

Bitdefender[®] ANTIVIRUS PLUS



ANVÄNDARMANUAL





Bitdefender Antivirus Plus Användarmanual

Publication date 20-07-2020

Copyright© 2020 Bitdefender

Juridisk notering

Alla rättigheter förbehållna. Ingen del av denna bok får reproduceras eller överföras i någon form eller på något sätt, elektroniskt eller mekaniskt, inklusive fotokopiering, inspelning eller på annan informationslagring eller något informationshämtningssystem, utan skriftligt tillstånd från en behörig företrädare för Bitdefender. Införande av korta citat i recensioner är möjligt endast med angivande av den citerade källan. Innehållet kan inte ändras på något sätt.

Varning och friskrivningsklausul. Denna produkt och dess dokumentation skyddas av upphovsrätt. Informationen i detta dokument tillhandahålls på "befintligt skick" utan garanti. Trots att alla försiktighetsåtgärder har tagits i utarbetandet av detta dokument kommer författarna inte ha något ansvar till någon person eller enhet med hänsyn till eventuell förlust eller skada som orsakats eller påstås ha orsakats direkt eller indirekt av informationen i detta arbete.

Denna bok innehåller länkar till tredje parts webbsidor som inte är under Bitdefenders kontroll, därför är inte Bitdefender ansvarig för innehållet av en länkad webbsida. Om du öppnar en webbplats från tredje part, som anges i detta dokument, kommer du göra det på egen risk. Bitdefender tillhandahåller endast dessa länkar som en förmån och integration av länkarna innebär inte att Bitdefender stöder eller accepterar något ansvar för innehållet av tredje parts webbsidor.

Varumärken. Varumärkets namn bör synas i denna bok. Alla registrerade och oregistrerade varumärken i detta dokument är respektive ägares enskilda egendom och är respektfullt erkända.



Innehållsförteckning

Installation	1
1. Förbereder för installation	2
2. Systemkrav	3
2.1. Programvarukrav	3
3. Installera din Bitdefender-produkt	4
3.1. Installera från Bitdefender Central	4
3.2. Installera från installationsdisk	7
Komma igång	12
4. Grunderna	13
4.1. Öppna Bitdefender-fönstret	14
4.2. Aviseringar	15
4.3. Profiler	15
4.3.1. Konfigurera automatisk aktivering av profiler	16
4.4. Lösenordskyddade Bitdefender-inställningar	17
4.5. Produktrapporter	17
4.6. Meddelanden om särskilda erbjudanden	18
5. Bitdefender-gränssnitt	19
5.1. Systemfältsikon	19
5.2. Navigeringsmeny	20
5.3. Kontrollpanel	21
5.3.1. Säkerhetsstatusområde	22
5.3.2. Autopilot	22
5.3.3. Snabbåtgärder	23
5.4. Bitdefender-avsnittet	24
5.4.1. Skydd	24
5.4.2. Sekretess	26
5.4.3. Verktyg	27
5.5. Ändra produktspråk	27
6. Bitdefender Central	28
6.1. Öppna Bitdefender Central	28
6.2. Tvåfaktorautentisering	29
6.2.1. Lägga till betrodda enheter	31
6.3. Mina prenumerationer	31
6.3.1. Kontrollera tillgängliga prenumerationer	31
6.3.2. Lägg till ny enhet	32
6.3.3. Förnya prenumeration	32
6.3.4. Aktivera prenumeration	33
6.4. Mina enheter	33
6.5. Aktivitet	35
6.6. Aviseringar	36



7. Se till att Bitdefender är uppdaterad	37
7.1. Kontrollerar om Bitdefender är uppdaterad	37
7.2. Utför en uppdatering	38
7.3. Slå på eller av automatisk uppdatering	38
7.4. Automatiska uppdateringsinställningar	39
7.5. Kontinuerliga uppdateringar	40

Hur 41

8. Installation	42
8.1. Hur installerar jag Bitdefender på en andra enhet?	42
8.2. Hur installerar jag om Bitdefender?	42
8.3. Varifrån kan jag hämta min Bitdefender-produkt?	43
8.4. Hur ändrar jag språk på min Bitdefender-produkt?	44
8.5. Hur använder jag min Bitdefender-prenumeration efter en Windows-uppgradering?	44
8.6. Hur uppgraderar jag till den senaste Bitdefender-versionen?	47

9. Bitdefender Central	48
9.1. Hur loggar jag in på Bitdefender-konto med ett annat konto?	48
9.2. Hur stänger jag av Bitdefender Central-hjälpmedelanden?	48
9.3. Jag har glömt det lösenord jag ställde in för mitt Bitdefender-konto. Hur återställer jag det?	49
9.4. Hur hanterar jag inloggningssessionerna kopplade till mitt Bitdefender-konto?	50

10. Skanna med Bitdefender	51
10.1. Hur skannar jag en fil eller en mapp?	51
10.2. Hur skannar jag mitt system?	51
10.3. Hur schemalägger jag en skanning?	51
10.4. Hur skapar jag ett anpassat skanningsjobb?	52
10.5. Hur undantar jag en mapp från att skannas?	54
10.6. Vad ska man göra när Bitdefender visar att en ren fil är infekterad?	55
10.7. Hur kontrollerar jag vilka hot Bitdefender upptäckte?	56

11. Privacy protection	57
11.1. Hur vet jag att min onlinetransaktion är säker?	57
11.2. Hur tar jag bort en fil permanent med Bitdefender?	57
11.3. Hur kan jag manuellt återställa krypterade filer när återställningsprocessen misslyckas?	58

12. Användbar information	59
12.1. Hur testar jag min säkerhetslösning?	59
12.2. Hur tar jag bort Bitdefender?	59
12.3. Hur tar jag bort Bitdefender VPN?	60
12.4. Hur tar jag bort tillägget Bitdefender Anti-tracker?	61
12.5. Hur stänger jag automatiskt ned enheten när skanningen är klar?	62
12.6. Hur konfigurerar jag Bitdefender för att använda en proxyanslutning till Internet?	63
12.7. Använder jag en 32-bitars eller en 64-bitars version av Windows?	64
12.8. Hur visar jag dolda objekt i Windows?	65



12.9. Hur tar jag bort andra säkerhetslösningar?	65
12.10. Hur startar jag om i Felsäkert läge?	66

Hantera din säkerhet 68

13. Antiviruskydd	69
13.1. Skanning vid återkomst (realtidsskydd)	70
13.1.1. Stänga av eller slå på realtidsskydd	70
13.1.2. Konfigurerar avancerade inställningar för realtidsskydd	70
13.1.3. Återställa standardinställningarna	73
13.2. Skanning på begäran	74
13.2.1. Skanna en fil eller mapp för hot	74
13.2.2. Köra en snabbskanning	74
13.2.3. Kör en systemskanning	75
13.2.4. Konfigurera en anpassad skanning	76
13.2.5. Guiden för Antiviruskanning	79
13.2.6. Kontrollera skanningsloggar	82
13.3. Automatisk skanning av borttagbara medier	82
13.3.1. Hur fungerar det?	83
13.3.2. Hantera skanning av borttagbara medier	83
13.4. Skanna världens fil	84
13.5. Konfigurera skanningsundantag	84
13.5.1. Undanta filer och mappar från skanning	85
13.5.2. Undanta filtillägg från skanning	85
13.5.3. Hantera skanningsundantag	86
13.6. Hantera filer i karantän	86
14. Avancerat hotskydd	88
14.1. Aktivera eller inaktivera Advanced Threat Defense	88
14.2. Kontrollera upptäckta skadliga attacker	88
14.3. Lägg till processer till undantag	89
14.4. Upptäckt av exploateringar	89
15. Förebygga onlinehot	91
15.1. Bitdefender-varningar i webbläsaren	92
16. Säkerhetsrisk	94
16.1. Skanna systemet för säkerhetsrisker	94
16.2. Använda automatisk sårbarhetsövervakning	96
16.3. Wi-Fi Security Advisor	98
16.3.1. Aktivera eller inaktivera meddelanden från Wi-Fi Security Advisor	98
16.3.2. Konfigurera trådlöst hemnätverk	99
16.3.3. Konfigurera trådlöst kontorsnätverk	99
16.3.4. Offentlig Wi-Fi	100
16.3.5. Kontrollera information om Wi-Fi-nätverk	100
17. Avhjälpning av ransomware	102
17.1. Aktivera eller inaktivera ransomwareavhjälpning	102
17.2. Aktivera eller inaktivera automatisk återställning	102
17.3. Visa filer som har återställts automatiskt	102
17.4. Återställa krypterade filer manuellt	103



17.5. Lägga till program till undantag	103
18. Lösenordshanteringsskydd för dina inloggningsuppgifter ...	105
18.1. Skapa en ny plånboksdatabas	106
18.2. Importera en befintlig databas	106
18.3. Exportera plånboksdatabasen	107
18.4. Synkronisera plånböckerna i molnet	107
18.5. Hantera dina plånboksinloggningsuppgifter	108
18.6. Aktivera eller inaktivera Password Manager-skyddet	108
18.7. Hantera inställningarna för Password Manager	109
19. Anti-tracker	112
19.1. Anti-tracker-gränssnitt	112
19.2. Inaktivera Bitdefender Anti-tracker	113
19.3. Tillåta att en webbplats spåras	113
20. VPN	115
20.1. Öppna VPN	115
20.2. VPN-gränssnitt	115
20.3. Prenumerationer	117
21. Safepay-säkerhet för onlinetranslationer	118
21.1. Använda Bitdefender Safepay™	119
21.2. Konfigurera inställningar	120
21.3. Hantera bokmärken	121
21.4. Inaktivera Safepay-meddelanden	122
21.5. Använda VPN med Safepay	122
22. USB Immunizer	123
Verktyg	124
23. Profiler	125
23.1. Arbetsprofil	126
23.2. Filmprofil	127
23.3. Spelprofil	128
23.4. Publik Wi-Fi-profil	129
23.5. Batterilägesprofil	130
23.6. Realtidsoptimering	131
24. Dataskydd	132
24.1. Radera filer permanent	132
Felsökning	133
25. Lösa vanliga problem	134
25.1. Mitt system verkar vara långsamt	134
25.2. Skanningen startar inte	135
25.3. Jag kan inte längre använda en app	138
25.4. Vad du ska göra när Bitdefender blockerar en webbplats, en domän, en IP-adress eller en onlineapp som är säker.	139
25.5. Så här uppdaterar du Bitdefender på en långsam Internet-anslutning	140



25.6. Tjänsterna för Bitdefender svarar inte	140
25.7. Funktionen Autofill i min plånbok fungerar inte	141
25.8. Bitdefender-borttagning misslyckades	142
25.9. Mitt system startar inte efter att ha installerat Bitdefender	143
26. Ta bort hot från ditt system	146
26.1. Räddningsmiljön	146
26.2. Vad ska du göra när Bitdefender hittar hot på enheten?	147
26.3. Hur rensar jag bort ett hot i ett arkiv?	148
26.4. Hur rensar jag ett e-postarkiv från hot?	149
26.5. Vad gör jag om jag misstänker att en fil är farlig?	150
26.6. Vad är de lösenordsskyddade filerna i skanningsloggen?	151
26.7. Vad är de överhoppade posterna i skanningsloggen?	151
26.8. Vad är de överkomprimerade filerna i skanningsloggen?	151
26.9. Varför raderade Bitdefender en infekterad fil automatiskt?	152
Contact us	153
27. Be om hjälp	154
28. Onlineresurser	156
28.1. Bitdefenders supportcenter	156
28.2. Bitdefender Supportforum	156
28.3. HOTforSecurity Portal	157
29. Contact information	158
29.1. Webbadresser	158
29.2. Lokala återförsäljare	158
29.3. Bitdefender-kontor	158
Ordlista	161



INSTALLATION



1. FÖRBEREDER FÖR INSTALLATION

Innan du installerar Bitdefender Antivirus Plus, fullför dessa förberedelser för att försäkra att installationen ska gå smidigt:

- Försäkra dig om att enheten som du har tänkt installera Bitdefender på, uppfyller systemkraven. Om enheten inte uppfyller alla systemkrav kommer inte Bitdefender att installeras, eller om den installeras kommer den inte att fungera som den ska och orsaka avmattning samt instabilitet på systemet. För en komplett lista över systemkrav, se "*Systemkrav*" (p. 3).
- Logga in på enheten genom att använda ett administratörskonto.
- Ta bort alla andra liknande program från enheten. Om något upptäcks under Bitdefender-installationsprocessen blir du meddelad om att avinstallera det. Att köra två säkerhetsprogram samtidigt kan påverka deras aktivitet samt orsaka stora problem med systemet. Windows Defender inaktiveras under installationen.
- Vi rekommenderar att din enhet är ansluten till Internet under installationen, även vid installation från en CD/DVD. Om nyare versioner av de app-filer som ingår i installationspaketet är tillgängliga kan Bitdefender hämta och installera dem.



2. SYSTEMKRAV

Du kan endast installera Bitdefender Antivirus Plus på enheter som använder följande operativsystem:

- Windows 7 med Service Pack 1
- Windows 8
- Windows 8.1
- Windows 10
- 2,5 GB tillgängligt hårddiskutrymme (minst 800 MB på systemenheten)
- 2 GB minne (RAM)



Viktigt

Systemprestanda kan påverkas på enheter som har gamla generationers processorer.



Notera

Ta reda på vilket Windows-operativsystem din enhet kör och maskinvaruinformation:

- I **Windows 7** högerklickar du på **Min dator** på skrivbordet och väljer sedan **Egenskaper** från menyn.
- I **Windows 8**, från Windows Start-skärm, leta upp **Dator** (du kan till exempel börja skriva "Dator" direkt i startskärmen) och högerklicka sedan på dess ikon. I **Windows 8.1** letar du upp **Den här datorn**.

Välj **Egenskaper** i menyn längst ned. Titta i **System**-området för att hitta information om din systemtyp.

- I **Windows 10**, skriver du **System** i sökrutan från aktivitetsfältet och klickar på ikonen. Titta i **System**-området för att hitta information om din systemtyp.

2.1. Programvarukrav

För att kunna använda Bitdefender och alla dess funktioner måste din enhet uppfylla följande programvarukrav:

- Microsoft Edge 40 och senare
- Internet Explorer 10 och senare
- Mozilla Firefox 51 och senare
- Google Chrome 34 och senare



3. INSTALLERA DIN BITDEFENDER-PRODUKT

Du kan installera Bitdefender från installationsskivan eller använda webbinstallationsprogrammet hämtat till din enhet från **Bitdefender Central**.

Om ditt köp omfattar mer än en enhet (du har till exempel köpt Bitdefender Antivirus Plus för 3 datorer), upprepar du installationsprocessen och aktiverar din produkt med samma konto på varje enhet. Det konto du måste använda är det som innehåller din Bitdefender aktiva prenumeration.

3.1. Installera från Bitdefender Central

Från Bitdefender Central kan du hämta installationspaketet som motsvarar den köpta prenumerationen. När installationsprocessen är klar är Bitdefender Antivirus Plus aktiverad.

Hämta Bitdefender Antivirus Plus från Bitdefender Central:

1. Öppna **Bitdefender Central**.
2. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.
3. Välj ett av två möjliga alternativ:
 - **Skydda den här enheten**
 - a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan klickar du på motsvarande knapp.
 - b. Spara installationsfilen.
 - **Skydda andra enheter**
 - a. Välj det här alternativet och välj sedan enhetens ägare. Om enheten tillhör någon annan klickar du på motsvarande knapp.
 - b. Klicka på **SKICKA NEDLADDNINGSLÄNK**.
 - c. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**.

Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.
 - d. Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtningsknapp.



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

Validerar installationen

Bitdefender kontrollerar först ditt system för att validera installationen.

Om systemet inte uppfyller kraven för att installera Bitdefender informeras du om de områden som behöver förbättras innan du kan fortsätta.

Om en inkompatibel säkerhetslösning eller en äldre version av Bitdefender hittas, uppmanas du att ta bort den från systemet. Följ anvisningarna för att ta bort programvaran från systemet och därmed undvika problem som inträffar senare. Du kanske måste starta om enheten för att slutföra borttagningen av de hittade säkerhetslösningarna.

Bitdefender Antivirus Plus-installationspaketet uppdateras fortlöpande.



Notera

Hämtning av installationsfilerna kan ta lång tid, särskilt över långsamma Internet-anslutningar.

När installationen är validerad visas konfigurationsguiden. Följ stegen för att installera Bitdefender Antivirus Plus.

Steg 1 - Bitdefender-installation

Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta en stund och läs igenom prenumerationsavtalet eftersom det innehåller de användningsvillkor enligt vilka du kan använda Bitdefender Antivirus Plus.

Om du inte accepterar dessa villkor stänger du fönstret. Installationsprocessen kommer att överges och du kommer att lämna installationen.

Två ytterligare uppgifter kan utföras vid det här steget:

- Behåll alternativet **Skicka produktrapporter** aktiverat. Genom att tillåta det här alternativet skickas rapporter som innehåller information om hur du använder produkten till Bitdefender-servrarna. Den här informationen är viktig för att förbättra produkten och kan hjälpa oss att tillhandahålla en bättre upplevelse i framtiden. Observera att dessa rapporter inte



innehåller konfidentiella uppgifter, som ditt namn eller IP-adress, och de kommer inte att användas i kommersiella syften.

- Välj det språk du vill installera produkten på.

Klicka på **INSTALLERA** för att starta installationsprocessen för din Bitdefender-produkt.

Steg 2 - Installation pågår

Vänta tills det är slutfört. Detaljerad information om förloppet visas.

Steg 3 - Installation slutförd

Din Bitdefender har installerats.

En sammanfattning av install processen kommer att visas. Om något aktivt hot upptäcktes och togs bort under installationen kan en omstart av datorn behövas.

Steg 4 – Enhetsanalys

Du kommer nu att få frågan om du vill genomföra en analys av din enhet för att säkerställa att den är säker. Under det här steget kommer Bitdefender söka igenom kritiska systemområden. Klicka på **Starta enhetsanalys** för att initiera den.

Du kan dölja skanningsgränssnittet genom att klicka på **Kör skanning i bakgrunden**. Sedan väljer du huruvida du vill informeras om när skanningen är klar.

När skanningen är slutförd klickar du på **Öppna Bitdefender-gränssnittet**.



Notera

Om du inte vill genomföra sökningen klickar du bara på **Hoppa över**.

Steg 5 - Kom igång

I fönstret **Komma igång** kan du se information om din aktiva prenumeration.

Klicka på **AVSLUTA** för att komma till Bitdefender Antivirus Plus-gränssnittet.



3.2. Installera från installationsskiva

Sätt i skivan i den optiska enheten för att installera Bitdefender från installationsskivan.

En installationsskärm visas inom några ögonblick. Följ instruktionerna för att starta installationen.

Om installationsskärmen inte visas använder du Utforskaren för att bläddra till skivans rotkatalog och dubbelklickar på filen `autorun.exe`.

Om din Internet-hastighet är långsam eller om systemet inte är anslutet till Internet klickar du på knappen **Installera från CD/DVD**. I det här fallet installeras den Bitdefender-produkt som är tillgänglig på skivan och en nyare version hämtas från Bitdefender-servrarna via produktuppdatering.

Validerar installationen

Bitdefender kontrollerar först ditt system för att validera installationen.

Om systemet inte uppfyller kraven för att installera Bitdefender informeras du om de områden som behöver förbättras innan du kan fortsätta.

Om en inkompatibel säkerhetslösning eller en äldre version av Bitdefender hittas, uppmanas du att ta bort den från systemet. Följ anvisningarna för att ta bort programvaran från systemet och därmed undvika problem som inträffar senare. Du kanske måste starta om enheten för att slutföra borttagningen av de hittade säkerhetslösningarna.



Notera

Hämtning av installationsfilerna kan ta lång tid, särskilt över långsamma Internet-anslutningar.

När installationen är validerad visas konfigurationsguiden. Följ stegen för att installera Bitdefender Antivirus Plus.

Steg 1 - Bitdefender-installation

Innan du fortsätter med installationen måste du godkänna prenumerationsavtalet. Ta en stund och läs igenom prenumerationsavtalet eftersom det innehåller de användningsvillkor enligt vilka du kan använda Bitdefender Antivirus Plus.



Om du inte accepterar dessa villkor stänger du fönstret. Installationsprocessen kommer att överges och du kommer att lämna installationen.

Två ytterligare uppgifter kan utföras vid det här steget:

- Behåll alternativet **Skicka produkt rapporter** aktiverat. Genom att tillåta det här alternativet skickas rapporter som innehåller information om hur du använder produkten till Bitdefender-serverna. Den här informationen är viktig för att förbättra produkten och kan hjälpa oss att tillhandahålla en bättre upplevelse i framtiden. Observera att dessa rapporter inte innehåller konfidentiella uppgifter, som ditt namn eller IP-adress, och de kommer inte att användas i kommersiella syften.
- Välj det språk du vill installera produkten på.

Klicka på **INSTALLERA** för att starta installationsprocessen för din Bitdefender-produkt.

Steg 2 - Installation pågår

Vänta tills det är slutfört. Detaljerad information om förloppet visas.

Steg 3 - Installation slutförd

En sammanfattning av install processen kommer att visas. Om något aktivt hot upptäcktes och togs bort under installationen kan en omstart av datorn behövas.

Steg 4 – Enhetsanalys

Du kommer nu att få frågan om du vill genomföra en analys av din enhet för att säkerställa att den är säker. Under det här steget kommer Bitdefender söka igenom kritiska systemområden. Klicka på **Starta enhetsanalys** för att initiera den.

Du kan dölja skanningsgränssnittet genom att klicka på **Kör skanning i bakgrunden**. Sedan väljer du huruvida du vill informeras om när skanningen är klar.

När skanningen är slutförd klickar du på **Fortsätt skapa konto**.



Notera

Om du inte vill genomföra sökningen klickar du bara på **Hoppa över**.



Steg 5 - Bitdefender-konto

När du slutför den initiala konfigurationen visas Bitdefender-kontofönstret. Ett Bitdefender-konto krävs för att aktivera produkten och använda dess onlinefunktioner. Mer information finns på "*Bitdefender Central*" (p. 28).

Fortsätt beroende på din situation.

● Jag vill skapa ett Bitdefender-konto

1. Skriv in den önskade informationen i de motsvarande fälten. De uppgifter du lämnar här kommer att hållas konfidentiella. Lösenordet måste vara minst 8 tecken långt och innehålla minst en siffra eller symbol och gemener och versaler.
2. Innan du går vidare måste du godkänna användningsvillkoren. Öppna användningsvillkoren och läs dem noggrant eftersom de innehåller de villkor under vilka du får använda Bitdefender.

Dessutom kan du öppna och läsa sekretesspolicyn.

3. Klicka på **SKAPA KONTO**.



Notera

När kontot har skapats kan du använda den medföljande e-postadressen och lösenordet för att logga in på ditt konto på <https://central.bitdefender.com> eller i Bitdefender Central-appen förutsatt att den är installerad på en av dina Android- eller iOS-enheter. För att installera Bitdefender Central-appen på Android måste du öppna Google Play, söka efter Bitdefender Central och sedan trycka på motsvarande installationsalternativ. För att installera Bitdefender Central-appen på iOS måste du öppna App Store, söka efter Bitdefender Central och sedan trycka på motsvarande installationsalternativ.

● Jag har redan ett Bitdefender konto

1. Klicka på **Logga in**.
2. Skriv e-postadressen i motsvarande fält och klicka sedan på **NÄSTA**.
3. Skriv lösenordet och klicka sedan på **LOGGA IN**.

Om du glömmer lösenordet för kontot eller om du bara vill återställa ett du redan angett:

- a. Klicka på **Glömt lösenord?**
- b. Skriv din e-postadress och klicka därefter på **NÄSTA**.



- c. Kontrollera e-postkontot, skriv in säkerhetskoden du fått och klicka på **NÄSTA**.

Alternativt kan du klicka på **Byt lösenord** i det e-postmeddelande vi skickat till dig.

