperiod för ditt barn.
- **Familjetid**
  Använd rutinen Familjetid för att avsätta tid för ditt barn att närvara vid till exempel familjemåltider.

Obs

Rutiner kontra daglig internettid:

Under rutinerna räknas inte den tid som tillbringas online in i den dagliga Internet-tidsgränsen. När rutinen avslutas fortsätter funktionen Daglig internettid att räkna barnets internetanvändning.

För att undvika förvirring hos föräldrar kommer kortet för daglig internettid inte att synas på barnets profilpanel förrän rutinen är klar när en rutin pågår. Istället kommer namnet på den aktiva rutinen att visas under denna tid.

2.7.1. Upprätta rutiner

För att ställa in någon av rutinerna för föräldrakontroll:

1. Gå till Bitdefender Central och logga in på ditt konto.
2. Klicka på fliken **Föräldrakontroll** i menyn på vänster sida.
3. Gå till barnets profil och välj önskad rutin från menyn **Mer**.
4. Klicka på knappen **Aktivera** för att aktivera den valda rutinen.
5. Detta leder till att panelerna **Schema** och **Internetåtkomst** visas.

   - **Tidsplan:**
     Skapa en rutin för en eller flera dagar i veckan:

     a. Välj önskade dagar.

     b. Välj start- och sluttid för rutinen i rullgardinsmenyn.

     c. Klicka slutligen på knappen **Spara ändringar** för att bekräfta dina val.

     Om du vill ta bort rutinen för en viss dag klickar du på knappen ⊗ som motsvarar den veckodagen.

   - **Internetåtkomst:**
     Panelen för internetåtkomst i en rutin har två huvudfunktioner för att kontrollera ett barns onlineaktiviteter under specifika tidsramar:

     - **Fullständig avstängning av internet:** Föräldrar har möjlighet att helt stänga av internetåtkomsten för sitt barn under den schemalagda rutintiden. Genom att stänga av

internetåtkomstknappen kommer barnets enheter inte att kunna komma åt internet inom den angivna tidsramen.

- **Selektiv kategori eller webbplats:** Alternativt kan föräldrar välja att tillåta internetåtkomst under vanliga tider men begränsa vissa webbplatser eller kategorier av innehåll. När du slår på omkopplaren **Internetåtomst** blir ytterligare två flikar synliga, nämligen flikarna **Kategorier** och **Undantag**, som ger dig tillgång till ytterligare inställningar för Innehållsfiltrering</link>. (sida 11)

2.8. Spåra var ditt barn befinner sig

Med utbredningen av smartphones och andra mobila enheter har spårning av ditt barns plats blivit ett viktigt verktyg för många familjer. Oavsett om det handlar om att veta var de befinner sig efter skolan eller när de är ute med vänner, ger möjligheten att övervaka deras plats sinnesfrid för föräldrar. Här är en steg-för-steg-guide om hur du spårar ditt barns plats med hjälp av Bitdefender Föräldrakontrolls platsfunktion.

1. Gå till Bitdefender Central och logga in på ditt konto.
2. När du är inloggad klickar du på fliken **Föräldrakontroll** i menyn på vänster sida.
3. Om du har flera barn väljer du **Visa detaljer** från det barns profil vars plats du vill spåra.
4. I panelen Plats väljer du den Android- eller iOS-enhet som du vill spåra och klickar sedan på knappen **Hitta**.

   Obs
   Platsfunktionen i Bitdefender Föräldrakontroll är inte tillgänglig för Windows- och macOS-enheter.

5. Efter en kort väntan visar en röd nål ditt barns aktuella plats på kartan.

   Obs
   Platsuppdateringar sker var 20:e minut. Om du försöker spåra ditt barns plats mindre än 20 minuter efter den senaste lokaliseringen kan det hända att den plats som visas inte återspeglar var barnet befinner sig i realtid.

3. AVINSTALLERA FÖRÄLDRAKONTROLL

Avinstallera Bitdefender Föräldrakontroll på Windows-enheter:

1. Ta bort enheten från ditt barns profil i Bitdefender Central.
2. Öppna Kontrollpanelen på enheten i fråga och leta reda på Bitdefender Föräldrakontroll i listan **Program och funktioner**.
3. Avinstallera Bitdefender Föräldrakontroll.

Avinstallera Bitdefender Föräldrakontroll på macOS-enheter:

1. Ta bort enheten från ditt barns profil i Bitdefender Central.
2. Öppna **Finder** på macOS-enheten.
3. Öppna dina program och leta reda på Bitdefender-mappen.
4. Öppna den och kör **Bitdefenders avinstallerare**.
5. Välj Bitdefender Föräldrakontroll i listan över produkter som ska avinstalleras.
6. Ange administratörsuppgifter och vänta på att avinstallationen ska slutföras.

Avinstallera Bitdefender Föräldrakontroll på Android- och iOS-enheter:

1. Ta bort enheten från ditt barns profil i Bitdefender Central.
2. Avinstallera Föräldrakontroll från den mobila enheten som alla andra program eller via Google Play Store respektive Appstore.

4. FÅ HJÄLP

4.1. 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.

4.2. 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.

4.2.1. 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/.

4.2.2. 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/

4.2.3. 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/.

4.3. 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 19).

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

4.3.1. 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.