- d. Skriv in det lösenord du vill ställa in och skriv det sedan en gång till. Klicka på **SPARA**.



Notera

Om du redan har ett MyBitdefender-konto kan du använda det för att logga in på ditt Bitdefender-konto. Om du glömt lösenordet måste du först gå till <https://my.bitdefender.com> för att återställa det. Använd sedan de uppdaterade inloggningsuppgifterna för att logga in på ditt Bitdefender-konto.

● Jag vill använda mitt Microsoft-, Facebook- eller Google-konto för att logga in

Logga in med ditt Microsoft-, Facebook- eller Google-konto:

1. Välj den tjänst du vill använda. Du kommer att omdirigeras till inloggningssidan för den tjänsten.
2. Följ instruktionerna från den valda tjänsten för att koppla ditt konto till Bitdefender.



Notera

Bitdefender får inte åtkomst till någon konfidentiell information som lösenordet till kontot du använder för att logga in eller personlig information om vänner och kontakter.

Steg 6 - Aktivera din produkt



Notera

Det här steget visas om du har valt att skapa ett nytt Bitdefender-konto under föregående steg eller om du har loggat in med ett konto med en prenumeration som gått ut.

En aktiv Internet-uppkoppling krävs för att slutföra aktiveringen av din produkt.

Fortsätt beroende på din situation:



● Jag har en aktiveringskod

I det här fallet aktiverar du produkten genom att följa de här stegen:

1. Skriv aktiveringskoden i fältet **Jag har en aktiveringskod** och klicka därefter på **FORTSÄTT**.



Notera

Du hittar din aktiveringskod:

- på CD/DVD-etiketten.
- på kortet för produktregistrering.
- i onlineköpsmeddelandet.

2. Jag vill utvärdera Bitdefender

I det här fallet kan du använda produkten i 30 dagar. Starta utvärderingsperioden genom att välja **Jag har ingen prenumeration, jag vill prova produkten gratis** och klicka sedan på **FORTSÄTT**.

Steg 7 - Kom igång

I fönstret **Kom igång** kan du se information om din aktiva prenumeration.

Klicka på **AVSLUTA** för att komma till Bitdefender Antivirus Plus-gränssnittet.



KOMMA IGÅNG



4. GRUNDERNA

När du har installerat Bitdefender Antivirus Plus är din enhet skyddad mot alla typer av hot (som skadlig kod, spionprogramvara, ransomware, exploateringar, botnets och trojaner).

Appen använder Photon-teknik för att förbättra hastigheten och prestanda för hotskanningsprocessen. Det fungerar genom att lära sig användningsmönstren för dina systemappar för att veta vad och när det ska skanna och minimerar därmed påverkan på din systemprestanda.

Att ansluta till offentliga nätverk som tillhör flygplatser, köpcenter, kaféer eller hotell utan skydd kan vara farligt för din enhet och dina data. Det beror huvudsakligen på att bedragare kan se din aktivitet och hitta det rätta ögonblicket för att stjäla personlig information, men också för att alla kan se din IP-adress och därmed göra din maskin till ett offer för framtida cyberattacker. För att undvika sådana olyckliga situationer ska du installera och använda appen *"VPN"* (p. 115).

Du kan hålla reda på dina lösenord och onlinekonton genom att lagra dem med *"Lösenordshanteringskydd för dina inloggningsuppgifter"* (p. 105) i en plånbok. Med ett enda huvudlösenord kan du skydda din integritet från inkräktare som kan försöka komma åt dina pengar.

För att skydda dig från eventuella snokar och spioner när din enhet är ansluten till ett osäkert trådlöst nätverk, analyserar Bitdefender dess säkerhetsnivå och när det behövs, ger rekommendationer för att öka säkerheten för dina onlineaktiviteter. Se *"Wi-Fi Security Advisor"* (p. 98) för anvisningar om hur du håller dina personuppgifter säkra.

Filer som krypterats av ransomware kan nu återställas utan att behöva betala pengar för en begärd lösensumma. Se *"Avhjälpling av ransomware"* (p. 102) för information om hur du återställer krypterade filer.

När du arbetar, spelar spel eller tittar på film kan Bitdefender ge dig en kontinuerlig användarupplevelse genom att fördröja uppgifter, eliminera avbrott och justera systemets visuella effekter. Du kan utnyttja allt detta genom att aktivera och konfigurera *"Profiler"* (p. 125).

Bitdefender fattar de mest säkerhetsrelaterade besluten åt dig och visar sällan popup-meddelanden. Detaljer om åtgärder som vidtas och information om programdrift finns i fönstret Meddelanden. Mer information finns på *"Aviseringar"* (p. 15).



Då och då bör du öppna Bitdefender och lösa eventuella existerande problem. Du kan behöva konfigurera särskilda Bitdefenderkomponenter eller ta till förebyggande åtgärder för att skydda din enhet och din information.

För att använda onlinefunktionerna i Bitdefender Antivirus Plus och hantera dina prenumerationer och enheter öppnar du ditt Bitdefender-konto. Mer information finns på "*Bitdefender Central*" (p. 28).


I avsnitt "*Hur*" (p. 41) hittar du alla steg för steg-anvisningar om hur du utför vanliga uppgifter. Om du upplever problem med Bitdefender kan du läsa avsnittet "*Lösa vanliga problem*" (p. 134) för möjliga lösningar till de vanligaste problemen.

4.1. Öppna Bitdefender-fönstret


Får att nå huvudgränssnittet i Bitdefender Antivirus Plus klickar du på -ikonen på skrivbordet.

Om det behövs kan du även följa nedanstående steg:

● I Windows 7:

1. Klicka på **Start** och gå till **Alla program**.
2. Klicka på **Bitdefender**.
3. Klicka på **Bitdefender Antivirus Plus** eller, snabbare, dubbelklicka på Bitdefender -ikonen i systemfältet.

● I Windows 8 och Windows 8.1:

Leta upp Bitdefender från Windows Start-skärm (du kan till exempel börja skriva "Bitdefender" direkt på Start-skärmen) och därefter klicka på ikonen. Alternativt kan du öppna skrivbordsappen och sedan dubbelklicka på Bitdefender -ikonen i systemfältet.

● I Windows 10:

Skriv "Bitdefender" i sökrutan från aktivitetsfältet och klicka sedan på dess ikon. Alternativt dubbelklickar du på Bitdefender -ikonen i systemfältet.


Mer information om Bitdefender-fönstret och ikonen i systemfältet finns i "*Bitdefender-gränssnitt*" (p. 19).



4.2. Aviseringar

Bitdefender för en detaljerad logg över händelser som rör dess aktivitet på din enhet. Varje gång något som är relevant för säkerheten för system eller data inträffar, läggs ett nytt meddelande till i området Bitdefender-meddelanden, på ett liknande sätt som när ett nytt e-postmeddelande visas i inkorgen.

Meddelanden är ett viktigt verktyg för att övervaka och hantera ditt Bitdefender-skydd. Exempelvis kan du enkelt kontrollera om uppdateringen utfördes med framgång, om hot eller säkerhetsrisker hittades på din enhet osv. Dessutom kan du vidta ytterligare åtgärder om det behövs eller ändra åtgärder som vidtagits av Bitdefender.

Öppna meddelandeloggen genom att klicka på **Meddelanden** på navigeringsmenyn på **Bitdefender-gränssnittet**. Varje gång en kritisk händelse inträffar kan du se en räknare på -ikonen.

Beroende på typ och allvarlighetsgrad grupperas meddelanden i:

- **Kritiska** händelser indikerar kritiska problem. Du bör kontrollera dem omedelbart.
- **Varnings**-händelser anger problem som inte är kritiska. Du bör kontrollera dem och åtgärda dem när du har tid.
- **Informations**-händelser indikerar lyckade åtgärder.

Klicka på varje flik för att hitta mer information om de genererade händelserna. Kort information visas med ett klicka på varje händelserubrik, nämligen: en kort beskrivning, åtgärden Bitdefender vidtog för den när den inträffade samt datum och tid när den inträffade. Alternativ kan finnas för att vidta ytterligare åtgärder om det behövs.

För att det ska vara enklare att hantera loggade händelser har meddelandefönstret alternativ för att ta bort alla händelser i det avsnittet eller markera dem som lästa.

4.3. Profiler

Vissa datoraktiviteter, som onlinespel eller videopresentationer, kräver ökad systemresponsivitet, hög prestanda och inga avbrott. När din bärbara dator körs på batterikraft är det bäst att onödiga åtgärder, som kräver ytterligare kraft, skjuts upp tills datorn återigen är ansluten till elnätet.



Bitdefender-profiler tilldelar mer systemresurser till de appar som körs genom att tillfälligt ändra skyddsinställningar och justera systemkonfiguration. Fördjupad minimeras systeminverkan på din aktivitet.

För att anpassa sig till olika aktiviteter levereras Bitdefender med följande profiler:

Arbetsprofil

Optimerar din arbetseffektivitet genom att identifiera och justera produkt- och systeminställningarna.

Filmprofil

Förbättrar visuella effekter och eliminerar avbrott när du tittar på film.

Spelprofil

Förbättrar visuella effekter och eliminerar avbrott när du spelar spel.

Publik Wi-Fi-profil

Tillämpar produktinställningar för att dra nytta av fullständigt skydd vid anslutning till ett osäkert trådlöst nätverk.

Batterilägesprofil

Tillämpar produktinställningar och håller ned bakgrundsaktivitet för att spara batteritid.

4.3.1. Konfigurera automatisk aktivering av profiler

För en lättanvänd upplevelse kan du konfigurera Bitdefender att hantera din arbetsprofil. I det här fallet upptäcker Bitdefender automatiskt den aktivitet du utför och tillämpar optimeringsinställningar för system och produkt.

Första gången du öppnar **Profiler** blir du ombedd att aktivera automatiska profiler. För att göra det klickar du bara på **AKTIVERA** i fönstret som visas.

Du kan klicka på **INTE NU** om du vill aktivera funktionen vid ett senare tillfälle.

För att låta Bitdefender aktivera profiler automatiskt:

1. Klicka på **Verktyg** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fliken **Profiler** klickar du på **Inställningar**.
3. Använd motsvarande omkopplare för att slå på **Aktivera profiler automatiskt**.

Om du inte vill att profilerna ska aktiveras automatiskt slår du av omkopplaren.



Slå på motsvarande omkopplare för att aktivera en profil manuellt. Av de första tre profilerna kan endast en aktiveras manuellt i taget.

Mer information om profiler finns i "*Profiler*" (p. 125)

4.4. Lösenordskyddade Bitdefender-inställningar

Om du inte är den enda personen med administrativa rättigheter som använder den här enheten, rekommenderas det att du skyddar dina Bitdefenderinställningar med ett lösenord.

Konfigurera lösenordsskydd för Bitdefender-inställningarna:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fönstret **Allmänt** aktiverar du **Lösenordsskydd**.
3. Skriv lösenordet i de två fälten och klicka därefter på **OK**. Lösenordet måste innehålla minst 8 tecken

När du har ställt in ett lösenord måste den som försöker ändra Bitdefender-inställningarna först ange lösenordet.



Viktigt

Kom ihåg ditt lösenord eller förvara det på en säker plats. Om du glömmer bort lösenordet måste du ominstallera programmet eller kontakta Bitdefender för support.

För att ta bort lösenordsskydd:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fönstret **Allmänt** inaktiverar du **Lösenordsskydd**.
3. Skriv lösenordet och klicka sedan på **OK**.



Notera

Ändra lösenordet för din produkt genom att klicka på **Ändra lösenord**. Skriv ditt aktuella lösenord och klicka sedan på **OK**. I det nya fönster som visas skriver du det nya lösenord du vill använda från och med nu för att begränsa åtkomsten till dina Bitdefender-inställningar.

4.5. Produktrapporter

Produktrapporter innehåller information om hur du använder den Bitdefender-produkt du har installerat. Den här informationen är viktig för



att förbättra produkten och kan hjälpa oss att ge dig en bättre upplevelse i framtiden.

Observera att dessa rapporter inte innehåller konfidentiella uppgifter, som ditt namn eller IP-adress, och de kommer inte att användas i kommersiella syften.

Om du under installationsprocessen har valt att skicka sådana rapporter till Bitdefender-servrarna och nu vill stoppa processen:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. Gå till **Avancerat** fliken.
3. Stäng av **Produktrapporter**.

4.6. Meddelanden om särskilda erbjudanden

När kampanjerbjudanden är tillgängliga ställs Bitdefender-produkten in på att meddela dig via ett popup-fönster. Det här ger dig möjlighet att dra nytta av fördelaktiga priser och hålla dina enheter skyddade under en längre tidsperiod.

För att slå av eller på meddelanden om specialerbjudanden:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. Slå av eller på motsvarande omkopplare i fönstret **Allmänt**.

Alternativet för specialerbjudanden och produktmeddelanden är aktiverad som standard.



5. BITDEFENDER-GRÄNSSNITT

Bitdefender Antivirus Plus uppfyller behoven lika mycket för nybörjare på datorer som för väldigt tekniska människor. Dess grafiska användargränssnitt är utformat för att passa alla sorters människor.

För att gå igenom Bitdefender-gränssnittet finns en introduktionsguide som innehåller information om hur du interagerar med produkten och hur du konfigurerar den på den övre vänstra sidan. Välj rätt höger vinkelparentes för att fortsätta guidas eller **Hoppa över rundtur** för att stänga guiden.

Bitdefenders **systemfältsikon** är tillgänglig när som helst, oavsett om du vill öppna huvudfönstret, köra en produktuppdatering eller visa information om den installerade versionen.

I huvudfönstret finns information om din säkerhetsstatus. Baserat på din enhetsanvändning och behov visar **Autopilot** här olika typer av rekommendationer som hjälper dig att förbättra din enhetssäkerhet och prestanda. Dessutom kan du lägga till snabbåtgärder som du använder ofta, så att du har dem till hands när du behöver dem.

Från navigeringsmenyn till vänster kan du öppna inställningsavsnittet, meddelanden och **Bitdefender-avsnittet** för detaljerad konfiguration och avancerade administrativa uppgifter.

Från den övre delen i huvudgränssnittet kan du öppna ditt **Bitdefender-konto**. Du kan även kontakta oss för support om du har frågor eller något oväntat inträffar.

5.1. Systemfältsikon


För att snabbare hantera hela produkten kan du använda Bitdefender-ikonen **B** i systemfältet.



Notera

Bitdefender-ikonen kanske inte är synlig hela tiden. För att ikonen ska visas permanent:

● I Windows 7, Windows 8 och Windows 8.1:

1. Klicka på pilen  i det nedre högra hörnet på skärmen.
2. Klicka på **Anpassa...** för att öppna fönstret Meddelandeområdesikoner.
3. Välj alternativet **Visa ikoner och meddelanden** för **Bitdefender-agent**-ikonen.



● I Windows 10:

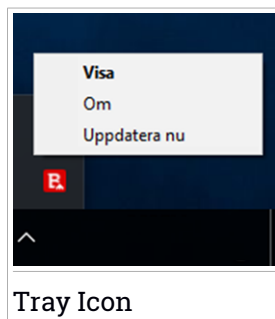
1. Högerklicka på aktivitetsfältet och välj **Inställningar för aktivitetsfält**.
2. Bläddra nedåt och klicka på länken **Välj vilka ikoner som ska visas på aktivitetsfältet** under **Aviseringsområde**.
3. Aktivera omkopplaren bredvid **Bitdefender-agenten**.

Om du dubbelklickar den här ikonen kommer Bitdefender att öppnas. Genom att högerklicka ikonen kommer en kontextmeny att snabbt låta dig hantera Bitdefenderprodukten.

● **Visa** - öppnar huvudfönstret i Bitdefender.

● **Om** - öppnar ett fönster där du kan se information om Bitdefender, var du kan få hjälp om något oväntat inträffar, var du hittar och visar prenumerationsavtalet, tredjepartskomponenter och sekretesspolicy.

● **Uppdatera nu** - startar en omedelbar uppdatering. Du kan följa upp uppdateringsstatusen i uppdateringspanelen i **Bitdefenders huvudfönster**.



Bitdefender systemfältsikon informerar dig när problem påverkar din enhet eller om hur produkten fungerar, genom att visa en speciell symbol, enligt följande:

B Det finns inga problem som påverkar ditt systems säkerhet.

B Kritiska problem påverkar ditt systems säkerhet. De kräver din omedelbara uppmärksamhet och måste lösas så snart som möjligt.







Om Bitdefender inte fungerar visas systemfältsikonen mot en grå bakgrund:

B Det här händer oftast när prenumerationen går ut. Det kan även hända när Bitdefender tjänsterna inte svarar eller när andra fel påverkar Bitdefender normala aktivitet.



5.2. Navigeringsmeny

På vänster sida i Bitdefender-gränssnittet finns navigeringsmenyn som ger dig snabb åtkomst till Bitdefender-funktioner och verktyg du behöver för att hantera din produkt. Flikarna som finns i det området är:



-  **Kontrollpanel.** Härifrån kan du snabbt åtgärda säkerhetsproblem, visa rekommendationer enligt dina systembehov och användningsmönster och utföra snabbåtgärder.
-
-  **Skydd.** Härifrån kan du öppna och konfigurera antivirus-sökningar, återställa data i händelse av att den krypteras av ransomware och konfigurera skydd medan du surfar på internet.
-  **Sekretess.** Här kan du skapa lösenordshanterare för dina konton online, göra betalningar online i en säker miljö och öppna VPN-appen.
-  **Verktyg.** Här kan du hantera profiler och få åtkomst till Data Protection-funktionen.
-  **Meddelanden.** Härifrån har du åtkomst till de genererade meddelandena.
-  **Inställningar.** Härifrån har du åtkomst till allmänna inställningar.

I den övre delen av huvudgränssnittet hittar du funktionerna **Mitt konto** och **Support**.

-  **Support.** Härifrån kan du, när du behöver hjälp med att lösa ett problem med Bitdefender Antivirus Plus, kontakta Bitdefenders tekniska supportavdelning.
-  **Mitt konto.** Härifrån kan du komma åt ditt Bitdefender-konto för att verifiera dina prenumerationer och utföra säkerhetsåtgärder på de enheter du hanterar. Information om Bitdefender-konto och pågående prenumeration finns också.

5.3. Kontrollpanel

I kontrollpanelsfönstret kan du utföra vanliga åtgärder, snabbt lösa säkerhetsproblem, visa information om produktfunktion och öppna panelerna varifrån du kan konfigurera produktinställningarna.

Allt är bara några klick borta.

Fönstret är indelat i tre huvudområden:



Säkerhetsstatusområde

Härifrån kan du kontrollera enhetens säkerhetsstatus.

Autopilot


Härifrån kan du kontrollera Autopilot-rekommendationerna för att säkerställa korrekt funktionalitet i systemet.

Snabbåtgärder

Härifrån kan du köra olika uppgifter för att hålla ditt system skyddat.

5.3.1. Säkerhetsstatusområde

Bitdefender använder system för spårning av problem för att upptäcka och informera dig om problem som kan påverka din enhets säkerhet och information. Upptäckta problem omfattar viktiga skyddsinställningar som är avstängda och andra förhållanden som kan innebära en säkerhetsrisk.

Varje gång problem påverkar säkerheten för din enhet ändras statusen som visas på den övre sidan av **Bitdefender-gränssnittet** till röd. Den visade statusen anger hur problemen påverkar ditt system. Dessutom ändras **systemfältsikonen** till  och om du för muspekaren över ikonen kommer en popup att bekräfta att det finns olösta problem.

Eftersom de upptäckta problemen kan förhindra Bitdefender från att skydda dig mot hot eller utgöra en stor säkerhetsrisk, rekommenderar vi att du är uppmärksam och löser dem så snabbt som möjligt. Klicka på knappen bredvid det upptäckta problemet för att lösa det.

5.3.2. Autopilot

För att ge dig en effektiv drift och ökat skydd när du utför olika aktiviteter, fungerar Bitdefender Autopilot som din personliga säkerhetsrådgivare. Beroende på vilken aktivitet du utför, om du antingen arbetar, utför onlinebetalningar, ser på film eller spelar spel, kommer Bitdefender Autopilot med kontextuella rekommendationer baserat på din enhetsanvändning och behov. De föreslagna rekommendationerna kan också handla om åtgärder du behöver utföra för att din produkt ska fungera fullt ut.

För att börja använda en föreslagen funktion eller göra förbättringar av din produkt, klickar du på motsvarande knapp.



Stänga av Autopilot-meddelanden

För att du ska uppmärksamma Autopilot-rekommendationerna är Bitdefender-produkten inställd på att meddela dig via ett popup-fönster.


Stänga av Autopilot-meddelanden:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fönstret **Allmänt** stänger du av **Rekommendationsmeddelanden**.

5.3.3. Snabbåtgärder

Med snabbåtgärder kan du snabbt starta uppgifter som anser vara viktiga för att hålla ditt system skyddat och förbättra ditt sätt att arbeta.

Som standard kommer Bitdefender med några snabbåtgärder som kan ersättas med dem du använder mest. Byta ut en snabbåtgärd:

1. Klicka på -ikonen i det övre högra hörnet på det kort du vill ta bort.
2. Peka på den uppgift du vill lägga till i huvudgränssnittet och klicka sedan på **LÄGG TILL**.

De uppgifter du kan lägga till i huvudgränssnittet är:

- **Snabbskanning.** Kör en snabbskanning för att direkt upptäcka möjliga hot som kan finns på din enhet.
- **Systemskanning.** Kör en systemskanning för att se till att din enhet är ren från hot.
- **Vulnerability Scan.** Skanna din enhet för säkerhetsrisker för att se till att alla installerade appar, tillsammans med operativsystemet, är uppdaterade och fungerar som de ska.
- **Wi-Fi Security Advisor.** Öppna Wi-Fi Security Advisor-fönstret i Vulnerability-modulen.
- **Plånböcker.** Visa och hantera dina plånböcker.
- **Öppna SafePay.** Öppna Bitdefender Safepay™ för att skydda dina känsliga data medan du utför onlinetransaktioner.
- **Öppna VPN.** Öppna Bitdefender VPN för att lägga till ett extra lager skydd när du är ansluten till Internet.
- **Filförstöraren.** Starta verktyget File Shredder för att ta bort spår efter känsliga data från din enhet.

Börja skydda ytterligare enheter med Bitdefender:

1. Klicka på **Installera på en annan enhet**.



Ett nytt fönster visas på skärmen.

2. Klicka på **DELA HÄMTNINGSLÄNK**.
3. Följ stegen på skärmen för att installera Bitdefender.

Beroende på ditt val installeras följande Bitdefender-produkter:

- Bitdefender Antivirus Plus på Windows-baserade enheter.
- Bitdefender Antivirus for Mac på macOS-baserade enheter.
- Bitdefender Mobile Security på Android-baserade enheter.
- Bitdefender Mobile Security på iOS-baserade enheter.

5.4. Bitdefender-avsnitten

Bitdefender-produkten kommer med tre avsnitt indelade i användbara funktioner som hjälper dig att hålla dig skyddad medan du arbetar, surfar på nätet eller gör onlinebetalningar, förbättrar hastigheten för systemet och mycket mer.

När du vill komma åt funktionerna för ett specifikt avsnitt eller börja konfigurera din produkt använder du följande ikoner som finns på navigeringsmenyn på **Bitdefender-gränssnittet**:

-  Skydd
-  Sekretess
-  Verktyg

5.4.1. Skydd

In avsnittet Skydd kan du konfigurera dina avancerade säkerhetsinställningar, ställa in funktionerna Online Threat Prevention, kontrollera och åtgärda eventuella systemsårbarheter och komma åt säkerheten för de trådlösa nätverk du ansluter till.

De funktioner du kan hantera i avsnittet Skydd är:

VIRUSSKYDD

Antiviruskydd är grunden i din säkerhet. Bitdefender skyddar dig i realtid och på begäran mot alla typer av hot, som skadlig kod, trojaner, spionprogramvara, adware, mm.



Från antivirusfunktionen kan du enkelt komma åt följande skanningsåtgärder:

- Snabbskanning
- Systemskanning
- Hantera skanningar
- Räddningsmiljön

Mer information om skanningsjobb och hur du konfigurerar antiviruskydd finns i "[Antiviruskydd](#)" (p. 69).

FÖREBYGGANDE AV ONLINEHOT

Med förebyggande av onlinehot kan du skydda dig mot nätfiskeattacker, bedrägeriförsök och läckage av privat information, när du surfar på nätet.

Mer information om hur du konfigurerar Bitdefender för att skydda din nättaktivitet finns i "[Förebygga onlinehot](#)" (p. 91).

ADVANCED THREAT DEFENSE

Avancerat hotförsvar skyddar aktivt ditt system mot hot som ransomware, spyware och trojaner genom att analysera beteende hos alla installerade appar. Misstänkta processer identifieras och blockeras, om det behövs.

Mer information om hur du skyddar systemet mot hot finns i "[Avancerat hotskydd](#)" (p. 88).

SÄKERHETSRIK

Vulnerability (sårbarhets)-modulen hjälper dig att hålla operativsystemet och de appar du regelbundet använder uppdaterade och att identifiera de osäkra trådlösa nätverk du ansluter till. Klicka på **Öppna** i Vulnerability-modulen för att komma åt funktionerna.

Funktionen **Sårbarhetsskanning** låter dig identifiera kritiska Windows-uppdateringar, app-uppdateringar, svaga lösenord som tillhör Windows-konton samt trådlösa nätverk som inte är säkra. Klicka på **Starta skanning** för att genomföra en skanning på din enhet.

Klicka på **Wi-Fi Security Advisor** för att visa listan över de trådlösa nätverk du ansluter till, tillsammans med vår ryktesutvärdering för var och en av de åtgärder du kan vidta för att skydda dig mot eventuella spioner.

Mer information om hur du konfigurerar säkerhetsriskskydd finns i "[Säkerhetsrisk](#)" (p. 94).



AVHJÄLPNING AV RANSOMWARE

Funktionen Avhjälpning av ransomware hjälper dig att återställa filer ifall de krypteras av ransomware.

Mer information om hur du återställer krypterade filer finns i "[Avhjälpning av ransomware](#)" (p. 102).

5.4.2. Sekretess

I avsnittet Sekretess kan du öppna Bitdefender VPN-appen, skydda dina onlinetransaktioner och se till att din surfupplevelse är säker.

De funktioner du kan hantera i avsnittet Sekretess är:

VPN

VPN säkrar din onlineaktivitet och döljer din IP-adress varje gång du ansluter till osäkra trådlösa nätverk när du är på flygplatser, köpcenter, kaféer eller hotell. Dessutom kan du komma åt innehåll som i normala fall är begränsat i vissa områden.

Mer information om den här funktionen finns i "[VPN](#)" (p. 115).

PASSWORD MANAGER

Bitdefender lösenordshanterare hjälper dig att hålla reda på dina lösenord, skyddar din integritet och ger en säker surfupplevelse.

Mer information om hur du konfigurerar lösenordshanteraren finns i "[Lösenordshanteringsskydd för dina inloggningsuppgifter](#)" (p. 105).

SAFEPAY

Webbläsaren Bitdefender Safepay™ hjälper dig att se till att dina bankärenden online, e-shopping och andra typer av onlinetransaktioner är privata och säkra.

Mer information om Bitdefender Safepay™ finns i "[Safepay-säkerhet för onlinetransaktioner](#)" (p. 118).

ANTI-TRACKER

Anti-tracker-funktionen hjälper dig att undvika spårning, så att dina data förblir privata medan du surfar online och minskar också den tid det tar för webbsidor att läsas in.

Mer information om Anti-tracker-funktionen finns på "[Anti-tracker](#)" (p. 112).



5.4.3. Verktyg

Dataskydd

Bitdefender File Shredder hjälper dig att radera data och fysiskt ta bort dem från din hårddisk permanent.

Mer information finns på "*Dataskydd*" (p. 132).

Profiler

Dagliga jobbaktiviteter, titta på film eller spela spel kan orsaka att systemet blir långsammare, särskilt om de körs samtidigt med Windows-uppdateringsprocesser och underhållsåtgärder.

Med Bitdefender kan du nu välja och tillämpa din föredragna profil, vilket gör att systemjusteringar anpassas för att öka prestandan för specifika installerade appar.

Mer information om den här funktionen finns i "*Profiler*" (p. 125).

5.5. Ändra produktspråk

Bitdefender-gränssnittet är tillgängligt på flera språk och kan ändras genom att följa dessa steg:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fönstret **Allmänt** klickar du på **Ändra språk**.
3. Välj önskat språk i listan och klicka därefter på **SPARA**.
4. Vänta en stund tills de nya inställningarna tillämpas.



6. BITDEFENDER CENTRAL

Bitdefender Central är en plattform vart du har tillgång till produktens alla onlinefunktioner och tjänster och kan fjärransluta viktiga uppgifter på enheterna Bitdefender är installerat på. Du kan logga in på ditt Bitdefender-konto från vilken enhet som helst som är ansluten till Internet genom att gå till <https://central.bitdefender.com>, eller direkt från Bitdefender Central-appen på Android- och iOS-enheter.

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

- **På Android** - sök Bitdefender Central på Google Play och hämta och installera appen. Följ stegen för att slutföra installationen.
- **På Android** - sök Bitdefender Central på App Store och hämta och installera appen. Följ stegen för att slutföra installationen.

När du är inloggad kan du börja göra följande:

- Hämta och installera Bitdefender på Windows, macOS, iOS och Android. De produkter som är tillgängliga för hämtning är:
 - Bitdefender Antivirus Plus
 - Bitdefender Antivirus för Mac
 - Bitdefender Mobile Security för Android
 - Bitdefender Mobile Security för iOS
- Hantera och förnya dina Bitdefender-prenumerationer.
- Lägg till nya enheter till nätverket och hantera dem var du än är.

6.1. Öppna Bitdefender Central

Det finns flera sätt att öppna Bitdefender Central:

- Från Bitdefenders huvudgränssnitt:
 1. Klicka på **Mitt konto** på navigeringsmenyn i **Bitdefender-gränssnittet**.
 2. Klicka på **Gå till Bitdefender Central**.
 3. Logga in till ditt Bitdefender-konto med e-postadress och lösenord.
- Från din webbläsare:
 1. Öppna en webbläsare på en enhet med Internet-åtkomst.



2. Gå till: <https://central.bitdefender.com>.

3. Logga in till ditt Bitdefender-konto med e-postadress och lösenord.

- Från din Android- eller iOS-baserade enhet:

Öppna Bitdefender Central-appen som du har installerat.



Notera

I det här materialet har du alternativ och instruktioner tillgängliga på webbplattformen.


6.2. Tvåfaktoraутентisering

2-faktoraутентiseringsmetoden ger ett extra säkerhetslager till ditt Bitdefender-konto, genom att kräva en autentiseringskod förutom dina inloggningsuppgifter. På det här sättet förhindrar du kontokapning och håller vissa typer av cyberattacker borta, som keyloggers, råstyrke- eller ordlisteattacker.

Aktivera tvåfaktoraутентisering

Genom att aktivera tvåfaktoraутентisering gör du ditt Bitdefender-konto mycket säkrare. Din identitet verifieras varje gång du loggar in från olika enheter, antingen för att installera en av Bitdefender-produkterna, kontrollera status för din prenumeration eller köra uppgifter via fjärrstyrning på dina enheter.

Aktivera tvåfaktoraутентisering:

1. Öppna **Bitdefender Central**.
2. Klicka på ikonen  uppe till höger på skärmen.
3. Klicka på **Bitdefender-konto** i reglagemenyn.
4. Välj fliken **Lösenord och säkerhet**.
5. Klicka på **Tvåfaktoraутентisering**.
6. Klicka på **KOM IGÅNG**.

Välj en av följande metoder:

- **Autentiseringsapp** - använd en autentiseringsapp för att generera en kod varje gång du vill logga in till ditt Bitdefender-konto.



Om du vill använda en autentiseringsapp, men inte är säker på vad du ska välja, finns det en lista över de autentiseringsappar vi rekommenderar.

- a. Klicka på **ANVÄND AUTENTISERINGSAPP** för att börja.
- b. Logga in på en Android- eller iOS-baserad enhet genom att använda enheten för att skanna QR-koden.

För att logga in på en bärbar eller stationär dator kan du manuellt lägga till den visade koden.

Klicka på **FORTSÄTT**.

- c. Infoga koden som appen gav eller den som visas i föregående steg och klicka sedan på **AKTIVERA**.

- **E-post** - varje gång du loggar in på ditt Bitdefender-konto skickas en verifieringskod till din e-postinkorg. Kontrollera ditt e-postkonto och skriv sedan in den kod du har fått.

- a. Klicka på **ANVÄND E-POST** för att starta.
- b. Kontrollera ditt e-postkonto och skriv in den angivna koden.

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

- c. Klicka på **AKTIVERA**.
- d. Du får tio aktiveringskoder. Du kan antingen kopiera, ladda ned eller skriva ut listan ifall du tappar bort din e-postadress eller inte kan logga in. Varje kod kan bara användas en gång.
- e. Klicka på **KLAR**.

Ifall du vill sluta använda tvåfaktorautentisering:

1. Klicka på **STÄNG AV TVÅFAKTORAUTENTISERING**.
2. Kontrollera din app eller ditt e-postkonto och skriv in koden du har fått.

Ifall du har valt att få autentiseringskoden via e-post har du fem minuter på dig att kontrollera ditt e-postkonto och skriva in den genererade koden. Om tiden går ut måste du generera en ny kod genom att följa samma steg.


3. Bekräfta ditt val.



6.2.1. Lägga till betrodda enheter

För att se till att bara du kan komma åt ditt Bitdefender-konto kan vi kräva en säkerhetskod först. Om du vill hoppa över det här steget varje gång du ansluter från samma enhet, rekommenderar vi att du utser den till en betrodd enhet.

Lägga till enheter som betrodda enheter:

1. Öppna **Bitdefender Central**.
2. Klicka på ikonen  uppe till höger på skärmen.
3. Klicka på **Bitdefender-konto** i reglagemenyn.
4. Välj fliken **Lösenord och säkerhet**.
5. Klicka på **Betrodda enheter**.
6. Listan över de enheter som Bitdefender är installerad på visas. Klicka på önskad enhet.

Du kan lägga till så många enheter du vill, förutsatt att de har Bitdefender installerat och att din prenumeration är giltig.

6.3. Mina prenumerationer

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

6.3.1. Kontrollera tillgängliga prenumerationer

Kontrollera dina tillgängliga prenumerationer:

1. Öppna **Bitdefender Central**.
2. Välj panelen **Mina prenumerationer**.

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

Du kan lägga till en ny enhet till en prenumeration eller förnya den genom att välja ett prenumerationsskort.



Notera

Du kan ha en eller flera prenumerationer på ditt konto förutsatt att de är för olika plattformar (Windows, macOS, iOS eller Android).



6.3.2. Lägg till ny enhet

Om din prenumeration omfattar mer än en enhet kan du lägga till en ny enhet och installera din Bitdefender Antivirus Plus på den, enligt följande:

1. Öppna **Bitdefender Central**.
2. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.
3. Välj ett av två möjliga alternativ:

● Skydda den här enheten

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

● Skydda andra enheter

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

Klicka på **SKICKA NEDLADDNINGSLÄNK**. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtknapp.

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

6.3.3. Förnya prenumeration

Om du inaktiverade att automatiskt förnya din Bitdefender-prenumeration, kan du manuellt förnya den genom att följa de här stegen:

1. Öppna **Bitdefender Central**.
2. Välj panelen **Mina prenumerationer**.
3. Välj önskat prenumerationkort.
4. Klicka på **FÖRNYA** för att fortsätta.

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



6.3.4. Aktivera prenumeration

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

Om du har köpt en aktiveringskod från någon av våra återförsäljare eller om du fått den som present, kan du lägga till dess tillgänglighet till en befintlig Bitdefender-prenumeration som är tillgänglig på kontot, förutsatt att de är för samma produkt.

Aktivera en prenumeration med en aktiveringskod:

1. Öppna **Bitdefender Central**.
2. Välj panelen **Mina prenumerationer**.
3. Klicka på knappen **AKTIVERINGSKOD** och skriv sedan in koden i motsvarande fält.
4. Klicka på **AKTIVERA** för att fortsätta.


Prenumerationen är nu aktiv. Gå till panelen **Mina enheter** och välj **INSTALLERA SKYDD** för att installera produkten på en av dina enheter.

6.4. Mina enheter

I området **Mina enheter** i Bitdefender Central har du möjlighet att installera, hantera och vidta fjärråtgärder på din Bitdefender-produkt på vilken enhet som helst, förutsatt att den är påslagen och ansluten till Internet. Enhetskorten visar enhetsnamn, skyddsstatus och om det finns säkerhetsrisker som påverkar enheternas skydd.


Visa en lista över dina enheter sorterad efter deras status eller användare genom att klicka på rullgardinspilen i det övre högra hörnet på skärmen.

För att enkelt identifiera dina enheter kan du anpassa enhetsnamnet:


1. Öppna **Bitdefender Central**.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på -ikonen i det övre högra hörnet på skärmen.
4. Välj **Inställningar**.
5. Skriv in ett nytt namn i fältet **Enhetsnamn**, klicka därefter på **SPARA**.



Du kan skapa och tilldela en ägare för varje enhet för bättre hantering:

1. Öppna **Bitdefender Central**.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på -ikonen i det övre högra hörnet på skärmen.
4. Välj **Profil**.
5. Klicka på **Lägg till ägare** och fyll i motsvarande fält. Anpassa profilen genom att lägga till ett foto och välj ett födelsedatum.
6. Klicka på **LÄGG TILL** för att spara profilen.
7. Välj önskad ägare från listan **Enhetsägare** och klicka på **TILLDELA**.

Fjärruppdatera Bitdefender på en Windows-enhet:

1. Öppna **Bitdefender Central**.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på -ikonen i det övre högra hörnet på skärmen.
4. Välj **Uppdatera**.

Klicka på önskat enhetskort för fler fjärråtgärder och information angående din Bitdefender-produkt på en specifik enhet.

När du klickar på ett enhetskort är följande flikar tillgängliga:

- **Kontrollpanel**. I det här fönstret kan du visa information om den valda enheten, kontrollera dess skyddsstatus, status för Bitdefender VPN och hur många hot som har blockerats de senaste sju dagarna. Skyddsstatus kan vara grönt när det inte finns några problem som påverkar enheten, gult när enheten behöver åtgärdas från din sida eller rött när enheten är utsatt för risk. När det finns problem som påverkar enheten klickar du på rullgardinsmenyn i det övre statusområdet för att se mer information. Härifrån kan du manuellt åtgärda problem som påverkar dina enheters säkerhet.
- **Skydd**. Från det här fönstret kan du fjärrstyra en snabb- eller systemskanning på dina enheter. Klicka på knappen **SKANNA** för att starta processen. Du kan också kontrollera när den senaste skanningen utfördes på enheten och det finns en rapport från den senaste skanningen med



den viktigaste informationen. Mer information om de här två skanningsprocesserna finns i *Avsnitt 13.2.3, "Kör en systemskanning"* och *"Köra en snabbskanning"* (p. 74).

- **Säkerhetsrisk.** Klicka på knappen **SKANNA** på fliken **Säkerhetsrisk** för att kontrollera en enhet för eventuella säkerhetsrisker som saknade Windows-uppdateringar, utdaterade appar eller svaga lösenord. Säkerhetsrisker kan inte åtgärdas via fjärrstyrning. Om en säkerhetsrisk hittas måste du köra en ny skanning på enheten och sedan vidta rekommenderade åtgärder. Klicka på **Mer information** för att komma åt en detaljerad rapport om de problem som hittas. Mer information om den här funktionen finns i *"Säkerhetsrisk"* (p. 94).

6.5. Aktivitet

I Aktivitetsområdet har du tillgång till information om de enheter som har Bitdefender installerad.

När du öppnar fönstret **Aktivitet** är följande kort tillgängliga:

- **Mina enheter.** Här kan du visa antal anslutna enheter tillsammans med deras skyddsstatus. Åtgärda problem via fjärrstyrning på de upptäckta enheterna, klicka på **Åtgärda problem** och klicka sedan på **SKANNA OCH ÅTGÄRDA PROBLEM**.


Visa information om de upptäckta problemen genom att klicka på **Visa problem**.

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

- **Blockerade hot.** Här kan du visa en graf som visar allmän statistik, däribland information om de hot som blockerats under de senaste 24 timmarna och sju dagarna. Den visade informationen hämtas beroende på det skadliga beteende som upptäckts på öppnade filer, appar och URL:er.
- **Topp användare med blockerade hot.** Här kan du visa en topp med de användare där flest hot hittats.
- **Topp enheter med blockerade hot.** Här kan du visa en topp med de enheter där flest hot hittats.



6.6. Aviseringar

För att du ska vara informerad om vad som händer på de enheter som är kopplade till ditt konto finns -ikonen till hands. När du klickar på den har du en översiktsbild som består av information om aktiviteten för de Bitdefender-produkter som är installerade på dina enheter.



7. SE TILL ATT BITDEFENDER ÄR UPPDATERAD

Nya hot hittas och identifieras varje dag. Det här är orsaken till varför det är mycket viktigt att se till att Bitdefender är uppdaterad med den senaste hotinformationsdatabasen.

Om du är ansluten till Internet via bredband eller DSL, tar Bitdefender hand om detta själv. Som standard söker det efter uppdateringar när du slår på din enhet samt varje **timme** efter det. Om en uppdatering upptäcks kommer den automatiskt att hämtas och installeras på din enhet.

Uppdateringsprocessen utförs i farten, vilket betyder att filerna som ska uppdateras ersätts efter hand. På så sätt kommer inte uppdateringsprocessen att påverka produktaktiviteten och samtidigt kommer alla säkerhetsrisker att exkluderas.



Viktigt

För att vara skyddad mot de senaste hoten ska du se till att Automatisk uppdatering är aktiverat.

I vissa särskilda situationer krävs ingripande från dig för att hålla ditt Bitdefender-skydd uppdaterat:

- Om din enhet ansluts till Internet via en proxyserver måste du konfigurera proxyinställningarna såsom beskrivs i "*Hur konfigurerar jag Bitdefender för att använda en proxyanslutning till Internet?*" (p. 63).
- Om du är ansluten till Internet via en uppringningsanslutning rekommenderas du att regelbundet uppdatera Bitdefender på användarbegäran. Mer information finns på "*Utför en uppdatering*" (p. 38).

7.1. Kontrollerar om Bitdefender är uppdaterad

Kontrollera tidpunkten för den senaste uppdateringen av din Bitdefender:

1. Klicka på **Meddelanden** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. På fliken **Alla** väljer du meddelandet som avser den senaste uppdateringen.

Du kan ta reda på när uppdateringar startades och information om dem (om de lyckades eller inte, om det krävs en omstart för att slutföra installationen). Om så krävs startar du om systemet så snabbt som möjligt.



7.2. Utför en uppdatering

För att göra uppdateringar krävs en Internet-anslutning.

Starta en uppdatering genom att högerklicka på Bitdefender -ikonen i **systemfälet** och sedan välja **Uppdatera nu**.

Uppdateringsfunktionen ansluter till Bitdefender-uppdateringsserver och kontrollerar om det finns uppdateringar. Om en uppdatering upptäcks kommer du antingen att ombes att bekräfta uppdateringen, eller så utförs uppdateringen automatiskt, beroende på **uppdateringsinställningarna**.




Viktigt

Det kan vara nödvändigt starta om enheten när du har slutfört uppdateringen. Vi rekommenderar att göra det så snart som möjligt.

Du kan också fjärrstyra uppdateringar på dina enheter, förutsatt att de är påslagna och anslutna till Internet.

Fjärruppdatera Bitdefender på en Windows-enhet:

1. Öppna **Bitdefender Central**.
2. Välj panelen **Mina enheter**.
3. Klicka på önskat enhetskort och sedan på -ikonen i det övre högra hörnet på skärmen.
4. Välj **Uppdatera**.

7.3. Slå på eller av automatisk uppdatering

Slå på eller av automatisk uppdatering:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. Välj fliken **Uppdatera**.
3. Slå av eller på motsvarande omkopplare.
4. Ett varningsfönster visas. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att automatisk uppdatering ska vara inaktiv. Du kan inaktivera den automatiska uppdateringen i 5, 15 eller 30 minuter, i en timme eller tills en systemomstart.



Varning

Det här är ett viktigt säkerhetsproblem. Vi rekommenderar att du inaktiverar automatisk uppdatering under så kort tid som möjligt. Om Bitdefender inte uppdateras regelbundet kan det inte skydda dig mot de senaste hoten.

7.4. Automatiska uppdateringsinställningar

Uppdateringarna kan utföras från det lokala nätverket, över Internet, direkt eller via en proxyserver. Som standard kommer Bitdefender att söka efter uppdateringar över Internet varje timme, och installera tillgängliga uppdateringar utan att meddela dig.

Standardinställningarna för uppdatering är anpassade efter de flesta användare och i normala fall behöver du inte ändra dem.

Justera uppdateringsinställningarna:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. Välj fliken **Uppdatera** och justera inställningarna enligt dina önskemål.

Uppdateringsfrekvens

Bitdefender är konfigurerad att kontrollera efter uppdateringar varje timme. Ändra uppdateringsfrekvensen genom att dra reglaget längs skalan för att ange önskad tidsperiod när uppdateringen ska ske.

Uppdatera bearbetningsregler

Varje gång en uppdatering är tillgänglig hämtar Bitdefender uppdateringen automatiskt och implementerar den utan att visa meddelanden. Stäng av alternativet **Tyst uppdatering** om du vill bli meddelad varje gång en ny uppdatering är tillgänglig.

Vissa uppdateringar kräver en omstart för att slutföra installationen.

Som standard fortsätter Bitdefender arbeta med de gamla filerna tills användaren frivilligt startar om enheten, om en uppdatering kräver en omstart. Det är för att förhindra Bitdefender-uppdateringsprocessen från att störa användarens arbete.

Om du vill ha ett meddelande när en uppdatering kräver en omstart slår du på **Omstartsmeddelande**.



7.5. Kontinuerliga uppdateringar

För att se till att du använder den senaste versionen kontrollerar Bitdefender automatiskt för produktuppdateringar. Dessa uppdateringar kan medföra nya funktioner och förbättringar, lösa produktproblem eller automatiskt uppgradera dig till en ny version. När den nya Bitdefender-versionen kommer via en uppdatering sparas anpassade inställningar och avinstallations- och ominstallationsproceduren hoppas över.

Dessa uppdateringar kräver en systemomstart för att installationen av nya filer ska starta. När en produktuppdatering är slutförd talar ett popup-fönster om att du ska starta om systemet. Om du missar det här meddelandet kan du antingen klicka på **STARTA OM NU** i fönstret **Meddelanden** där den senaste uppdateringen nämns eller starta om systemet manuellt.



Notera

Uppdateringarna omfattar nya funktioner och förbättringar som endast levereras till användare som har Bitdefender 2020 installerat.



HUR



8. INSTALLATION

8.1. Hur installerar jag Bitdefender på en andra enhet?

Om den prenumeration du har köpt omfattar mer än en enhet kan du använda ditt Bitdefender-konto för att aktivera en andra PC.

Installera Bitdefender på en andra enhet:

1. Klicka på **Installera på annan enhet** i det nedre vänstra hörnet av **Bitdefender-gränssnittet**.

Ett nytt fönster visas på skärmen.

2. Klicka på **DELA HÄMTNINGSLÄNK**.
3. Följ instruktionerna på skärmen för att installera Bitdefender.

Den nya enhet på vilken du har installerat Bitdefender-produkten visas i Bitdefender Central-kontrollpanelen.

8.2. Hur installerar jag om Bitdefender?

Typiska situationer när du skulle behöva installera om Bitdefender kan vara följande:

- du har installerat om operativsystemet.
- du vill lösa problem som kan ha orsakat nedgångar eller krascher.
- din Bitdefender-produkt startar inte eller fungerar inte korrekt.

Om något av de nämnda situationerna är ditt fall följer du de här stegen:

● I Windows 7:

1. Klicka på **Start** och gå till **Alla program**.
2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
3. Klicka på **INSTALLERA OM** i det fönster som visas.
4. Du måste starta om enheten för att slutföra processen.

● I Windows 8 och Windows 8.1:

1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.



2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **INSTALLERA OM** i det fönster som visas.
5. Du måste starta om enheten för att slutföra processen.

● I Windows 10:

1. Klicka på **Start**, därefter på **Inställningar**.
2. Klicka på **System**-ikonen i området **Inställningar** och välj sedan **Appar och funktioner**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
5. Klicka på **INSTALLERA OM**.
6. Du måste starta om enheten för att slutföra processen.



Notera

Genom att följa den här ominstallationsproceduren sparas anpassade inställningar och är tillgängliga i den nyinstallerade produkten. Andra inställningar kan växlas tillbaka till sin standardkonfiguration.

8.3. Varifrån kan jag hämta min Bitdefender-produkt?

Du kan installera Bitdefender från installationsskivan eller använda webbinstallationsprogrammet du kan hämta till din enhet från Bitdefender Central-plattformen.



Notera

Innan du kör satsen rekommenderar vi att du tar bort alla säkerhetslösningar som är installerade på ditt system. När du använder fler än en säkerhetslösning på samma enhet blir systemet instabilt.

Installera Bitdefender från Bitdefender Central:

1. Öppna **Bitdefender Central**.
2. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.
3. Välj ett av två möjliga alternativ:
 - **Skydda den här enheten**



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

● Skydda andra enheter

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

Klicka på **SKICKA NEDLADDNINGSLÄNK**. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtknapp.

4. Kör den Bitdefender-produkt du har hämtat.

8.4. Hur ändrar jag språk på min Bitdefender-produkt?

Bitdefender-gränssnittet är tillgängligt på flera språk och kan ändras genom att följa dessa steg:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fönstret **Allmänt** klickar du på **Ändra språk**.
3. Välj önskat språk i listan och klicka därefter på **SPARA**.
4. Vänta en stund tills de nya inställningarna tillämpas.

8.5. Hur använder jag min Bitdefender-prenumeration efter en Windows-uppgradering?

Den här situationen uppstår när du uppgraderar operativsystemet och du vill fortsätta använda din Bitdefender-prenumeration.

Om du använder en tidigare Bitdefender-version kan du uppgradera utan kostnad till den senaste Bitdefender, enligt följande:

- Från en tidigare Bitdefender Antivirus-version till den senaste Bitdefender Antivirus som finns tillgänglig.
- Från en tidigare Bitdefender Internet Security-version till den senaste Bitdefender Internet Security som finns tillgänglig.



- Från en tidigare Bitdefender Total Security-version till den senaste Bitdefender Total Security som finns tillgänglig.

Det är två fall som kan dyka upp:

- Du har uppgraderat operativsystemet med Windows Update och märker att Bitdefender inte längre fungerar.

I det här fallet måste du installera om produkten genom att följa de här stegen:

● I Windows 7:

1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
3. Klicka på **INSTALLERA OM** i det fönster som visas.
4. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
Öppna gränssnittet i din nyinstallerade Bitdefender-produkt för att komma åt funktionerna.

● I Windows 8 och Windows 8.1:

1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **INSTALLERA OM** i det fönster som visas.
5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
Öppna gränssnittet i din nyinstallerade Bitdefender-produkt för att komma åt funktionerna.

● I Windows 10:

1. Klicka på **Start**, därefter på **Inställningar**.
2. Klicka på **System**-ikonen i området **Inställningar** och välj sedan **Appar**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **Avinstallera** igen för att bekräfta ditt val.



5. Klicka på **INSTALLERA OM** i det fönster som visas.
6. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
Öppna gränssnittet i din nyinstallerade Bitdefender-produkt för att komma åt funktionerna.



Notera

Genom att följa den här ominstallationsproceduren sparas anpassade inställningar och är tillgängliga i den nyinstallerade produkten. Andra inställningar kan växlas tillbaka till sin standardkonfiguration.

- Du ändrade systemet och vill fortsätta använda Bitdefender-skyddet. Därför måste du installera om produkten med den senaste versionen.

Åtgärda den här situationen:

1. Hämta installationsfilen:

- a. Öppna **Bitdefender Central**.
- b. Välj panelen **Mina enheter** och klicka på **INSTALLERA SKYDD**.
- c. Välj ett av två möjliga alternativ:

- **Skydda den här enheten**

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

- **Skydda andra enheter**

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

Klicka på **SKICKA NEDLADDNINGSLÄNK**. Skriv in en e-postadress i motsvarande fält och klicka därefter på **SKICKA E-POST**. Observera att den genererade nedladdningslänken endast är giltig i 24 timmar. Om länken går ut måste du generera en ny genom att följa samma steg.

Kontrollera e-postkontot på den enhet du vill installera Bitdefender-produkt på och klicka på motsvarande hämtknapp.

2. Kör den Bitdefender-produkt du har hämtat.



Mer information om Bitdefender-installationsprocessen finns i "*Installera din Bitdefender-produkt*" (p. 4).

8.6. Hur uppgraderar jag till den senaste Bitdefender-versionen?

Från och med nu går det att uppgradera till den nyaste versionen utan att följa proceduren med manuell avinstallation och ominstallation. Mer exakt så levereras den nya produkten inklusive nya funktioner och stora produktförbättringar via produktuppdatering och om du redan har en aktiv Bitdefender-prenumeration aktiveras produkten automatiskt.

Om du använde 2020-versionen kan du uppgradera till den senaste versionen genom att följa de här stegen:

1. Klicka på **STARTA OM NU** i det meddelande du får med uppgraderingsinformationen. Om du missade det öppnar du fönstret **Meddelanden**, pekar på den senaste uppdateringen och klickar därefter på knappen **STARTA OM NU**. Vänta tills enheten startar om.

Fönstret **Nyheter** med information om de förbättrade och nya funktionerna visas.

2. Klicka på länkarna **Läs mer** för att dirigeras om till vår särskilda sida med mer information och användbara artiklar.
3. Stäng fönstret **Nyheter** för att gå till gränssnittet för den installerade versionen.

Användare som vill uppgradera kostnadsfritt från Bitdefender 2016 eller en tidigare version till den senaste versionen av Bitdefender måste ta bort den aktuella versionen från Kontrollpanelen och därefter hämta den senaste installationsfilen från Bitdefenders webbplats på följande adress: <https://www.bitdefender.com/Downloads/>. Aktiveringen är endast möjlig med en giltig prenumeration.



9. BITDEFENDER CENTRAL

9.1. Hur loggar jag in på Bitdefender-konto med ett annat konto?

Du har nu skapat ett nytt Bitdefender-konto och du vill använda det från och med nu.

Logga in med ett annat Bitdefender-konto:

1. Klicka på ditt kontonamn i den övre delen av **Bitdefender-gränssnittet**.
2. Klicka på **Växla konto** i det övre högra hörnet av skärmen för att ändra kontot som är länkat till enheten.
3. Skriv e-postadressen i motsvarande fält och klicka sedan på **NÄSTA**.
4. Skriv lösenordet och klicka sedan på **LOGGA IN**.



Notera


Bitdefender-produkten från din enhet ändras automatiskt enligt prenumerationen som är kopplad till det nya Bitdefender-konto.

Om det inte finns någon tillgänglig prenumeration kopplad till det nya Bitdefender-kontot eller om du vill överföra den från det tidigare kontot, kontakta du Bitdefender för support som beskrivs i avsnitt *"Be om hjälp"* (p. 154).

9.2. Hur stänger jag av Bitdefender Central-hjälpmeddlanden?

För att hjälpa dig förstå vad varje alternativ i Bitdefender Central används för visas hjälpmeddlanden på kontrollpanelen.

Om du inte längre vill se den här typen av meddelanden:

1. Öppna **Bitdefender Central**.
2. Klicka på ikonen  uppe till höger på skärmen.
3. Klicka på **Mitt konto** i reglagemenyn.
4. Klicka på **Inställningar** i reglagemenyn.
5. Inaktivera alternativet **Slå på/av hjälpmeddlanden**.



9.3. Jag har glömt det lösenord jag ställde in för mitt Bitdefender-konto. Hur återställer jag det?

Det finns två möjligheter att ange ett nytt lösenord för ditt Bitdefender-konto:

● Från **Bitdefender-gränssnittet**:

1. Klicka på **Mitt konto** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. Klicka på **Byt konto** i det övre högra hörnet av skärmen.
Ett nytt fönster visas.
3. Skriv din e-postadress och klicka på **NÄSTA**.
Ett nytt fönster visas.
4. Klicka på **Glömt lösenord?**.
5. Klicka **NÄSTA**.
6. Kontrollera e-postkontot, skriv in säkerhetskoden du fått och klicka på **NÄSTA**.
Alternativt kan du klicka på **Byt lösenord** i det e-postmeddelande vi skickat till dig.
7. Skriv in det lösenord du vill ställa in och skriv det sedan en gång till.
Klicka på **SPARA**.

● Från din webbläsare:


1. Gå till: <https://central.bitdefender.com>.
2. Klicka på **LOGGA IN**.
3. Skriv din e-postadress och klicka därefter på **NÄSTA**.
4. Klicka på **Glömt lösenord?**.
5. Klicka **NÄSTA**.
6. Kontrollera ditt e-postkonto och följ de angivna instruktionerna för att ställa in ett nytt lösenord för ditt Bitdefender-konto.

För att öppna ditt Bitdefender-konto från och med nu skriver du din e-postadress och det nya lösenordet du precis har ställt in.



9.4. Hur hanterar jag inloggningssessionerna kopplade till mitt Bitdefender-konto?

I ditt Bitdefender-konto har du möjlighet att visa de senaste inaktiva och aktiva inloggningssessionerna som körs på enheter som är kopplade till ditt konto. Dessutom kan du logga ut via fjärrstyrning genom att följa de här stegen:

1. Öppna **Bitdefender Central**.
2. Klicka på ikonen  uppe till höger på skärmen.
3. Klicka på **Sessioner** i reglagemenyn.
4. I området **Aktiva sessioner** väljer du alternativet **LOGGA UT** bredvid den enhet du vill ska slutföra inloggningssessionen.



10. SKANNA MED BITDEFENDER

10.1. Hur skannar jag en fil eller en mapp?

Det enklaste sättet att skanna en fil eller en mapp är att högerklicka på det objekt du vill skanna, peka på Bitdefender och välja **Skanna med Bitdefender** från menyn.

Följ Antivirus-guiden för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer.

Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

Typiska situationer när du skulle använda denna skanningsmetod innefattar följande:

- Du misstänker att en specifik fil eller mapp är infekterad.
- När du hämtar filer från Internet som du tror kan vara skadliga.
- Skanna nätverksresurser innan du kopierar filer till din enhet.

10.2. Hur skannar jag mitt system?

Utföra en fullständig skanning av systemet:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. Klicka på knappen **Kör skanning** bredvid **Systemskanning**.
4. Följ guiden för Systemskanning för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer.


Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem. Mer information finns på "*Guiden för Antivirusskanning*" (p. 79).

10.3. Hur schemalägger jag en skanning?

Du kan ställa in Bitdefender-produkten att börja skanna viktiga systemplatser när du inte sitter vid enheten.

Schemalägga en skanning:



1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. Klicka på  bredvid skanningstypen du vill schemalägga, Systemskanning och Snabbskanning, i den nedre delen av gränssnittet och välj sedan **Redigera**.

Alternativt kan du skapa en skanningstyp som passar dina behov genom att klicka på **+Skapa skanning** bredvid **Hantera skanningar**.

4. Anpassa en skanning enligt dina behov och klicka sedan på **Nästa**.
5. Markera rutan bredvid **Välj när det här jobbet ska utföras**.

Välj ett av motsvarande alternativ för att ställa in ett schema:

- Vid systemstart
- Dagligen
- Veckovis
- Månadsvis

Om du väljer Varje dag, Varje månad eller Varje vecka, drar du reglaget till önskad tidsperiod när den schemalagda skanningen ska starta.

Om du väljer att skapa en ny anpassad skanning visas fönstret **Skanningsjobb**. Härifrån kan du välja de platser du vill ska skannas.

10.4. Hur skapar jag ett anpassat skanningsjobb?

Om du vill skanna specifika platser på din enhet eller konfigurera skanningsalternativen konfigurerar och kör du ett anpassat skanningsjobb.

Gör enligt följande för att skapa ett anpassat skanningsjobb:

1. I panelen **VIRUSSKYDD** klickar du på **Öppna**
2. Klicka på **+Skapa skanning** bredvid **Hantera skanningar**.
3. I uppgiftsnamnsfältet skriver du ett namn på skanningen, väljer platser du vill ska skannas och sedan klickar du på **NÄSTA**.
4. Konfigurera dessa allmänna alternativ:
 - Skanna endast program**. Du kan konfigurera Bitdefender till att skanna endast öppnade appar.



- **Prioritet för skanningsjobb.** Du kan välja vilken inverkan en skanningsprocess ska ha på din systemprestanda.
 - Auto - Prioritet för skanningsprocessen beror på systemaktiviteten. För att se till att skanningsprocessen inte påverkar systemaktiviteten bestämmer Bitdefender om skanningsprocessen ska köras med hög eller låg prioritet.
 - Hög - Skanningsprocessens prioritet är hög. Genom att välja det här alternativet kommer du att tillåta andra program att köras långsammare och minska tiden som behövs för att skanningsprocessen ska slutföras.
 - Låg - Skanningsprocessens prioritet är låg. Genom att välja det här alternativet kommer du att tillåta andra program att köras snabbare och öka tiden som behövs för att skanningsprocessen ska slutföras.
 - **Efterskanningsåtgärder.** Välj vilken åtgärd Bitdefender ska utföra om inga hot upptäcks:
 - Visa sammanfattningsfönster
 - Stäng ned enhet
 - Stäng skanningsfönster
5. Om du vill konfigurera skanningsalternativen i detalj klickar du på **Visa avancerade alternativ**.
- Klicka **Nästa**.
6. Du kan aktivera alternativet **Schemalägg skanningsjobb** och sedan välja när den anpassade skanningen du skapade ska starta.
- Vid systemstart
 - Dagligen
 - Månadsvis
 - Veckovis
- Om du väljer Varje dag, Varje månad eller Varje vecka, drar du reglaget till önskad tidsperiod när den schemalagda skanningen ska starta.
7. Klicka på **Spara** för att spara inställningarna och stänga konfigurationsfönstret.



Beroende på de platser som ska skannas kan skanningen ta en stund. Om hot hittas under skanningsprocessen ombes du att välja åtgärder som ska vidtas för de hittade filerna.

Om du vill kan du snabbt köra om en föregående anpassad skanning genom att klicka på motsvarande post i den tillgängliga listan.

10.5. Hur undantar jag en mapp från att skannas?

Bitdefender tillåter undantag av specifika filer, mappar eller filändelsen från skanning.

Undantag ska användas av användare som har avancerad datorkunskap och endast i följande situationer:

- Du har en stor mapp på ditt system där du förvarar filmer och musik.
- Du har ett stort arkiv på ditt system där du förvarar olika data.
- Du har en mapp där du installerar olika typer av programvara och appar i testsyften. Skanning av mappen kan innebära att du förlorar vissa data.

Lägg till en mapp i undantagslistan:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. Klicka på fliken **Inställningar**.
4. Klicka på **Hantera undantag**.
5. Klicka på **+Lägg till undantag**.
6. Ange sökvägen till mappen du vill undanta från skanning i motsvarande fält.

Du kan även navigera till mappen genom att klicka på bläddra-knappen till höger i gränssnittet, välja den och klicka på **OK**.

7. Aktivera reglaget bredvid skyddsfunktionen som inte ska skanna mappen. Det finns tre alternativ:
 - Antivirus
 - Förebygga onlinehot
 - Avancerat hotskydd
8. Klicka **Spara** för att spara ändringarna och stänga fönstret.



10.6. Vad ska man göra när Bitdefender visar att en ren fil är infekterad?

Det finns tillfällen då Bitdefender av misstag flaggar en legitim fil som ett hot (en falsk positiv). För att rätta till det här felet lägger du till filen till området för Bitdefender-undantag:

1. Slå av Bitdefenders realtidsskydd:
 - a. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
 - b. I panelen **VIRUSSKYDD** klickar du på **Öppna**
 - c. I fönstret **Avancerat** stänger du av **Bitdefender Shield**.
Ett varningsfönster visas. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att realtidsskyddet ska vara inaktivt. Du kan inaktivera realtidsskyddet i 5, 15 eller 30 minuter, i en timme, permanent eller till en systemomstart.
2. Visa dolda objekt i Windows. Se i *"Hur visar jag dolda objekt i Windows?" (p. 65)* hur du gör det.
3. Återskapa filen från karantänområdet:
 - a. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
 - b. I panelen **VIRUSSKYDD** klickar du på **Öppna**
 - c. I fönstret **Inställningar** klickar du på **Hantera karantän**.
 - d. Välj filen och klicka sedan på **Återställ**.
4. Lägg till filen till undantagslistan. Se i *"Hur undantar jag en mapp från att skannas?" (p. 54)* hur du gör det.
Som standard lägger Bitdefender automatiskt till återställda filer i undantagslistan.
5. Slå på Bitdefender realtids-antiviruskydd.
6. Kontakta våra supportmedarbetare så att vi kan ta bort upptäckten av hotinformationsuppdateringen. Se i *"Be om hjälp" (p. 154)* hur du gör det.



10.7. Hur kontrollerar jag vilka hot Bitdefender upptäckte?

Varje gång en skanning utförs skapas en skanningslogg och Bitdefender registrerar de upptäckta problemen.

Skanningsloggen innehåller detaljerad information om de loggade skanningsprocesserna, som skanningsalternativ, skanningsmål, vilka hot som hittats samt vilka åtgärder som vidtagits på dessa hot.

Du kan öppna skanningsloggen direkt från guiden för skanning när skanningen slutförts, genom att klicka **VISA LOGG**.

Kontrollera en skanningslogg eller en upptäckt infektion vid ett senare tillfälle:

1. Klicka på **Meddelanden** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. På fliken **Alla** väljer du meddelandet som avser den senaste skanningen.

Här hittar du alla hotskanningshändelser, inklusive hot upptäckta av pågående skanning, användarinitierade skanningar och statusändringar för automatiska skanningar.

3. I meddelandelistan kan du kontrollera vilka skanningar som har utförts på senaste tiden. Klicka på ett meddelande för att visa information om det.
4. Öppna en skanningslogg genom att klicka på **Visa logg**.




11. PRIVACY PROTECTION

11.1. Hur vet jag att min onlinetransaktion är säker?

För att vara säker på att det du gör online förblir privat kan du använda webbläsaren som finns i Bitdefender för att skydda dina transaktioner och bankappar.

Bitdefender Safepay™ är en säker webbläsare designad för att skydda din kreditkortsinformation, kontonummer eller annan känslig information du kan ange på olika platser online.

För att se till att din onlineaktivitet är säker och privat:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I **SAFEPAY**-panelen klickar du på **Inställningar**.
3. I fönstren **Säker betalning** klickar du på **Öppna Säker betalning**.
4. Klicka på knappen  för att öppna det **virtuella tangentbordet**.

Använd det **virtuella tangentbordet** när du skriver känslig information som lösenord.

11.2. Hur tar jag bort en fil permanent med Bitdefender?

Om du vill ta bort en fil permanent från ditt system måste du ta bort data fysiskt från din hårddisk.

Bitdefender File Shredder hjälper dig att snabbt strimla filer eller mappar från enheten med kontextmenyn i Windows genom att följa de här stegen:

1. Högerklicka på filen eller mappen som du vill ta bort permanent, peka på Bitdefender och välj **File Shredder**.
2. Klicka på **Ta bort permanent** och bekräfta sedan att du vill fortsätta med processen.

Vänta medan Bitdefender slutför filborttagning.

3. Resultaten visas. Klicka på **SLUTFÖR** för att lämna guiden.



11.3. Hur kan jag manuellt återställa krypterade filer när återställningsprocessen misslyckas?

ifall krypterade filer inte kan återställas automatiskt kan du manuellt återställa dem genom att följa de här stegen:

1. Klicka på **Meddelanden** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. På fliken **Alla** markerar du information avseende det senast upptäckta ransomwarebeteendet som upptäckts och klickar sedan på **Krypterade filer**.
3. Listan med krypterade filer visas.
Klicka på **Återställ filer** för att fortsätta.
4. Ifall hela eller en del av återställningsprocessen misslyckas måste du välja den plats där de avkrypterade filerna ska sparas. Klicka på **Återställ plats** och välj sedan en plats på din dator.
5. Ett bekräftelsefönster visas.

Klicka på **Slutför** för att avsluta återställningsprocessen.

Filer med följande tillägg kan återställas ifall de blir krypterade:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb; .doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html; .ico; .jar; .java; .jpeg; .jpg; .js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp; .odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;



12. ANVÄNDBAR INFORMATION

12.1. Hur testar jag min säkerhetslösning?

För att vara säker på att din Bitdefender-produkt körs som den ska rekommenderar vi att du använder Eicar-testet.

Med Eicar-testet kan du kontrollera din säkerhetslösning med en säker fil utvecklad för detta ändamål.

Testa din säkerhetslösning:

1. Hämta testet från den officiella hemsidan för EICAR-organisationen <http://www.eicar.org/>.
2. Klicka på fliken **Antimalware-testfil**.
3. Klicka på **Hämta** i menyn på vänster sida.
4. Från **Hämtningsområde som använder standardprotokollet http** klickar du på testfilen **eicar.com**.
5. Du informeras om att den sida du försöker öppna innehåller EICAR-Test-File (inte ett hot).

Om du klickar på **Jag förstår riskerna, ta mig dit iallafall**, startar hämtningen testet och en Bitdefender-popup informerar dig om att ett hot upptäcktes.

Klicka på **Mer information** för att hitta mer information om den här åtgärden.

Om du inte får någon Bitdefender-avisering rekommenderar vi att du kontaktar Bitdefender för support såsom beskrivs i avsnitt "*Be om hjälp*" (p. 154).

12.2. Hur tar jag bort Bitdefender?

Om du vill ta bort Bitdefender Antivirus Plus:

● I Windows 7:

1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
3. Klicka på **TA BORT** i det fönster som visas.



4. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

● I Windows 8 och Windows 8.1:

1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **TA BORT** i det fönster som visas.
5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

● I Windows 10:

1. Klicka på **Start**, därefter på **Inställningar**.
2. Klicka på **System**-ikonen i området **Inställningar** och välj sedan **Appar**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
5. Klicka på **TA BORT** i det fönster som visas.
6. Vänta tills avinstallationen slutförts och starta sedan om ditt system.



Notera

Den här ominstallationsproceduren tar bort de anpassade inställningarna permanent.

12.3. Hur tar jag bort Bitdefender VPN?

Proceduren för att ta bort Bitdefender VPN liknar den du använder för att ta bort andra program från enheten:

● I Windows 7:

1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
2. Hitta **Bitdefender VPN** och välj **Avinstall**.
Vänta tills avinstallationsprocessen är slutförd.

● I Windows 8 och Windows 8.1:



1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
3. Hitta **Bitdefender VPN** och välj **Avinstall**.
Vänta tills avinstallationsprocessen är slutförd.


● I Windows 10:

1. Klicka på **Start**, därefter på Inställningar.
2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
3. Hitta **Bitdefender VPN** och välj **Avinstall**.
4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
Vänta tills avinstallationsprocessen är slutförd.


12.4. Hur tar jag bort tillägget Bitdefender Anti-tracker?

Beroende på vilken webbläsare du använder följer du de här stegen för att avinstallera tillägget Bitdefender Anti-tracker:

● Internet Explorer



1. Klicka på  bredvid sökfältet och välj sedan Hantera tillägg.
En lista med installerade tillägg visas.
2. Klicka på Bitdefender Anti-tracker.
3. Klicka på **Inaktivera** längst ned till höger.

● Google Chrome

1. Klicka på  bredvid sökfältet.
2. Välj **Fler verktyg** och därefter **Tillägg**.
En lista med installerade tillägg visas.
3. Klicka på **Ta bort** i kortet Bitdefender Anti-tracker.
4. Klicka på **Ta bort** i den popup-ruta som visas.

● Mozilla Firefox



1. Klicka på  bredvid sökfältet.
2. Välj **Tillägg** och därefter **Utökningar**.
En lista med installerade tillägg visas.
3. Klicka på  och välj sedan **Ta bort**.


12.5. Hur stänger jag automatiskt ned enheten när skanningen är klar?

Bitdefender erbjuder flera skanningsjobb som du kan använda för att vara säker på att systemet inte är infekterat av hot. Att skanna hela enheten kan ta längre tid att slutföra beroende på systemet hårdvaru- och programvarukonfiguration.

Av det skälet tillåter Bitdefender att du konfigurerar din produkt så att den stänger systemet så fort skanningen är klar.

Fundera på det här exemplet: du har avslutat ditt arbete och vill gå och lägga dig. Du vill att Bitdefender ska kontrollera hela ditt system.

Stänga ned enheten när Snabbskanning eller Systemskanning är klart:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstret **Skanningar** klickar du på  bredvid Snabbskanning eller Systemskanning och väljer **Redigera**.
4. Anpassa skanningen enligt dina behov och klicka på **Nästa**.
5. Markera rutan bredvid **Välj när den här uppgiften ska schemaläggas** och välj sedan när uppgiften ska starta.
Om du väljer Varje dag, Varje månad eller Varje vecka, drar du reglaget till önskad tidsperiod när den schemalagda skanningen ska starta.
6. Klicka **Spara**.

Stänga ned enheten när en anpassad skanning är klar:

1. Klicka på  bredvid den anpassade skanning som du skapat.



2. Klicka på **Nästa** och sedan på **Nästa** igen.
3. Markera rutan bredvid **Välj när den här uppgiften ska schemaläggas** och välj sedan när uppgiften ska starta.
4. Klicka **Spara**.

Om inga hot hittas stängs enheten ned.

Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem. Mer information finns på "*Guiden för Antiviruskanning*" (p. 79).

12.6. Hur konfigurerar jag Bitdefender för att använda en proxyanslutning till Internet?

Om din enhet ansluts till Internet via en proxyserver måste du konfigurera Bitdefender med proxyinställningarna. Normalt upptäcker och importerar Bitdefender automatiskt proxyinställningarna från ditt system.



Viktigt

Internet-anslutningar från hemmet använder vanligtvis inte en proxyserver. Som en tumregel ska du kontrollera och konfigurera proxyinställningarna för Bitdefender-programmet när uppdateringarna inte fungerar. Om Bitdefender kan uppdatera är den korrekt konfigurerad för att ansluta till Internet.

Hantera proxyinställningar:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. Gå till **Avancerat** fliken.
3. Aktivera **Proxy-server**.
4. Klicka på **Proxy-ändring**.
5. Det finns två alternativ för att ange proxyinställningarna:

- **Importera proxyinställningar från standardwebbläsare** - proxyinställningar för aktuell användare, extraherade från standardwebbläsaren. Om proxyservern kräver ett användarnamn och lösenord måste du skriva in dem i motsvarande fält.



Notera

Bitdefender kan importera proxy-inställningar från de mest populära webbläsarna, däribland de senaste versionerna av Microsoft Edge, Internet Explorer, Mozilla Firefox och Google Chrome.



- **Anpassade proxy-inställningar** - proxy-inställningar som du kan konfigurera själv. Följande inställningar måste specificeras:
 - **Adress** - skriv in proxyserverns IP.
 - **Port** - skriv in vilken port som Bitdefender använder för att ansluta till proxyservern.
 - **Användarnamn** - skriv in ett användarnamn som känns igen av proxy.
 - **Lösenord** - skriv in det giltiga lösenordet för den tidigare valde användaren.

6. Klicka **OK** för att spara ändringarna och stänga fönstret.

Bitdefender använder tillgängliga proxy-inställningar tills den kan ansluta till Internet.

12.7. Använder jag en 32-bitars eller en 64-bitars version av Windows?

Ta reda på om du har ett 32-bitars eller ett 64-bitars operativsystem:

● I Windows 7:

1. Klicka **Starta**.
2. Lokalisera **Dator** i **Start** menyn.
3. Högerklicka **Dator** och välj **Egenskaper**.
4. Se under **System** för att kontrollera informationen om ditt system.

● I Windows 8:

1. Från Windows Start-skärm, leta upp **Dator** (du kan till exempel börja skriva "Dator" direkt i startskärmen) och högerklicka sedan på dess ikon.

I **Windows 8.1** letar du upp **Den här datorn**.

2. Välj **Egenskaper** i menyn längst ned.
3. Titta i området System för att se din systemtyp.

● I Windows 10:

1. Skriv "System" i sökrutan från aktivitetsfältet och klicka sedan på dess ikon.
2. Titta i System-området för att hitta information om din systemtyp.



12.8. Hur visar jag dolda objekt i Windows?

Dessa steg är användbara i de fall där du arbetar med en situation med hot och behöver hitta och radera den infekterade filen, som kan vara dold.

Följ dessa steg för att visa dolda objekt i Windows:

1. Klicka på **Start** och gå sedan till **Kontrollpanelen**.

I **Windows 8 och Windows 8.1**: Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.

2. Välj **Mappalternativ**.
3. Gå till fliken **Visa**
4. Välj **Visa dolda filer och mappar**.
5. Avmarkera **Dölj tillägg för kända filtyper**.
6. Rensa **Dölj skyddade operativsystemfiler**.
7. Klicka på **Verkställ** och sedan på **OK**.

I **Windows 10**:

1. Skriv "Visa dolda filer och mappar" i sökrutan från aktivitetsfältet och klicka på ikonen.
2. Välj **Visa dolda filer, mappar och enheter**.
3. Avmarkera **Dölj tillägg för kända filtyper**.
4. Rensa **Dölj skyddade operativsystemfiler**.
5. Klicka på **Verkställ** och sedan på **OK**.

12.9. Hur tar jag bort andra säkerhetslösningar?

Den huvudsakliga orsaken för att använda en säkerhetslösning är för att tillhandahålla skydd och säkerhet för dina data. Men vad händer om man har fler än en säkerhetsprodukt på samma system?

När du använder fler än en säkerhetslösning på samma enhet blir systemet instabilt. Bitdefender Antivirus Plus installeraren upptäcker automatiskt andra säkerhetsprogram och ger dig möjlighet att avinstallera dessa.

Om du inte tog bort de andra säkerhetslösningarna under installationen:

- I **Windows 7**:



1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
2. Vänta ett ögonblick tills dess listan med installerade program visas.
3. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.
4. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

● I Windows 8 och Windows 8.1:

1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
3. Vänta ett ögonblick tills dess listan med installerade program visas.
4. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.
5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

● I Windows 10:

1. Klicka på **Start**, därefter på **Inställningar**.
2. Klicka på **System**-ikonen i området **Inställningar** och välj sedan **Appar**.
3. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.
4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

Om du misslyckas med att ta bort den andra säkerhetslösningen från ditt system, hämta avinstalleringsverktyget från försäljarens webbsida eller kontakta dem direkt för att få riktlinjer för avinstallering.

12.10. Hur startar jag om i Felsäkert läge?

Felsäkert läge är ett diagnosticerande driftläge som vanligtvis används för att söka efter problem som påverkar den vanliga driften av Windows. Den typen av problem sträcker sig från konflikter mellan enheter, till hot som förhindrar att Windows startas normalt. I felsäkert läge fungerar endast ett fåtal appar och Windows laddar bara de grundläggande drivrutinerna samt ett minimum av operativsystemets komponenter. Det är därför de flesta hot är inaktiva och enkelt kan tas bort när du kör Windows i felsäkert läge.

För att starta Windows i felsäkert läge:



● I Windows 7:

1. Starta om enheten.
2. Tryck tangenten **F8** flera gånger innan Windows startar för att nå boot-menyn.
3. Välj **Felsäkert läge** i boot-menyn eller **Felsäkert läge med nätverk** om du vill ha Internet-åtkomst.
4. Tryck **Enter** och vänta tills Windows laddas i Felsäkert läge.
5. Den här processen avslutas med ett bekräftelsemeddelande. Klicka på **OK** för att bekräfta.
6. För att starta Windows normalt, bara starta om systemet.

● I Windows 8, Windows 8.1 och Windows 10:

1. Starta **Systemkonfiguration** i Windows genom att samtidigt trycka på knapparna **Windows + R** på tangentbordet.
2. Skriv **msconfig** i dialogrutan **Öppna**, klicka därefter **OK**.
3. Välj fliken **Boot**.
4. I området **Startalternativ** markerar du kryssrutan **Säker start**.
5. Klicka på **Nätverk** och därefter **OK**.
6. Klicka **OK** i fönstret **Systemkonfiguration** som informerar dig om att systemet måste startas om för att kunna göra de ändringar du har ställt in.

Ditt system startar om i felsäkert läge med nätverksanslutning.

För att starta om i normalläge ställer du tillbaka inställningarna genom att starta **Systemdrift** igen och avmarkera kryssrutan **Säker start**. Klicka på **OK** och sedan på **Starta om**. Vänta tills de nya inställningarna tillämpas.



HANTERA DIN SÄKERHET



13. ANTIVIRUSSKYDD

Bitdefender skyddar din enhet från alla typer av hot (skadlig kod, trojaner, spionprogram, spökprogram osv). Skyddet som Bitdefender erbjuder delas in i två kategorier:

- **Skanning vid åtkomst** - förhindrar nya hot från att komma in i systemet. Bitdefender kan till exempel skanna ett Word-dokument efter kända hot när du öppnar det och ett e-postmeddelande när du får det.

Skanning vid åtkomst säkerställer realtidsskydd mot hot och är en viktig komponent i alla datorsäkerhetsprogram.



Viktigt

Förhindra hot från att infektera din enhet genom att ha **skanning vid åtkomst** aktiverat.

- **På begäran-skanning** - tillåter upptäckt och borttagning av hot som redan finns i systemet. Detta är en klassisk skanning som startats av användaren - du bestämmer vilken enhet, mapp eller fil som Bitdefender ska skanna, och Bitdefender skannar den på begäran.

Bitdefender skannar automatiskt alla borttagbara medier som är anslutna till enheten för att se till att den går att använda säkert. Mer information finns på "[Automatisk skanning av borttagbara medier](#)" (p. 82).

Avancerade användare kan konfigurera undantag från skanning om de inte vill att särskilda filer eller filtyper ska skannas. Mer information finns på "[Konfigurera skanningsundantag](#)" (p. 84).

När det upptäcker ett hot kommer Bitdefender automatiskt att försöka ta bort den skadliga koden från den infekterade filen och återställa originalfilen. Denna aktivitet är känd som desinfektering. Filer som inte kan desinfekteras flyttas till karantän för att stänga in smittan. Mer information finns på "[Hantera filer i karantän](#)" (p. 86).

Om din enhet har infekterats med virus finns mer information i "[Ta bort hot från ditt system](#)" (p. 146). För att hjälpa dig rensa enheten från hot som inte kan tas bort inifrån Windows-operativsystemet, tillhandahåller Bitdefender "[Räddningsmiljön](#)" (p. 146). Det här en betrodd miljö, särskilt utvecklad för att ta bort hot, vilket gör det möjligt för dig att starta din enhet oberoende av Windows. När enheten körs i felsäkert läge är Windows-hot inaktiva, vilket gör det enkelt att ta bort dem.



13.1. Skanning vid åtkomst (realtidsskydd)

Bitdefender ger realtidsskydd mot flera olika hot genom att skanna alla öppnade filer och e-postmeddelanden.

13.1.1. Stänga av eller slå på realtidsskydd

Stänga av eller slå på realtidsskydd mot hot:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstret **Avancerat** stänger du av eller slår på **Bitdefender Shield**.
4. Om du vill inaktivera realtidsskydd visas ett varningsfönster. Du måste bekräfta ditt val genom att i menyn välja hur länge du vill att realtidsskyddet ska vara inaktivt. Du kan inaktivera realtidsskyddet i 5, 15 eller 30 minuter, i en timme, permanent eller till en systemomstart. Realtidsskyddet slås automatiskt på när den valda tiden löper ut.



Varning

Det här är ett viktigt säkerhetsproblem. Vi rekommenderar att du inaktiverar realtidsskyddet under så kort tid som möjligt. Om realtidsskydd är inaktiverat är du inte skyddad mot hot.

13.1.2. Konfigurerar avancerade inställningar för realtidsskydd

Avancerade användare kan vilja dra fördel av de skanningsinställningar som Bitdefender erbjuder. Du kan konfigurera inställningarna för realtidsskyddet detaljerat genom att skapa en anpassad skyddsnivå.

Konfigurera avancerade inställningar för realtidsskydd:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstret **Avancerat** kan du konfigurera skanningsinställningarna efter behov.

Information om skanningsalternativ

Du kan finna denna information användbar:



- **Skanna endast program.** Du kan konfigurera Bitdefender till att skanna endast öppnade appar.
- **Skanna potentiellt oönskade program.** Välj det här alternativet för att skanna efter oönskade program. En eventuellt oönskad applikation (PUA) eller eventuellt oönskat program (PUP) är en programvara som oftast ingår i freewareprogram och som visar popup-rutor eller installerar ett verktygsfält i standardwebbläsaren. Vissa av dem ändrar hemsidan eller sökmotorn, andra kär flera processer i bakgrunden som gör datorn långsammare eller visar många annonser. De här programmen kan installeras utan ditt samtycke (kallas även adware) eller ingår som standard i expressinstallationspaketet (annonsstöd).
- **Skanna skript.** Med funktionen Skanna skript kan Bitdefender skanna powershell-skript och office-dokument som kan innehålla skriptbaserad skadlig kod.
- **Skanna nätverksresurser.** För att säkert komma åt ett fjärrnätverk från enheten rekommenderar vi att du har alternativet Skanna nätverksdelningar aktiverat.
- **Skanna arkiv.** Att skanna inne i arkiv är en långsam och resursintensiv process och rekommenderas därför inte för realtidsskydd. Arkiv som innehåller infekterade filer är inte ett direkt hot mot ditt systems säkerhet. Hotet kan endast påverka ditt system om den infekterade filen extraheras från arkivet och körs utan att realtidsskyddet är aktiverat.

Om du bestämmer dig för att använda det här alternativet aktiverar du det och drar sedan reglaget längs skalan för att exkludera skanning av arkiv som är längre än ett givet värde i MB (megabytes).

- **Skanna bootsektorer.** Du kan konfigurera Bitdefender att skanna startsektorerna på hårddisken. Den här sektorn på hårddisken innehåller den datorkod som behövs för att starta bootprocessen. När ett hot infekterar startsektorn kan enheten bli oåtkomlig och du kanske inte kan starta systemet och komma åt dina data.
- **Skanna endast nya och ändrade filer.** Genom att endast skanna nya och ändrade filer, kan du kraftigt förbättra systemets responsivitet med en minimal förlust av säkerhet.
- **Skanna efter tangentloggning.** Välj det här alternativet för att skanna systemet efter keyloggerappar. Keyloggers spelar in det du skriver på tangentbordet och skickar rapporter över Internet till en person med ont



uppsåt (hackare). Hackaren kan utvinna känslig information, såsom bankkontonummer och lösenord ur den stulna uppgifterna, och använda detta för att skaffa sig personliga fördelar.

- **Tidig uppstartsskanning.** Välj alternativet **Tidig startskanning** för att skanna systemet vid start så fort alla kritiska tjänster har laddats. Syftet med den här funktionen är att förbättra hotupptäckt vid systemstart och starttid för systemet.

Åtgärder som vidtas vid upptäckta hot

Du kan konfigurera de åtgärder som vidtas av realtidsskyddet genom att följa de här stegen:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstret **Avancerat** bläddrar du ner i fönstret tills du ser alternativet **Hothändelser**.
4. Konfigurera skanningsinställningarna efter behov.

Följande åtgärder kan vidtas av realtidsskyddet i Bitdefender:

Vidta rätt åtgärder

Bitdefender vidtar rekommenderade åtgärder beroende på typ av upptäckt fil:

- **Smittade filer.** Filer som upptäcks som infekterade matchar en del av den hotinformation som hittas i Bitdefenders hotinformationsdatabas. Bitdefender kommer automatiskt att försöka ta bort den skadliga koden från den infekterade filen och återställa originalfilen. Denna aktivitet är känd som desinfektering.

Filer som inte kan desinfekteras flyttas till karantän för att stänga in smittan. Filer i karantän kan inte utföras eller öppnas; därför försvinner risken att bli infekterad. Mer information finns på "*Hantera filer i karantän*" (p. 86).



Viktigt

För vissa typer av hot är desinfektion inte möjligt, eftersom den upptäckta filen är helt och hållet skadlig. Vid sådana tillfällen raderas den infekterade filen från enheten.



- **Misstänkta filer.** Filer har upptäckts som misstänkta av den heuristiska analysen. Misstänkta filer kan inte desinficeras eftersom ingen desinfektionsrutin finns tillgänglig. De flyttas till karantän för att förhindra en eventuell infektion.

Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefenders hotforskare. Om en hotnärvaro bekräftas släpps en hotinformationsuppdatering för att tillåta borttagning av hotet.

- **Arkiv som innehåller infekterade filer.**
 - Arkiv som endast innehåller infekterade filer tas bort automatiskt.
 - Om ett arkiv innehåller både infekterade och rena filer försöker Bitdefender att ta bort de infekterade filerna förutsatt att det går att rekonstruera arkivet med rena filer. Om en arkivrekonstruktion inte är möjlig, informeras du om att ingen åtgärd kan vidtas för att undvika förlora rena filer.

Flytta till karantän

Flyttar upptäckta filer till karantän. Filer i karantän kan inte utföras eller öppnas; därför försvinner risken att bli infekterad. Mer information finns på "[Hantera filer i karantän](#)" (p. 86).

Neka åtkomst

Om en infekterad fil hittas nekas åtkomst till den.

13.1.3. Återställa standardinställningarna

Standardinställningarna för realtidsskyddet försäkrar ett bra skydd mot hot, med liten påverkan på systemets prestanda.

För att återställa standardinställningarna för realtidsskyddet:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstret **Avancerat** bläddrar du ner i fönstret tills du ser alternativet **Återställ avancerade inställningar**. Välj det här alternativet för att återställa antivirusinställningarna till standard.



13.2. Skanning på begäran

Huvudmålet för Bitdefender är att hålla din enhet ren från hot. Detta görs genom att hålla nya hot borta från din enhet och genom att skanna dina e-postmeddelanden och alla nya filer som hämtas eller kopieras till ditt system.

Det finns en risk för att ett hot redan finns i systemet innan du ens installerar Bitdefender. Därför är det en god idé att skanna din enhet för befintliga hot efter att du installerat Bitdefender. Och det är definitivt en bra idé att regelbundet skanna enheten för hot.

På begäran-skanning baseras på skanningsuppgifter. Skanningsuppgifter specificerar skanningsalternativen och de objekt som ska skannas. Du kan när du vill skanna enheten genom att köra standarduppgifterna för dina egna skanningsuppgifter (användardefinierade uppgifter). Om du vill skanna specifika platser på din enhet eller konfigurera skanningsalternativen konfigurerar och kör du ett anpassat skanningsjobb.

13.2.1. Skanna en fil eller mapp för hot

Du borde alltid skanna filer och mappar när du misstänker att de kan vara infekterade. Högerklicka på de filer eller mappar du vill skanna, peka på **Bitdefender** och välj **Skanna med Bitdefender**. **Guiden för antiviruskanning** kommer att visas och leda dig genom skanningsprocessen. I slutet av skanningen ombes du att välja de åtgärder som ska vidtas för de upptäckta filerna, om det finns några.

13.2.2. Köra en snabbskanning

Snabbskanning använder skanning i "molnet" för att upptäcka hot som körs på ditt system. Att köra en snabbskanning tar vanligtvis under en minut och använder en bråkdel av de systemresurser som krävs vid en vanlig antiviruskanning.

Köra en snabbskanning:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstren **Skanningar** klickar du på knappen **Kör skanning** bredvid **Quick Scan**.



4. Följ guiden för **Antivirusskanning** för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer. Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

13.2.3. Kör en systemskanning

Systemskanningen skannar hela enheten efter alla typer av hot som är riskabla för säkerheten, som skadlig kod, spionprogramvara, adware, rootkits och annat.



Notera

Eftersom **Systemskanning** utför en noggrann skanning av hela systemet kan skanningen ta en stund. Därför rekommenderas du att köra det här jobbet när du inte använder din enhet.

Innan du kör en skanning rekommenderas följande:

- Se till att Bitdefender är uppdaterad med sin hotinformationsdatabas. Om du skannar enheten med en utdaterad hotinformationsdatabas kan Bitdefender förhindras från att upptäcka nya hot som hittats sedan den senaste uppdateringen. Mer information finns på "*Se till att Bitdefender är uppdaterad*" (p. 37).
- Stäng ned alla öppna program.

Om du vill skanna specifika platser på din enhet eller konfigurera skanningsalternativen konfigurerar och kör du ett anpassat skanningsjobb. Mer information finns på "*Konfigurera en anpassad skanning*" (p. 76).

Köra en systemskanning:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstren **Skanningar** klickar du på knappen **Kör skanning** bredvid **Systemskanning**.
4. Första gången du kör en systemskanning presenteras du för funktionen. Klicka **Jag förstår** för att fortsätta.
5. Följ guiden för **Antivirusskanning** för att slutföra skanningen. Bitdefender vidtar automatiskt rekommenderade åtgärder på upptäckta filer. Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.



13.2.4. Konfigurera en anpassad skanning

I fönstret **Hantera skanningar** kan du ställa in Bitdefender på att köra skanningar när du anser att din enhet behöver kontrolleras för eventuella hot. Du kan välja att schemalägga en **Systemskanning** eller en **Snabbskanning**, eller så kan du skapa en anpassad skanning när det passar dig.

Konfigurera en ny anpassad skanning i detalj:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstren **Skanningar** klickar du på **+Skapa skanning**.
4. I fältet **Uppgiftsnamn** skriver du ett namn på skanningen, sedan väljer du platser du vill ska skannas och sedan klickar du på **Nästa**.
5. Konfigurera dessa allmänna alternativ:
 - **Skanna endast program**. Du kan konfigurera Bitdefender till att skanna endast öppnade appar.
 - **Prioritet för skanningsjobb**. Du kan välja vilken inverkan en skanningsprocess ska ha på din systemprestanda.
 - Auto - Prioritet för skanningsprocessen beror på systemaktiviteten. För att se till att skanningsprocessen inte påverkar systemaktiviteten bestämmer Bitdefender om skanningsprocessen ska köras med hög eller låg prioritet.
 - Hög - Skanningsprocessens prioritet är hög. Genom att välja det här alternativet kommer du att tillåta andra program att köras långsammare och minska tiden som behövs för att skanningsprocessen ska slutföras.
 - Låg - Skanningsprocessens prioritet är låg. Genom att välja det här alternativet kommer du att tillåta andra program att köras snabbare och öka tiden som behövs för att skanningsprocessen ska slutföras.
 - **Efterskanningsåtgärder**. Välj vilken åtgärd Bitdefender ska utföra om inga hot upptäcks:
 - Visa sammanfattningsfönster
 - Stäng ned enhet
 - Stäng skanningsfönster



6. Om du vill konfigurera skanningsalternativen i detalj klickar du på **Visa avancerade alternativ**. Du kan hitta information om de listade skanningarna i slutet av det här avsnittet.

Klicka **Nästa**.

7. Du kan aktivera **Schemalägg skanningsjobb** om du vill och sedan välja när den anpassade skanningen du skapade ska starta.

- Vid systemstart
- Dagligen
- Månadsvis
- Veckovis

Om du väljer Varje dag, Varje månad eller Varje vecka, drar du reglaget till önskad tidsperiod när den schemalagda skanningen ska starta.

8. Klicka på **Spara** för att spara inställningarna och stänga konfigurationsfönstret.

Beroende på de platser som ska skannas kan skanningen ta en stund. Om hot hittas under skanningsprocessen ombes du att välja åtgärder som ska vidtas för de hittade filerna.

Information om skanningsalternativ

Du kan finna denna information användbar:

- Om du inte är bekant med några av dessa termer, kontrollera dem i **ordlistan**. Du kan också hitta användbar information genom att söka på Internet.
- **Skanna potentiellt oönskade program.** Välj det här alternativet för att skanna efter oönskade program. En eventuellt oönskad applikation (PUA) eller eventuellt oönskat program (PUP) är en programvara som oftast ingår i freewareprogram och som visar popup-rutor eller installerar ett verktygsfält i standardwebbläsaren. Vissa av dem ändrar hemsidan eller sökmotorn, andra kär flera processer i bakgrunden som gör datorn långsammare eller visar många annonser. De här programmen kan installeras utan ditt samtycke (kallas även adware) eller ingår som standard i expressinstallationspaketet (annonsstöd).
- **Skanna arkiv.** Arkiv som innehåller infekterade filer är inte ett direkt hot mot ditt systems säkerhet. Hotet kan endast påverka ditt system om den



infekterade filen extraheras från arkivet och körs utan att realtidsskyddet är aktiverat. Det rekommenderas dock att använda det här alternativet för att upptäcka och ta bort alla potentiella hot, även om det inte är ett direkt hot.

Dra reglaget längs skalan för att exkludera arkiv som är längre än ett givet värde i MB (megabytes) från skanning.



Notera

Skanning av arkiverade filer ökar den totala skanningstiden och kräver högre systemresurser.

- **Skanna endast nya och ändrade filer.** Genom att endast skanna nya och ändrade filer, kan du kraftigt förbättra systemets responsivitet med en minimal förlust av säkerhet.
- **Skanna bootsektorer.** Du kan konfigurera Bitdefender att skanna startsektorerna på hårddisken. Den här sektorn på hårddisken innehåller den datorkod som behövs för att starta bootprocessen. När ett hot infekterar startsektorn kan enheten bli oåtkomlig och du kanske inte kan starta systemet och komma åt dina data.
- **Skanna minne.** Välj det här alternativet för att skanna program som körs i systemets minne.
- **Skanna register.** Välj det här alternativet för att skanna registernycklar. Windows Registry är en databas som lagrar konfigurationsinställningar och alternativ för systemkomponenter i Windows operativsystem, samt för installerade appar.
- **Skanna cookies.** Välj det här alternativet för att skanna de cookies som din webbläsare har lagrat på enheten.
- **Skanna efter tangentloggning.** Välj det här alternativet för att skanna systemet efter keyloggerappar. Keyloggers spelar in det du skriver på tangentbordet och skickar rapporter över Internet till en person med ont uppsåt (hackare). Hackaren kan utvinna känslig information, såsom bankkontonummer och lösenord ur den stulna uppgifterna, och använda detta för att skaffa sig personliga fördelar.



13.2.5. Guiden för Antiviruskanning

När du än inleder en på begäranskanning (till exempel högerklickar på en mapp, pekar på Bitdefender och väljer **Skanna med Bitdefender**), kommer Bitdefenders guide för antiviruskanning att visas. Följ guiden för att slutföra skanningsprocessen.



Notera

Om guiden för skanning inte visas kan skanningen vara konfigurerad att köras tyst i bakgrunden. Sök efter **B** ikonerna för skanningsframgång i **systemfältet**. Du kan klicka på den här ikonen för att öppna skanningsfönstret och se skanningsframgången.

Steg 1 - Utför skanning

Bitdefender kommer att börja skanna de valda objekten. Du kan se realtidsinformation om skanningsstatus och statistik (däribland förfluten tid, en uppskattning av återstående tid och antalet upptäckta hot).

Vänta medan Bitdefender slutför skanningen. Skanningsprocessen kan ta en stund beroende på hur komplicerad den är.

Stoppar eller pausar skanningen. Du kan stoppa skanningen när du vill genom att klicka på **STOPP**. Du kommer att gå direkt till att se guidens sista steg. För att tillfälligt stoppa skanningsprocessen klickar du bara på **Pause**. Du måste klicka på **FORTSÄTT** för att återuppta skanningen.

Lösenordsskyddade arkiv. När ett lösenordsskyddat arkiv upptäcks, beroende på skanningsinställningarna, kan du bli ombedd att skriva in lösenordet. Lösenordsskyddade arkiv kan inte skannas om du inte skriver in lösenordet. Följande alternativ är tillgängliga:

- **Lösenord.** Om du vill att Bitdefender ska skanna arkivet, välj detta alternativ och skriv in lösenordet. Om du inte kan lösenordet, välj ett av de andra alternativen.
- **Fråga inte efter lösenordet och hoppa över denna post för skanning.** Välj det här alternativet för att hoppa över skanning av det här arkivet.
- **Hoppa över alla lösenordsskyddade poster utan att skanna dem.** Välj detta alternativ om du ej vill störas om lösenordsskyddade arkiv. Bitdefender kommer inte att kunna skanna dem, men ett register kommer att finnas i skanningsloggen.



Välj önskat alternativ och klicka på **OK** för att fortsätta skanningen.

Steg 2 - Välj åtgärder

I slutet av skanningen ombes du att välja de åtgärder som ska vidtas för de upptäckta filerna, om det finns några.



Notera

När du kör en snabbskanning eller en systemskanning vidtar Bitdefender automatiskt rekommenderade åtgärder på upptäckta filer under skanningen. Om olösta hot återstår uppmanas du att välja vilka åtgärder som ska vidtas mot dem.

De infekterade objekten visas i grupper baserade på vilken typ av hot de är infekterade med. Klicka länken som motsvarar ett hot för att få mer information om de infekterade objekten.

Du kan välja en omfattande åtgärd som ska tas på alla problem, eller så kan du välja separata åtgärder för varje problemgrupp. Ett eller flera av följande alternativ kan visas i menyn:

Vidta rätt åtgärder

Bitdefender vidtar rekommenderade åtgärder beroende på typ av upptäckt fil:

- **Smittade filer.** Filer som upptäcks som infekterade matchar en del av den hotinformation som hittas i Bitdefenders hotinformationsdatabas. Bitdefender kommer automatiskt att försöka ta bort den skadliga koden från den infekterade filen och återställa originalfilen. Denna aktivitet är känd som desinfektering.

Filer som inte kan desinfekteras flyttas till karantän för att stänga in smittan. Filer i karantän kan inte utföras eller öppnas; därför försvinner risken att bli infekterad. Mer information finns på "[Hantera filer i karantän](#)" (p. 86).



Viktigt

För vissa typer av hot är desinfektion inte möjligt, eftersom den upptäckta filen är helt och hållet skadlig. Vid sådana tillfällen raderas den infekterade filen från enheten.

- **Misstänkta filer.** Filer har upptäckts som misstänkta av den heuristiska analysen. Misstänkta filer kan inte desinficeras eftersom ingen



desinfektionsrutin finns tillgänglig. De flyttas till karantän för att förhindra en eventuell infektion.

Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefenders hotforskare. Om en hotnärvaro bekräftas släpps en informationsuppdatering för att tillåta borttagning av hotet.

- **Arkiv som innehåller infekterade filer.**
 - Arkiv som endast innehåller infekterade filer tas bort automatiskt.
 - Om ett arkiv innehåller både infekterade och rena filer försöker Bitdefender att ta bort de infekterade filerna förutsatt att det går att rekonstruera arkivet med rena filer. Om en arkivrekonstruktion inte är möjlig, informeras du om att ingen åtgärd kan vidtas för att undvika förlora rena filer.

Radera

Tar bort upptäckta filer från enheten.

Om infekterade filer lagras i ett arkiv tillsammans med rena filer försöker Bitdefender ta bort de infekterade filerna och bygga om arkivet med de rena filerna. Om en arkivrekonstruktion inte är möjlig, informeras du om att ingen åtgärd kan vidtas för att undvika förlora rena filer.

Vidta ingen åtgärd.

Ingen åtgärd kommer att tas på de upptäckta filerna. När skanningen är slutförd kan du öppna skanningsloggen för att se information om dessa filer.

Klicka **Fortsätt** för att tillämpa den valda åtgärden.

Steg 3 - Sammanfattning

När Bitdefender är färdig med att lösa problemen kommer skanningsresultaten att visas i ett nytt fönster. Om du vill få omfattande information om skanningsprocessen, klicka **VISA LOGG** för att visa skanningsloggen.



Viktigt

I de flesta fall lyckas Bitdefender desinficera de infekterade filer den upptäcker, annars isolerar den infektionen. Dock finns det problem som inte kan lösas automatiskt. Om det krävs startar du om systemet för att slutföra



rensningsprocessen. Mer information och instruktioner om hur du tar bort ett hot manuellt finns i "*Ta bort hot från ditt system*" (p. 146).

13.2.6. Kontrollera skanningsloggar

Varje gång en skanning utförs skapas en skanningslogg och Bitdefender registrerar de upptäckta problemen i fönstret Antivirus. Skanningsloggen innehåller detaljerad information om de loggade skanningsprocesserna, som skanningsalternativ, skanningsmål, vilka hot som hittats samt vilka åtgärder som vidtagits på dessa hot.

Du kan öppna skanningsloggen direkt från guiden för skanning när skanningen slutförts, genom att klicka **VISA LOGG**.

Kontrollera en skanningslogg eller en upptäckt infektion vid ett senare tillfälle:

1. Klicka på **Meddelanden** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. På fliken **Alla** väljer du meddelandet som avser den senaste skanningen.

Här hittar du alla hotskanningshändelser, inklusive hot upptäckta av pågående skanning, användarinitierade skanningar och statusändringar för automatiska skanningar.

3. I meddelandelistan kan du kontrollera vilka skanningar som har utförts på senaste tiden. Klicka på ett meddelande för att visa information om det.
4. Öppna skanningsloggen genom att klicka på **Visa logg**.

13.3. Automatisk skanning av borttagbara medier

Bitdefender upptäcker automatiskt när du ansluter en flyttbar lagringsenhet till din enhet och skannar den i bakgrunden när alternativet Autoskanning är aktiverad. Detta rekommenderas för att förhindra hot från att infektera enheten.

Upptäckta enheter placeras i en av dessa kategorier:


- CDs/DVDs
- Flash-enheter, som flash-stickor och externa hårddiskar
- kartlagda (fjärr) nätverksenheter

Du kan konfigurera automatisk skanning separat för varje kategori lagringsenheter. Automatisk skanning av mappade nätverksenheter är inaktiverat som standard.



13.3.1. Hur fungerar det?

När Bitdefender upptäcker en borttagbar lagringsenhet börjar den skanna efter hot (förutsatt att automatisk skanning är aktiverat för den typen av enhet). Du meddelas via ett popup-fönster att en ny enhet har upptäckts och att den skannas.

En Bitdefender-skanningsikon  visas i **systemfältet**. Du kan klicka på den här ikonen för att öppna skanningsfönstret och se skanningsframgången.

När skanningen är klar visas skanningsresultatfönstret för att informera dig om du säkert kan öppna filer på det borttagbara mediet.

I de flesta fall tar Bitdefender automatiskt bort upptäckta hot eller isolerar infekterade filer i karantän. Om olösta hot återstår efter skanningen uppmanas du att välja vilka åtgärder som ska vidtas mot dem.



Notera

Tänk på att inga åtgärder kan vidtas för infekterade eller misstänkta filer som hittas på CD-/DVD-skivor. På samma sätt kan inga åtgärder vidtas för infekterade eller misstänkta filer som upptäcks på mappade nätverksenheter om du inte har rätt behörigheter.

Den här informationen kan vara användbar för dig:

- Var försiktig när du använder en hotinfekterad CD/DVD, eftersom hotet inte kan tas bort från disken (mediet är skrivskyddat). Se till att realtidsskydd är aktiverat för att förhindra hot från att spridas till ditt system. Det är bästa praxis att kopiera alla värdefulla data från skivan till ditt system och sedan kasta bort skivan.
- I vissa fall kan inte Bitdefender ta bort hot från specifika filer på grund av juridiska eller tekniska begränsningar. Ett sådant exempel är filer som arkiverats med en egen teknik (det är för att arkivet inte kan rekonstrueras korrekt).

Information om hur du hanterar hot finns i "*Ta bort hot från ditt system*" (p. 146).

13.3.2. Hantera skanning av borttagbara medier

Hantera automatisk skanning av borttagbara medier:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**



3. Välj fönstret **Inställningar**.

Skanningsalternativen är förkonfigurerade för bästa upptäcktsresultat. Om smittade filer hittas försöker Bitdefender desinfektera dem (ta bort den skadliga koden) eller flytta dem till karantän. Om båda åtgärderna misslyckas, kommer guiden för Antivirus-skanning att låta dig välja andra åtgärder att ta till mot infekterade filer. Skanningsalternativen är standard och du kan inte ändra dem.

För bästa skydd rekommenderar vi att alternativet **Autoskanning** är markerat för alla typer av borttagbara lagringsenheter.

13.4. Skanna världens fil

Världens filer kommer som standard med installationen av operativsystemet och används för att mappa värddamn till IP-adresser varje gång du öppnar en ny webbsida, ansluter till en FTP eller till andra Internet-servrar. Det är vanlig textfil och skadliga program kan ändra den. Avancerade användare vet hur de ska använda den för att blockera irriterande annonser, banners, tredjepartscookies eller kapare.

Konfigurera skanning av värdfil:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. Gå till **Avancerat** fliken.
3. Aktivera eller inaktivera **Skanna värdfil**.

13.5. Konfigurera skanningsundantag

Bitdefender tillåter undantag av specifika filer, mappar eller filändelsen från skanning. Den här funktionen är avsedd för att undvika att du störs i ditt arbete och den kan också bidra till att förbättra systemprestanda. Undantag ska användas av användare som har avancerad datorkunskap eller som annars följer rekommendationerna från en Bitdefender-medarbetare.

Du kan konfigurera undantag att gälla endast för vid åtkomst- eller på begäran-skanning, eller för båda. De objekt som exkluderas från en på begäran-skanning kommer inte att skannas även om de öppnas av dig eller ett program.



Notera

Undantag kommer INTE att tillämpas på kontextskanning. Innehållsskanning är en typ av på begäran-skanning: du högerklickar filen eller mappen du vill söka igenom och väljer **Skanna med Bitdefender**.

13.5.1. Undanta filer och mappar från skanning

Undanta specifika filer och mappar från skanning:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstret **Inställningar** klickar du på **Hantera undantag**.
4. Klicka på **+Lägg till undantag**.
5. Ange sökvägen till mappen du vill undanta från skanning i motsvarande fält.

Du kan även navigera till mappen genom att klicka på bläddra-knappen till höger i gränssnittet, välja den och klicka på **OK**.

6. Aktivera reglaget bredvid skyddsfunktionen som inte ska skanna mappen. Det finns tre alternativ:
 - Antivirus
 - Förebygga onlinehot
 - Avancerat hotskydd
7. Klicka **Spara** för att spara ändringarna och stänga fönstret.

13.5.2. Undanta filtillägg från skanning

När du undantar ett filtillägg från skanning, skannar Bitdefender inte längre filer med det tillägget, oavsett var de finns på din enhet. Undantaget gäller även filer på borttagbara medier, som CD-skivor, DVD-skivor, USB-lagringsenheter eller nätverksenheter.



Viktigt

Var försiktig när du undantar filtillägg från skanning eftersom sådana undantag kan göra enheten mer sårbar för hot.

Undanta filtillägg från skanning:




1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstret **Inställningar** klickar du på **Hantera undantag**.
4. Klicka på **+Lägg till undantag**.
5. Skriv in de filtillägg som du vill ska undantas från skanning med en punkt framför dem, separerade med semikolon (;).
txt;avi;jpg
6. Aktivera reglaget bredvid skyddsfunktionen som inte ska skanna filtillägget.
7. Klicka **Spara**.

13.5.3. Hantera skanningsundantag

Om de inställda undantagen från skanning inte längre behövs rekommenderar vi att du raderar dem eller inaktiverar skanningsundantag.

Hantera skanningsundantag:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstret **Inställningar** klickar du på **Hantera undantag**. En lista med alla dina undantag visas.
4. För att ta bort eller redigera skanningsundantag klickar du på en av de tillgängliga knapparna. Fortsätt enligt följande:
 - För att ta bort en post från listan klickar du på knappen  bredvid den.
 - För att redigera en post i tabellen, klicka på knappen **Redigera** bredvid den. Ett nytt fönster visas där du kan ändra det tillägg eller den sökväg som ska undantas och den typ av säkerhetsfunktion du vill att de ska undantas från, efter behov. Gör de nödvändiga ändringarna och klicka sedan på **ÄNDRA**.

13.6. Hantera filer i karantän

Bitdefender isolerar de hotinfekterade filerna den inte kan desinfektera och de misstänkta filerna i ett säkert område som kallas karantän. När ett hot



är satt i karantän kan det inte göra någon skada eftersom det inte kan köras eller läsas.

Som standard skickas filer i karantän automatiskt till Bitdefender Labs för att analyseras av Bitdefenders hotforskare. Om en hotnärvaro bekräftas släpps en informationsuppdatering för att tillåta borttagning av hotet.

Dessutom skannar Bitdefender filerna som är satta i karantän varje gång hotinformationsdatabasen uppdateras. Rengjorda filer flyttas automatiskt tillbaka till sin ursprungliga plats.

Kontrollera och hantera filer i karantän:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. Gå till fönstret **Inställningar**.

Här kan du visa namnet på filerna i karantän, deras ursprungliga plats och namnet på de upptäckta hoten.

4. Filer satta i karantän hanteras automatiskt av Bitdefender enligt standardinställningarna för karantän.

Även om det inte rekommenderas kan du justera karantäninställningarna enligt dina önskemål genom att klicka på **Visa inställningar**.

Klicka på reglagen för att aktivera eller inaktivera:

Skanna om karantän efter uppdatering av information

Behåll detta alternativ aktiverat för att automatiskt skanna filer i karantän varje gång hotinformationsdatabas uppdateras. Rengjorda filer flyttas automatiskt tillbaka till sin ursprungliga plats.

Ta bort innehåll äldre än 30 dagar

Filer i karantän äldre än 30 dagar raderas automatiskt.

Skapa undantag för återställda filer

De filer du återställer från karantän flyttas tillbaka till sin ursprungliga plats utan att repareras och undantas automatiskt från kommande skanningar.

5. För att radera en fil i karantän, markera den och klicka knappen **Radera**. Om du vill återställa en fil från karantän till sin ursprungliga plats, välj den och klicka **Återställ**.



14. AVANCERAT HOTSKYDD

Bitdefender Advanced Threat Defense är en innovativ proaktiv detekteringsteknologi som använder avancerade heuristiska metoder för att upptäcka ransomware och andra nya eventuella hot i realtid.

Advanced Threat Defense övervakar kontinuerligt de appar som körs på enheten på jakt efter hotlika aktiviteter. Alla dessa åtgärder poängsätts och en total poäng räknas ut för varje process.

Som en säkerhetsåtgärd meddelas du varje gång hot och eventuellt skadliga processer upptäcks och blockeras.

14.1. Aktivera eller inaktivera Advanced Threat Defense

Aktivera eller inaktivera Advanced Threat Defense:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **ADVANCED THREAT DEFENSE** klickar du på **Öppna**.
3. Gå till fönstret **Inställningar** och klicka på reglaget bredvid **Bitdefender Advanced Threat Defense**.



Notera

För att systemet ska vara skyddat mot ransomware och andra hot rekommenderar vi att du inaktiverar Advanced Threat Defense under så kort tid som möjligt.

14.2. Kontrollera upptäckta skadliga attacker

Varje gång hot eller potentiellt skadliga processer upptäcks blockerar Bitdefender dem för att förhindra att enheten infekteras av ransomware eller annan skadlig kod. Du kan när som helst kontrollera listan med upptäckta skadliga attacker genom att följa de här stegen:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **ADVANCED THREAT DEFENSE** klickar du på **Öppna**.
3. Gå till fönstret **Threat Defense**.

De attacker som upptäckts under de senaste 90 dagarna visas. För att visa information om typen av upptäckt ransomware, sökvägen till den



skadliga processen eller om desinfektionen har lyckats, klickar du bara på det.

14.3. Lägg till processer till undantag

Du kan konfigurera uteslutningsregler för betrodda program så att Advanced Threat Defense inte blockerar dem om de utför hotliknande åtgärder.

Börja lägga till processer till undantagslistan för Advanced Threat Defense:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **ADVANCED THREAT DEFENSE** klickar du på **Öppna**.
3. I fönstret **Inställningar** klickar du på **Hantera undantag**.
4. Klicka på **+Lägg till undantag**.
5. Ange sökvägen till mappen du vill undanta från skanning i motsvarande fält.

Du kan även navigera till program genom att klicka på bläddra-knappen till höger i gränssnittet, välja den och klicka på **OK**.

6. Aktivera reglaget bredvid **Advanced Threat Defense**.
7. Klicka **Spara**.

14.4. Upptäckt av exploateringar

Ett sätt som hackare använder för att bryta sig in i system är att utnyttja särskilda buggar eller sårbarheter som finns i datorprogramvara (appar eller plugin-program) och hårdvara. För att säkerställa att din enhet hålls borta från sådana attacker, som normalt sprider sig mycket fort, använder Bitdefender de senaste antiexploateringsteknikerna.

Aktivera eller inaktivera exploateringsupptäckt

Aktivera eller inaktivera exploateringsupptäckt:

- Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
- I panelen **ADVANCED THREAT DEFENSE** klickar du på **Öppna**.
- Gå till fönstret **Inställningar** och klicka på reglaget bredvid **Exploit detection** för att aktivera eller inaktivera funktionen.



Notera

Alternativet Exploateringsupptäckt aktiveras som standard.



15. FÖREBYGGA ONLINEHOT

Bitdefender Online Threat Prevention säkerställer en säker surfupplevelse genom att varna dig om möjliga skadliga webbsidor.

Bitdefender tillhandahåller förebyggande av onlinehot för:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Konfigurera inställningar för förebyggande av onlinehot:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **FÖREBYGGANDE AV ONLINEHOT** klickar du på **Inställningar**.

I avsnittet **Webbskydd** klickar du på reglagen för att aktivera eller inaktivera:

- Förebyggande av webbattacker blockerar hot som kommer från Internet, däribland drive-by-nedladdningar.
- Search Advisor, en komponent som rankar resultat från dina sökmotorfrågor och de länkar som publicerats på sociala nätverk genom att placera en ikon bredvid varje resultat:
 - Du bör inte besöka den här webbsidan.
 - Den här webbsidan kan innehålla farligt innehåll. Iaktta försiktighet om du besöker den.
 - Det här är en säker sida att besöka.

Search Advisor rankar resultaten från följande sökmotorer:

- Google
- Yahoo!
- Bing
- Baidu

Search Advisor rankar länkar som publicerats på följande sociala nätverkstjänster:

- Facebook



- Twitter

- Krypterad webbskanning.

Mer sofistikerade attacker kan använda säker webbftrafik för att missleda sina offer. Därför rekommenderar vi att du har alternativet Krypterad webbskanning aktiverat.


- Dataskydd.

- Skydd mot nätfiske.

Bläddra ner tills du hittar avsnittet **Förhindrande av nätverkshot**. Här har du alternativet **Förhindrande av nätverkshot**. För att hålla enheten borta från attacker från komplexa skadeprogram (som ransomware) via exploatering av säkerhetsbrister ska du ha det här alternativet aktiverat.

Du kan skapa en lista över webbplatser, domäner och IP-adresser som inte skannas av antihot-, antinätfiske- och antibedrägerimotorerna i Bitdefender. Listan ska endast innehålla webbplatser, domäner och IP-adresser som du litar helt på.

Konfigurera och hantera webbplatser, domäner och IP-adresser via funktionen Online Threat Prevention från Bitdefender:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **FÖREBYGGANDE AV ONLINEHOT** klickar du på **Inställningar**.
3. Klicka på **Hantera undantag**.
4. Klicka på **+Lägg till undantag**.
5. Skriv namnet på webbplatsen, domänen eller IP-adressen du vill lägga till i undantagen i motsvarande fält.
6. Klicka på reglaget bredvid **Onlinehotskydd**.
7. För att ta bort en post från listan klickar du på knappen  bredvid den. Klicka **Spara** för att spara ändringarna och stänga fönstret.

15.1. Bitdefender-varningar i webbläsaren

Varje gång du försöker besöka en webbplats som är klassad som osäker blockeras webbplatsen och en varningssida visas i webbläsaren.

Den här sidan innehåller information som webbplats-URL och upptäckta hot.



Du måste bestämma vad som ska göras härnäst. Följande alternativ är tillgängliga:

- Navigera bort från webbplatsen genom att klicka på **TA MIG TILLBAKA TILL SÄKERHETEN**.
- Fortsätt till webbplatsen, trots varningen, genom att klicka på **Jag förstår risken, ta mig dit ändå**.
- Om du är säker på att den hittade webbplatsen är säker klickar du på **SKICKA** för att lägga till den i undantagen. Vi rekommenderar att du bara lägger till webbplatser du verkligen litar på.



16. SÄKERHETSRISK

Ett viktig steg för att skydda din enhet mot skadliga aktiviteter och program är att se till att operativsystemet och de appar du regelbundet använder är uppdaterade. Dessutom måste starka lösenord (lösenord som inte enkelt kan gissas) konfigureras för varje Windows-användarkonto och för de Wi-Fi-nätverk du ansluter till, för att förhindra obehörig fysisk åtkomst till din enhet.

Bitdefender har två enkla sätt att åtgärda säkerhetsbristerna i ditt system:

- Du kan skanna systemet efter säkerhetsbrister och åtgärda dem steg för steg genom att använda alternativet **Sårbarhetsskanning**.
- Med automatisk sårbarhetsövervakning kan du kontrollera och åtgärda upptäckta säkerhetsbrister i fönstret **Meddelanden**.

Du bör kontrollera och åtgärda systemsäkerhetsbrister varje eller varannan vecka.

16.1. Skanna systemet för säkerhetsrisker

För att hitta systemsårbarheter kräver Bitdefender en aktiv Internet-anslutning.

Skanna systemet för säkerhetsrisker:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I rutan **SÅRBARHET** klickar du på **Öppna**.
3. På fliken **Sårbarhetsskanning** klickar du på **Starta skanning** och vänta på att Bitdefender kontrollerar ditt system för sårbarheter. De upptäckta sårbarheterna är grupperade i tre kategorier:

● OPERATIVSYSTEM

● Operativsystemssäkerhet

Ändrade systeminställningar kan påverka din enhet och dina data så att varningar inte visas när programfiler gör ändringar i ditt system utan ditt godkännande eller när MTP-enheter såsom telefoner eller kameror ansluter och öppnar olika operationer utan din vetskap.

● Kritiska Windows-uppdateringar



En lista över kritiska Windows-uppdateringar som inte är installerade på datorn visas. En systemomstart kan krävas för att Bitdefender ska avsluta installationen. Observera att det kan ta en stund att installera uppdateringarna.

● Svaga Windows-konton

Du kan se den ändrade listan över Windows-användarkonton på din enhet, och skyddsnivån deras lösenord håller. Du kan välja mellan att be användaren ändra lösenordet vid nästa inloggning eller ändra lösenordet själv direkt. Ange ett nytt lösenord för systemet genom att välja **Byt lösenord nu**.

För att skapa ett starkt lösenord rekommenderar vi att du använder en kombination av versaler och gemener, siffror och specialtecken (som till exempel #, \$ eller @).

● APPLIKATIONER

● Webbbläsarsäkerhet

Ändring av enhetens inställningar som gör att du kan köra filer och program som laddas ner via Internet Explorer utan någon integritetsvalidering som kan leda till att din enhet komprometteras.

● Programuppdateringar

Klicka på namnet i listan för att se information om den app som måste uppdateras.

Om en app inte är uppdaterad klickar du på **Ladda ner ny version** för att hämta den senaste versionen.

● NÄTVERK

● Nätverk och behörigheter

Ändrade systeminställningar såsom automatisk anslutning till öppna hotspot-nätverk utan din vetskap eller ej tvingad kryptering på utgående säker kanaltrafik.

● Wi-Fi-nätverk och routrar

Klicka på namnet i listan för att läsa mer om det trådlösa nätverk och den router du är ansluten till. Om det rekommendera att du ställer in ett starkare lösenord för ditt hemmanätverk ska du se till att följa våra anvisningar, så att du kan fortsätta vara ansluten utan att oroa dig om din integritet.



När andra rekommendationer är tillgängliga följer du angivna instruktioner för att se till att hemnätverket förblir säkert för hackares nyfikna ögon.

16.2. Använda automatisk sårbarhetsövervakning

Bitdefender skannar regelbundet systemet efter sårbarheter, i bakgrunden, och håller reda på upptäckta problem i fönstret **Meddelanden**.

Kontrollera och åtgärda upptäckta problem:

1. Klicka på **Meddelanden** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. På fliken **Alla** väljer du meddelandet som avser den senaste sårbarhetsskanningen.
3. Du kan se detaljerad information avseende de upptäckta säkerhetsbristerna i systemet. Beroende på händelse, för att åtgärda ett specifikt säkerhetsproblem fortsätt enligt följande:
 - Om det finns tillgängliga Windows-uppdateringar klickar du på **Installera**.
 - Om automatisk Windows-uppdatering är inaktiverat klickar du på **Aktivera**.
 - Om en app är utdaterad klickar du på **Uppdatera nu** för att hitta en länk till leverantörens hemsida varifrån du kan installera den senaste versionen av appen.
 - Om ett Windows-användarkonto har ett svagt lösenord klickar du på **Byt lösenord** för att tvinga användaren att byta lösenord vid nästa inloggning eller så kan du ändra lösenordet själv. För ett starkt lösenord, använd en kombination av versaler och gemener, siffror och specialtecken (som till exempel #, \$ eller @).
 - Om Windows-funktionen Autorun är aktiverad klickar du **Åtgärda** för att inaktivera den.
 - Om den router du har konfigurerat har angett ett svagt lösenord klickar du på **Ändra lösenord** för att komma till dess gränssnitt varifrån du kan ange ett starkt.
 - Om det nätverk du är ansluten till har säkerhetsbrister som kan försätta systemet i risk klickar du på **Ändra Wi-Fi-lösenord**.

Konfigurera inställningar för säkerhetsbristövervakning:



1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I rutan **SÅRBARHET** klickar du på **Öppna**.



Viktigt

För att regelbundet meddelas om system- eller appsäkerhetsbrister ska du ha alternativet **Säkerhetsbrist** aktiverat.

3. Gå till fliken **Inställningar**.
4. Välj de systemsäkerhetsbrister du regelbundet vill ska kontrolleras genom att använda motsvarande omkopplare.

Windows updates

Kontrollera om operativsystemet Windows har de senaste kritiska säkerhetsuppdateringarna från Microsoft.

Programuppdateringar

Kontrollera om appar installerade på ditt system är uppdaterade. Utdaterade appar kan exploateras av skadlig programvara, vilket gör din PC sårbar för utomstående attacker.

Användarlösenord

Kontrollera om lösenorden för de Windows-konton och routrar som är konfigurerade på systemet är enkla att gissa eller inte. Att konfigurera lösenord som svåra att gissa (starka lösenord) gör det mycket svårt för hackare att bryta sig in i systemet. Ett starkt lösenord innehåller en kombination av versaler och gemener, siffror och specialtecken (som till exempel #, \$ eller @).

Spela automatiskt

Kontrollera statusen för Windows-funktionen Autorun. Den här funktionen gör att appar automatiskt startas från CD-skivor, DVD-skivor, USB-enheter eller andra externa enheter.

Vissa typer av hot använder Autorun för att spridas automatiskt från borttagbara medier till datorn. Därför rekommenderar vi att du inaktiverar den här Windows-funktionen.

Wi-Fi Security Advisor

Kontrollera om det trådlösa hemnätverk du är ansluten till är säkert eller inte, eller om det har säkerhetsbrister. Kontrollera också om lösenordet för din hemrouter är tillräckligt starkt och hur du kan göra det säkrare.



De flesta oskyddade nätverk är inte säkra och tillåter därmed att en hackare får tillgång till dina privata aktiviteter.



Notera

Om du stänger av övervakning av en specifik säkerhetsbrist kommer tillhörande problem inte längre att registreras i meddelandefönstret.

16.3. Wi-Fi Security Advisor

När du är på språng, arbetar på kafé eller väntar på flygplatsen, kan den snabbaste lösningen vara att ansluta till ett publikt trådlöst nätverk för att göra betalningar, kolla e-post eller sociala nätverkskonton. Men det kan finnas någon som försöker kapa dina personuppgifter där och som ser hur informationen läcker genom nätverket.

Personuppgifter innebär lösenord och användarnamn du använder för att få åtkomst till dina onlinekonton, som e-post, bankkonton, sociala mediekonton, men även de meddelanden du skickar.

Oftast är det mer troligt att publika trådlösa nätverk är osäkra, eftersom de inte kräver lösenord vid inloggning, och om de gör det, kan det lösenordet göras tillgängligt för alla som vill ansluta. Dessutom kan de vara skadliga nätverk, som utgör en måltavla för kriminella.

För att skydda dig mot farorna med osäkra eller okrypterade publika trådlösa surfzoner, analyserar Bitdefender Wi-Fi Security Advisor hur säkert ett trådlöst nätverk är, och om det behövs, rekommenderar dig att använda **Bitdefender VPN**.

Bitdefender Wi-Fi Security Advisor ger dig följande information om:

- Trådlösa hemnätverk
- Trådlösa kontorsnätverk
- Trådlösa publika nätverk

16.3.1. Aktivera eller inaktivera meddelanden från Wi-Fi Security Advisor

Aktivera eller inaktivera meddelanden från Wi-Fi Security Advisor:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.



2. I rutan **SÅRBARHET** klickar du på **Öppna**.
3. Gå till fönstret **Inställningar** och aktivera eller inaktivera alternativet **Säkerhetsrådgivare**.

16.3.2. Konfigurera trådlöst hemnätverk

För att börja konfigurera ditt hemnätverk:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I rutan **SÅRBARHET** klickar du på **Öppna**.
3. Gå till fönstret **Wi-Fi Security Advisor** och klicka på **Hemma Wi-Fi**.

4. På fliken **Hem-Wi-Fi** klickar du på knappen **VÄLJ HEM-WI-FI**.

En lista med de trådlösa nätverk du anslutit till hittills visas.

5. Peka på ditt hemnätverk och klicka därefter på **VÄLJ**.

Om ett hemnätverk anses vara osäkert, visas konfigurationsrekommendationer för att förbättra dess säkerhet.

Ta bort det trådlösa nätverk du har angett som hemnätverk genom att klicka på knappen **TA BORT**.

Lägg till ett nytt trådlöst nätverk som hemma genom att klicka på **Välj nytt hem-Wi-Fi**.

16.3.3. Konfigurera trådlöst kontorsnätverk

För att börja konfigurera ditt kontorsnätverk:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I rutan **SÅRBARHET** klickar du på **Öppna**.
3. Gå till fönstret **Wi-Fi Security Advisor** och klicka på **Jobb Wi-Fi**.
4. På fliken **Kontors-Wi-Fi** klickar du på knappen **VÄLJ KONTORS-WI-FI**.

En lista med de trådlösa nätverk du anslutit till hittills visas.

5. Peka på ditt kontorsnätverk och klicka därefter på **VÄLJ**.

Om ett kontorsnätverk anses vara osäkert, visas konfigurationsrekommendationer för att förbättra dess säkerhet.

Ta bort det trådlösa nätverk du har angett som kontorsnätverk genom att klicka på **TA BORT**.



Lägg till ett nytt trådlöst nätverk som kontor genom att klicka på **Välj nytt kontors-Wi-Fi**.

16.3.4. Offentlig Wi-Fi

Medan du är ansluten till ett osäkert trådlöst nätverk är profilen Publikt Wi-Fi aktiverad. När den körs i den här profilen är Bitdefender Antivirus Plus inställd på att automatiskt uppnå följande programinställningar:

- Advanced Threat Defense är aktiverat
- Följande inställningar från Förebyggande av onlinehot är aktiverade:
 - Krypterad webbskanning
 - Skydd mot bedrägeri
 - Skydd mot nätfiske
- En knapp som öppnar Bitdefender Safepay™ är tillgänglig. I det här fallet är hotspot-skydd för osäkra nätverk aktiverat som standard.

16.3.5. Kontrollera information om Wi-Fi-nätverk

Kontrollera information om de trådlösa nätverk du oftast ansluter till:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I rutan **SÅRBARHET** klickar du på **Öppna**.
3. Gå till fönstret **Wi-Fi Security Advisor**.
4. Beroende på vilken information du behöver väljer du en av de tre flikarna, **Hem-Wi-Fi**, **Kontors-Wi-Fi** eller **Publikt Wi-Fi**.
5. Klicka på **Visa information** bredvid det nätverk du vill hitta mer information om.

Det finns tre typer av trådlösa nätverk som filtreras efter deras betydelse, varje typ anges av en specifik ikon:

● **✘ Wi-Fi är osäkert** - anger att säkerhetsnivån för nätverket är låg. Det innebär att det är en stor risk att använda det och vi rekommenderar inte att göra betalningar eller kontrollera bankkonton utan extra skydd. I sådana situationer rekommenderar vi att du har Bitdefender Safepay™ med hotspotskydd för osäkra nätverk aktiverat.

● **Wi-Fi är osäkert** - anger att säkerhetsnivån för nätverket är måttlig. Det innebär att det kan finnas säkerhetsbrister och vi rekommenderar inte att



göra betalningar eller kontrollera bankkonton utan extra skydd. I sådana situationer rekommenderar vi att du har Bitdefender Safepay™ med hotspotskydd för osäkra nätverk aktiverat.

■ ■ ■ **Wi-Fi är säkert** - anger att det nätverk du använder är säkert. I det här fallet kan du använda känslig information för onlineåtgärder.

Genom att klicka på **Visa information** i området för varje nätverk, visas följande information:

- **Säkert** - här kan du se om det valda nätverket är säkert eller inte. Okrypterade nätverk kan exponera den information du använder.
- **Krypteringstyp** - här kan du visa den krypteringstyp som används av valt nätverk. Vissa krypteringstyper kanske inte är säkra. Därför rekommenderar vi att du kontrollerar informationen om den visade krypteringstypen för att vara säker på att du är skyddad när du surfar på nätet.
- **Kanal/Frekvens** - här kan du visa den kanalfrekvens som används av det valda nätverket.
- **Lösenordsstyrka** - här kan du visa hur starkt lösenordet är. Observera att de nätverk som har svaga lösenord utgör en måltavla för cyberbrottslingar.
- **Typ av inloggning** - här kan du visa om valt nätverk är skyddat av ett lösenord eller inte. Vi rekommenderar att du endast ansluter till nätverk som har konfigurerat starka lösenord.
- **Autentiseringstyp** - här kan du visa den autentiseringstyp som används av valt nätverk.



17. AVHJÄLPNING AV RANSOMWARE

Bitdefender Ransomware Remediation säkerhetskopierar filer som dokument, bilder, videor eller musik för att se till att de skyddas från att skadas eller förloras i händelse av ransomwarekryptering. Varje gång en ransomwareattack upptäcks blockerar Bitdefender alla processer som är inblandade i attacken och startar avhjälpningsprocessen. På så sätt kan du återställa innehållet för alla dina filer utan att betala den begärda lösensumman.

17.1. Aktivera eller inaktivera ransomwareavhjälpning

Aktivera eller inaktivera ransomwareavhjälpning:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **AVHJÄLPNING AV RANSOMWARE** aktiverar eller inaktiverar du omkopplaren.



Notera

För att säkerställa att dina filer är skyddade mot ransomware rekommenderar vi att du har Avhjälpning av ransomware aktiverat.

17.2. Aktivera eller inaktivera automatisk återställning

Med Automatisk återställning kan du se till att dina filer återställs automatiskt i händelse av ransomwarekryptering.

Aktivera eller inaktivera automatisk återställning:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **AVHJÄLPNING AV RANSOMWARE** klickar du på **Hantera**.
3. I fönstret **Inställningar** aktiverar du eller inaktiverar reglaget **Automatisk återställning**.

17.3. Visa filer som har återställts automatiskt

När alternativet **Automatisk återställning** är aktiverat återställer Bitdefender automatiskt filer som krypterats av ransomware. På så sätt kan du ha en bekymmersfri upplevelse och veta att dina filer är säkra.

Visa filer som har återställts automatiskt:



1. Klicka på **Meddelanden** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. På fliken **Alla** markerar du meddelandet avseende det senast upptäckta ransomwarebeteendet som avhjälpts och klickar sedan på **Återställda filer**.

Listan med återställda filer visas. Här kan du även visa platsen dit dina filer har återställts.

17.4. Återställa krypterade filer manuellt

Ifall du manuellt måste återställa filer som krypterats av ransomware följer du de här stegen:

1. Klicka på **Meddelanden** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. På fliken **Alla** markerar du information avseende det senast upptäckta ransomwarebeteendet som upptäckts och klickar sedan på **Krypterade filer**.

3. Listan med krypterade filer visas.

Klicka på **Återställ filer** för att fortsätta.

4. Ifall hela eller en del av återställningsprocessen misslyckas måste du välja den plats där de avkrypterade filerna ska sparas. Klicka på **Återställ plats** och välj sedan en plats på din dator.

5. Ett bekräftelsefönster visas.

Klicka på **Slutför** för att avsluta återställningsprocessen.

Filer med följande tillägg kan återställas ifall de blir krypterade:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb; .doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html; .ico; .jar; .java; .jpeg; .jpg; .js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp; .odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

17.5. Lägga till program till undantag

Du kan konfigurera undantagsregler för betrodda appar så att funktion Avhjälpning av ransomware inte blockerar dem om de utför ransomwareliknande åtgärder.



Lägga till appar till undantagslistan för avhjälpning av ransomware:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **AVHJÄLPNING AV RANSOMWARE** klickar du på **Hantera**.
3. Gå till fönstret **Undantag** och klicka på **+Lägg till undantag**.



18. LÖSENORDSHANTERINGSSKYDD FÖR DINA INLOGGNINGSUPPGIFTER

Vi använder våra enheter för att shoppa online eller betala räkningar, för att ansluta till sociala media-plattformar eller logga in med snabbmeddelandeappar.

Men som alla vet är det inte alltid så lätt att komma ihåg lösenordet!

Och om vi inte är försiktiga när vi surfar online kan vår privata information, som e-postadress, snabbmeddelande-ID eller kreditkortsinformation komprometteras.

Att ha sina lösenord eller personuppgifter på ett papper eller i datorn kan vara farligt, eftersom de kan hittas och användas av andra personer som vill stjäla och använda den informationen. Och det är inte så lätt att komma ihåg alla lösenord du ställt in för dina onlinekonton eller för dina favoritwebbsidor.

Finns det därför något sätt för att vi ska vara säkra på att vi hittar våra lösenord när vi behöver dem? Och kan vi lita på att våra hemliga lösenord alltid är säkra?

lösenordshanterare hjälper dig att hålla reda på dina lösenord, skyddar din integritet och ger en säker surfupplevelse.

Genom att använda ett enda huvudlösenord för att komma åt dina inloggningsuppgifter gör Password Manager det enkelt för dig att ha dina lösenord säkra i en plånbok.

Password Manager är integrerat med Bitdefender Safepay™ för att erbjuda det bästa skyddet för dina onlineaktiviteter och ger en enhetlig lösning för de olika sätt på vilka din privata information kan komprometteras.

Password Manager skyddar följande privata information:

- Personlig information, som e-postadress eller telefonnummer
- Inloggningsuppgifter för webbplatserna
- Bankkontoinformation eller kreditkortsnummer
- Komma åt data till e-postkonton
- Lösenord till apparna
- Lösenord för Wi-Fi-nätverken



18.1. Skapa en ny plånboksdatabas

Bitdefender Wallet är platsen där du kan lagra din personliga information. För en enklare surfupplevelse måste du skapa en plånboksdatabas så här:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. I fönstret **Mina plånböcker** klickar du på **Lägg till plånbok**.
4. Klicka på **Skapa ny**.
5. Skriv in den önskade informationen i de motsvarande fälten.
 - Plånboksnamn - skriv ett unikt namn för din plånboksdatabas.
 - Huvudlösenord - skriv ett lösenord för din plånbok.
 - Ledtråd - skriv en ledtråd för att komma ihåg lösenordet.
6. Klicka på **Fortsätt**.
7. I det här steget kan du välja att spara dina uppgifter i molnet genom att aktivera reglaget bredvid **Synkronisera på alla mina enheter**. Välj önskat alternativ och klicka på **Fortsätt**.
8. Välj den webbläsare du vill importera inloggningsuppgifter från.
9. Klicka **Slutför**.

18.2. Importera en befintlig databas

Importera en plånbok lagrad lokalt:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. I fönstret **Mina plånböcker** klickar du på **Lägg till plånbok**.
4. Klicka på **Importera en befintlig databas**.
5. Gå till den plats på enheten där du sparade plånboksdatabasen och välj den.
6. Klicka **Öppna**.
7. Ge ett namn åt din plånbok och skriv in det lösenord du tilldelade när den skapades första gången.
8. Klicka på **Importera**.



9. Välj de program du vill att plånboken ska importera inloggningsuppgifter från och sedan knappen **Slutför**.

18.3. Exportera plånboksdatan

Exportera plånboksdatan:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. Öppna fönstret **Mina plånböcker**.
4. Klicka på **☰**-ikonen i önskad plånbok och välj sedan **Exportera**.
5. Gå till den plats på enheten där du vill spara plånboksdatan och välj sedan ett namn för den.
6. Klicka **Spara**.



Notera

Plånböckerna måste vara öppna för att **Exportera**-funktionen ska vara tillgänglig.

Om den plånbok du behöver exportera är låst klickar du på **Aktivera plånbok** och skriver därefter i det lösenord som tilldelades när den skapades första gången.

18.4. Synkronisera plånböckerna i molnet

Aktivera eller inaktivera plånbokssynkronisering i molnet:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. Öppna fönstret **Mina plånböcker**.
4. Klicka på **☰**-ikonen i önskad plånbok och välj sedan **Inställningar**.
5. Välj det önskade alternativet i det fönster som visas och klicka sedan på **Spara**.



Notera

Plånböckerna måste vara öppna för att **Exportera**-funktionen ska vara tillgänglig.



Om den plånbok du behöver synkronisera är låst klickar du på **AKTIVERA PLÅNBOK** och skriver därefter i det lösenord som tilldelades när den skapades första gången.

18.5. Hantera dina plånboksinloggningsuppgifter


Hantera dina lösenord:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. Öppna fönstret **Mina plånböcker**.
4. Välj den önskade plånboksdatabasen och klicka sedan på **Aktivera plånbok**.
5. Skriv huvudlösenordet och klicka sedan på **OK**.

Ett nytt fönster visas. Välj önskad kategori från den övre delen i fönstret:

- Identitet
- Webbssidor
- Internetbank
- E-postmeddelanden
- Program
- Wi-Fi-nätverk

Lägga till/redigera inloggningsuppgifter

- Lägg till ett nytt lösenord genom att välja önskad kategori överst, klicka på **+ Lägg till objekt**, infoga informationen i motsvarande fält och klicka på **Spara**.
- För att redigera en post i tabellen, välj den och klicka på knappen **Redigera** på höger sida.
- Ta bort en post genom att markera den och klicka på  **Ta bort**.

18.6. Aktivera eller inaktivera Password Manager-skyddet

Aktivera eller inaktivera Password Manager-skyddet:



1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **PASSWORD MANAGER** aktiverar eller inaktiverar du omkopplaren.

18.7. Hantera inställningarna för Password Manager

Konfigurera huvudlösenordet i detalj:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. Gå till fönstret **Inställningar**.

I avsnittet **Säkerhetsinställningar** finns följande alternativ tillgängliga:

- **Fråga om mitt huvudlösenord när jag loggar in till min enhet** - du ombes att infoga ditt huvudlösenord när du öppnar enheten.
- **Fråga om mitt huvudlösenord när jag öppnar mina webbläsare och appar** - du ombes att infoga ditt huvudlösenord när du öppnar en webbläsare eller en app.
- **Fråga inte efter mitt huvudlösenord** - du kommer inte att tillfrågas om ditt huvudlösenord när du öppnar enheten, en webbläsare eller en app.
- **Lås automatiskt plånbok när jag lämnar min enhet utan uppsikt** - du uppmanas att infoga ditt huvudlösenord när du återgår till enheten efter 15 minuter.



Viktigt

Kom ihåg ditt huvudlösenord eller förvara det på en säker plats. Om du glömmet bort lösenordet måste du ominstallera programmet eller kontakta Bitdefender för support.

Förbättra din upplevelse

Välj de appar eller appar där du vill integrera Password Manager:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. Välj fönstret **Inställningar**.

Aktivera reglaget bredvid en app för att använda Lösenordshanteraren och förbättra din upplevelse:



- Internet Explorer
- Mozilla Firefox
- Google Chrome
- Säker betalning

Konfigurera Automatisk ifyllnad

Funktionen Automatisk ifyllnad gör det enkelt att ansluta till dina favoritwebbsidor eller logga in med dina onlinekonton. Första gången du anger dina inloggningsuppgifter och personliga information i webbläsaren är de automatiskt säkrade i plånboken.

Konfigurera inställningarna för **Automatisk ifyllnad**:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **PASSWORD MANAGER** klickar du på **Inställningar**.
3. I fönstret **Inställningar** bläddrar du till fliken **Autofyll-inställningar**.
4. Konfigurera följande alternativ:


- **Konfigurera hur plånboken håller dina inloggningsuppgifter säkra:**
 - **Spara inloggningsuppgifter automatiskt i plånboken** - inloggningsuppgifter och annan identifierbar information som person- och kreditkortsuppgifter sparas automatiskt och uppdateras i plånboken.
 - **Fråga mig varje gång** - du tillfrågas varje gång du om du vill lägga till dina uppgifter i plånboken.
 - **Spara inte, jag uppdaterar informationen manuellt** - inloggningsuppgifterna kan endast läggas till manuellt i plånboken.
- **Fyll i inloggningsuppgifter automatiskt:**
 - **Fyll i inloggningsuppgifter automatiskt varje gång** - inloggningsuppgifterna infogas automatiskt i webbläsaren.
- **Fyll i formulär automatiskt:**
 - **Fråga efter mina ifyllningsalternativ när jag besöker en sida med formulär** - en poppruta med ifyllningsalternativen visas varje gång Bitdefender upptäcker att du vill utföra en onlinebetalning eller registrera dig.



Hantera Password Manager-information från webbläsaren

Du kan enkelt hantera Password Manager-information direkt från webbläsaren för att ha all viktig information till hands. Tillägget Bitdefender-plånbok stöds av följande webbläsare: Google Chrome, Internet Explorer och Mozilla Firefox, och är även integrerat med Safepay.

För att komma till Bitdefender-plånboken öppnar du webbläsaren, tillåter att

tillägget installeras och klickar på -ikonen i verktygsfältet.

Tillägget Bitdefender-plånbok innehåller följande alternativ:

- Öppna plånbok - öppnar plånboken.
- Lås plånbok - låser plånboken.
- Webbssidor - öppnar en undermeny med alla webbplatsinloggningar sparade i plånboken. Klicka på **Lägg till webbsida** för att lägga till nya webbplatser i listan.
- Fyll i formulär - öppnar en undermeny som innehåller den information du lagt till för en särskild kategori. Härifrån kan du lägga till nya uppgifter i plånboken.
- Lösenordsgenerator - gör att du kan generera slumpmässiga lösenord du kan använda för befintliga konton. Klicka på **Visa avancerade inställningar** för att anpassa komplexiteten för lösenordet.
- Inställningar - öppnar inställningsfönstret för lösenordshanteraren.
- Rapportera problem - rapportera alla problem du stöter på med Bitdefenders lösenordshanterare.



19. ANTI-TRACKER

Många webbplatser du besöker använder spårningsverktyg för att samla in information om ditt beteende, antingen för att dela den med tredjepartsföretag eller för att visa annonser som är mer relevanta för dig. På så sätt tjänar webbplatsägare pengar för att kunna ge dig innehåll utan kostnad eller fortsätta vara verksamma. Förutom att samla in information kan spårningsverktyg göra din surfupplevelse långsammare eller slösa på bandbredd.

Med tillägget Bitdefender Anti-tracker aktiverat i webbläsaren undviker du att bli spårad så att dina data fortsätter att vara privata medan du surfar online och du ökar hastigheten som webbplatserna behöver för att läsas in.


Bitdefender-tillägget är kompatibelt med följande webbläsare:

- Internet Explorer
- Google Chrome
- Mozilla Firefox

De spårningsverktyg vi hittar grupperas i följande kategorier:

- **Reklam** - används för att analysera webbsidestrafik, användarbeteende eller besökares trafikmönster.
- **Kundinteraktion** - används för att mäta användarinteraktion med olika inmatningsformulär som chatt eller support.
- **Viktigt** - används för att övervaka viktiga webbsidesfunktioner.
- **Sidanalys** - används för att samla in data avseende webbsidesanvändning.
- **Sociala medier** - används för att övervaka social målgrupp, aktivitet och användarengagemang med olika sociala medieplattformar.

19.1. Anti-tracker-gränssnitt

När tillägget Bitdefender Anti-tracker är aktiverat visas ikonen  bredvid sökfältet i webbläsaren. Varje gång du besöker en webbplats ses en räknare på ikonen, som hänvisar till upptäckta och blockerade spårningsverktyg. För att visa mer information om de blockerade spårningsverktygen klickar du på ikonen för att öppna gränssnittet. Förutom antalet blockerade spårningsverktyg kan du visa den tid som krävs för att sidan ska ladda och



kategorierna till vilka de upptäckta spårningsverktygen hör. Klicka på önskad kategori för att visa listan över webbplatser som spårar.



Inaktivera Bitdefender från att blockera spårningsverktyg på den webbplats du besöker genom att klicka på **Pausa skydd på den här webbplatsen**. Den här inställningen gäller endast så länge som du har webbplatsen öppen och återgår till den initiala tillståndet när du stänger webbplatsen.

För att tillåta spårningsverktyg från en specifik kategori att övervaka din aktivitet klickar du på önskad aktivitet och sedan på motsvarande knapp. Om du ändrar dig klickar du på samma knapp en gång till.

19.2. Inaktivera Bitdefender Anti-tracker

Inaktivera Bitdefender Anti-tracker:

● Från din webbläsare:

1. Öppna webbläsaren.
2. Klicka på ikonen  bredvid adressfältet i webbläsaren.
3. Klicka på ikonen  i det övre högra hörnet.
4. Använd motsvarande omkopplare för att aktivera eller inaktivera. Bitdefender-ikonen blir grå.

● Från Bitdefenders gränssnitt:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I **ANTI-TRACKER**-panelen klickar du på **Inställningar**.
3. Bredvid webbläsaren för vilken du vill inaktivera tillägget slår du av motsvarande omkopplare.


19.3. Tillåta att en webbplats spåras

Om du vill bli spårad medan du besöker en viss webbplats kan du lägga till dess adress till undantagen så här:

1. Öppna webbläsaren.
2. Klicka på ikonen  bredvid sökfältet.
3. Klicka på ikonen  i det övre högra hörnet.



4. Om du är på den webbplats du vill lägga till bland undantagen klickar du på **Lägg till aktuell webbplats i listan**.

Om du vill lägga till en annan webbplats skriver du in adressen i motsvarande fält och klickar på .



20. VPN

VPN-appen kan installeras från din Bitdefender-produkt och användas varje gång du vill lägga till en extra skyddslag till din anslutning. VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter till för att säkra din anslutning, kryptera data med kryptering i bankklass och dölja din IP-adress oavsett var du är. Din trafik omdirigeras via en separat server och gör det därmed näst intill omöjligt att identifiera din enhet bland de myriader av andra enheter som använder våra tjänster. När du är ansluten till Internet via Bitdefender VPN, kan du dessutom ha åtkomst till innehåll som i normala fall är begränsat i vissa områden.



Notera

Vissa länder censurerar Internet och därför kan användning av VPN på deras territorier vara förbjudet enligt lag. För att undvika juridiska konsekvenser kan ett varningsmeddelande visas när du försöker använda Bitdefender VPN-appen första gången. Genom att fortsätta använda funktionen bekräftar du att du är medveten om regelverken i det land du befinner dig i och de risker du kan utsättas för.

20.1. Öppna VPN

För att komma åt huvudgränssnittet för Bitdefender VPN använder du en av följande metoder:

● Från systemfältet

1. Högerklicka på -ikonen i systemfältet och klicka sedan på **Visa**.

● Från Bitdefenders gränssnitt:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I **VPN**-panelen klickar du på **Öppna VPN**.


20.2. VPN-gränssnitt

VPN-gränssnittet visar status för appen, ansluten eller frånkopplad. Serverplatsen för användare med den fria versionen ställs automatiskt av Bitdefender till den lämpligaste servern, medan premium användare har möjlighet att ändra serverplatsen de vill ansluta till. Mer information om VPN-prenumerationer finns i "*Prenumerationer*" (p. 117).



Klicka bara på den status som visas längst upp på skärmen för att ansluta eller koppla ifrån, eller högerklicka på systemfältsikonen. Systemfält ikonen visar ett grönt kontrollmärke när VPN är ansluten och en röd markering när VPN är fränkopplad.

När du är ansluten visas den förflutna tiden och bandbreddsanvändningen under den nedre delen av gränssnittet.

För att visa området **Meny** helt klickar du på ikonen  i den övre vänstra sidan. Här har du följande alternativ:

- **Mitt Konto** - information om ditt Bitdefender-konto och VPN-prenumeration visas. Klicka på **Växla konto** om du vill logga in med ett annat konto.

Klicka på **Lägg till den här** för att lägga till en aktiveringskod för Bitdefender Premium VPN.

- **Inställningar** – beroende på dina behov kan du anpassa produktens beteende. Inställningarna är grupperade i två kategorier:

- **Allmänt**

- Aviseringar
- Upstart - välj huruvida Bitdefender VPN ska köras vid upstart eller inte
- Produktrapporter - skicka anonyma produktrapporter för att hjälpa oss att förbättra din upplevelse
- Mörkt läge
- Språk

- **Avancerat**

- Internet Kill-Switch - den här funktionen stoppar tillfälligt all internettrafik om VPN-anslutningen plötsligt förloras. Så fort du är tillbaka online återuprättas VPN-anslutningen.
- Autoconnect - Anslut Bitdefender VPN automatiskt när du ansluter till offentliga/osäkra Wi-Fi-nätverk eller när en peer-to-peer-fildelnings-app startas

- **Support** - du kan öppna vår supportcenterplattform varifrån du kan läsa en användbar artikel om hur du använder Bitdefender VPN eller skicka feedback till oss.

- **Om** - information om den installerade versionen visas.



20.3. Prenumerationer

Bitdefender VPN erbjuder utan kostnad 200 MB trafiksaldo per enhet för att säkra din anslutning varje gång du behöver det och ansluter dig automatiskt till den optimala serverplatsen.

För att få obegränsad trafik och obegränsad åtkomst till innehåll världen över genom att välja en server när du vill, ska du uppgradera till premiumversionen.

Du kan uppgradera till Bitdefender Premium VPN-versionen när som helst genom att klicka på knappen **Uppgradera** som finns i produktgränssnittet.

Bitdefender Premium VPN-prenumerationen är oberoende av Bitdefender Antivirus Plus-prenumerationen, vilket betyder att du kommer att kunna använda den under hela tillgänglighetsperioden, oavsett säkerhetslösningens prenumetationsstatus. Om Bitdefender Premium VPN-prenumerationen går ut, men den för Bitdefender Antivirus Plus fortfarande är aktiv återgår du till gratisversionen.

Bitdefender VPN är en produkt över flera plattformar, tillgänglig i Bitdefender-produkter kompatibla med Windows, macOS, Android och iOS. När du uppgraderar till premiumplanen kan du använda din prenumeration på alla produkter, förutsatt att du loggar in med samma Bitdefender-konto.



21. SAFEPAY-SÄKERHET FÖR ONLINETRANSLATIONER

Datorn blir snabbt huvudverktyg för att shoppa och utföra bankärenden. Betala räkningar, överföra pengar, köpa i princip allt du kan föreställa dig har aldrig varit snabbare eller enklare.

Det innebär att skicka personlig information, konto- och kreditkortsuppgifter, lösenord och andra typer av privat information över Internet, med andra ord exakt den typ av informationsflöde som cyberbrottslingar är mycket intresserade av att komma över. Hackare är outtröttliga i sina ansträngningar att stjäla den här informationen, så du kan aldrig vara nog försiktig när det gäller säkra onlinetransaktioner.

Bitdefender Safepay™ är först och främst en skydda webbläsare, en förseglad miljö som är utvecklad för att hålla dina bankärende, e-handel och andra typer av onlinetransaktioner privata och säkra.

För bästa integritetsskydd har Bitdefender Password Manager integrerats i Bitdefender Safepay™ för att säkra dina inloggningsuppgifter varje gång du vill öppna privata onlineplatser. Mer information finns på "[Lösenordshanteringsskydd för dina inloggningsuppgifter](#)" (p. 105).

Bitdefender Safepay™ erbjuder följande funktioner:

- Det blockerar åtkomst till ditt skrivbord och alla försök att ta bilder av din skärm.
- Det skyddar dina hemliga lösenord när du surfar online med Password Manager.
- Den har ett virtuellt tangentbord som när det används, gör det omöjligt för hackare att avläsa tangenttryckningar.
- Den är helt oberoende av dina andra webbläsare.
- Den har inbyggt hotspotskydd som ska användas när enheten är ansluten till osäkra Wi-Fi-nätverk.
- Den har stöd för bokmärken och tillåter att du navigerar mellan dina favoritwebbplatser för bankärenden/shopping.
- Den är inte begränsad till bankärenden och e-handel. Alla webbplatser kan öppnas i Bitdefender Safepay™.



21.1. Använda Bitdefender Safepay™

Som standard upptäcker Bitdefender när du navigerar till en bankwebbplats online eller onlinebutik i en webbläsare på enheten och uppmanar dig att starta den i Bitdefender Safepay™.

För att komma åt huvudgränssnittet för Bitdefender Safepay™ använder du en av följande metoder:

- Från **Bitdefender-gränssnittet**:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I **SAFEPAY**-panelen klickar du på **Inställningar**.
3. I fönstret **Säker betalning** klickar du på **Öppna Säker betalning**.

- Från Windows:

- I **Windows 7**:

1. Klicka på **Start** och gå till **Alla program**.
2. Klicka på **Bitdefender**.
3. Klicka på **Bitdefender Safepay™**.

- I **Windows 8 och Windows 8.1**:

Leta upp Bitdefender Safepay™ från Windows Start-skärm (du kan till exempel börja skriva "Bitdefender Safepay™" direkt på Start-skärmen) och därefter klicka på ikonen.




- I **Windows 10**:

Skriv "Bitdefender Safepay™" i sökrutan från aktivitetsfältet och klicka sedan på dess ikon.







Om du är van vid webbläsare har du inga problem med att använda Bitdefender Safepay™ - den ser ut och fungerar som en vanlig webbläsare:

- ange de webbadresser du vill gå till i adressfältet.
- lägg till flikar för att besöka flera webbplatser i Bitdefender

Safepay™-fönstret genom att klicka på .

- navigera tillbaka och framåt och uppdatera sidor med respektive   




- öppna Bitdefender Safepay™-**inställningar** genom att klicka på  och välja **Inställningar**.
- skydda dina lösenord med **Password Manager** genom att klicka på .
- hantera dina **bokmärken** genom att klicka på  bredvid adressfältet.
- öppna det virtuella tangentbordet genom att klicka på .
- öka eller minska webbläsarens storlek genom att trycka samtidigt på **Ctrl**- och **+/-**-tangenter på den numeriska knappsatsen.
- visa information om din Bitdefender-produkt genom att klicka på  och välja **Om**.
- skriv ut viktig information genom att klicka på  och välja **Skriv ut**.



Notera

För att växla mellan Bitdefender Safepay™ och Windows-skrivbordet trycker du på **Alt+Tab**-tangenter eller klickar på alternativet **Växla till skrivbord** på den övre vänstra sidan av fönstret.

21.2. Konfigurera inställningar

Klicka på  och välj **Inställningar** för att konfigurera Bitdefender Safepay™:

Använd Bitdefender Safepay-regler för öppnade domäner

De webbplatser du lagt till i **Bokmärken** med alternativet **Öppna automatiskt i Safepay** aktiverat visas här. Om du vill sluta att automatiskt öppna en webbplats från listan med Bitdefender Safepay™, klickar du på **x** bredvid önskad post från kolumnen **Ta bort**.

Blockera popup-rutor

Du kan välja att blockera popup-rutor genom att klicka på motsvarande omkopplare.

Du kan också skapa en lista över webbplatser att tillåta popup-rutor från. Listan bör endast innehålla webbsidor du litar fullständigt på.



Lägg till en webbplats till listan, ange dess adress i motsvarande fält och klicka på **Lägg till domän**.

Ta bort en webbplats från listan genom att välja X för önskad post.

Manage Plugins

Du kan välja om du vill aktivera eller inaktivera specifika insticksprogram i Bitdefender Safepay™.

Hantera certifikat

Du kan importera certifikat från systemet till ett certifikatlager.

Klicka på **IMPORTERA** och följ guiden för att använda certifikaten i Bitdefender Safepay™.

Använd virtuellt tangentbord

Det virtuella tangentbordet visas automatiskt när ett lösenordsfält väljs.

Använd motsvarande omkopplare för att aktivera eller inaktivera funktionen.

Skriver ut bekräftelse

Aktivera det här alternativet om du vill bekräfta innan utskriftsprocessen startar.

21.3. Hantera bokmärken

Om du har inaktiverat den automatiska upptäckten av vissa eller alla webbplatser eller om Bitdefender helt enkelt inte hittar vissa webbplatser kan du lägga till bokmärken till Bitdefender Safepay™ så att du enkelt kan gå till favoritwebbplatser i framtiden.

Följ de här stegen för att lägga till en webbadress till Bitdefender Safepay™-bokmärken:

1. Klicka på  och välj **Bokmärken** för att öppna sidan Bokmärken.



Notera

Sidan Bokmärken öppnas som standard när du startar Bitdefender Safepay™.

2. Klicka på **+**-knappen för att lägga till ett nytt bokmärke.
3. Skriv in webbadressen och titel på bokmärket och klicka på **SKAPA**. Markera alternativet **Öppna automatiskt i Safepay** om du vill att den



bokmärkta sidan ska öppnas med Bitdefender Safepay™ varje gång du öppnar den. Webbadressen läggs också till i domänlistan på sidan **Inställningar**.

21.4. Inaktivera Safepay-meddelanden

När en bankwebbplats hittas är Bitdefender-produkten inställd på att meddela dig via en popup-ruta.

Inaktivera Safepay-meddelandena:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I **SAFEPAY**-panelen klickar du på **Inställningar**.
3. I fönstret **Inställningar** stänger du av reglaget bredvid **Notiser för säkra betalningar**.

21.5. Använda VPN med Safepay

För att göra onlinebetalningar i en säker miljö när du är ansluten till osäkra nätverk kan Bitdefender-produkten ställas in för att automatiskt starta VPN-appen samtidigt med Safepay.

Börja använda VPN-appen tillsammans med Safepay:

1. Klicka på **Sekretess** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I **SAFEPAY**-panelen klickar du på **Inställningar**.
3. I fönstret **Inställningar** aktiverar du reglaget bredvid **Använd VPN med Säkra betalningar**.



22. USB IMMUNIZER

Den inbyggda funktionen Autorun i Windows-operativsystem är ett mycket användbart verktyg som gör att enheter automatiskt kör en fil från de medier som är anslutna till den. Till exempel kan programvaruinstallationer startas automatiskt när en CD sätts in i den optiska enheten.

Tyvärr kan den här funktionen även användas av hot för att automatiskt starta och infiltrera din enhet från skrivbara medier, som USB-flashenheter och minneskort anslutna via kortläsare. Flera Autorun-baserade attacker har skapats de senaste åren.

Med USB Immunizer kan du förhindra att NTFS-, FAT32- eller FAT-formaterade flashenheter från att automatiskt exekvera hot. När en USB-enhet är immuniserad kan inte hot längre konfigurera den för att köra vissa appar när enheten är ansluten till en enhet som kör Windows.

Immunisera en USB-enhet:

1. Anslut flashenheten till enheten.
2. Sök på enheten för att hitta den borttagbara lagringenheten och högerklicka på dess ikon.
3. I kontextmenyn pekar du på **Bitdefender** och väljer **Immunisera den här enheten**.



Notera

Om enheten redan är immuniserad visas meddelandet **USB-enheten är skyddad mot autorun-baserade hot** istället för alternativet Immunisera.

För att förhindra enheten från att köra hot från ej immuniserade USB-enheter inaktiverar du funktionen för autokörning av medier. Mer information finns på "*Använda automatisk sårbarhetsövervakning*" (p. 96).



VERKTYG



23. PROFILER

Dagliga jobbaktiviteter, titta på film eller spela spel kan orsaka att systemet blir långsammare, särskilt om de körs samtidigt med Windows-uppdateringsprocesser och underhållsåtgärder. Med Bitdefender kan du nu välja och tillämpa din föredragna profil, vilket gör att systemjusteringar anpassas för att öka prestandan för specifika installerade appar.

Bitdefender tillhandahåller följande profiler:

- Arbetsprofil
- Filmprofil
- Spelprofil
- Publik Wi-Fi-profil
- Batterilägesprofil

Om du bestämmer dig för att inte använda **Profiler**, aktiveras en standardprofil som heter **Standard** och den skapar ingen optimering för ditt system.

Enligt din aktivitet tillämpas följande produktinställningar när profilerna Arbete, Film eller Spel aktiveras:

- Alla Bitdefendervarningar och popups är inaktiverade.
- Automatisk uppdatering skjuts upp.
- Schemalagda skanningar skjuts upp.
- Sakhjälp inaktiveras.
- Meddelanden om specialerbjudanden inaktiveras.

Enligt din aktivitet tillämpas följande systeminställningar när profilerna Arbete, Film eller Spel aktiveras:

- Automatiska uppdateringar för Windows skjuts upp.
- Windows-varningar och popups är inaktiverade.
- Onödiga bakgrundsprogram stängs av.
- Visuella effekter justeras för bästa prestanda.
- Underhållsåtgärder skjuts upp.



- Energiplansinställningar justeras.

När den körs i profilen publik Wi-Fi är Bitdefender Antivirus Plus inställd på att automatiskt uppnå följande programinställningar:

- Advanced Threat Defense är aktiverat
- Följande inställningar från Förebyggande av onlinehot är aktiverade:
 - Krypterad webbskanning
 - Skydd mot bedrägeri
 - Skydd mot nätfiske

23.1. Arbetsprofil

Att köra flera uppgifter på jobbet, som att skicka e-post, ha en videokommunikation med avlägsna kollegor eller arbeta med att designa appar kan påverka systemprestanda. Arbetsprofilen har designats för att hjälpa dig förbättra din arbetseffektivitet, genom att stänga av vissa av dina bakgrundstjänster och underhållsuppgifter.

Konfigurera Arbetsprofil

Konfigurera de åtgärder som ska vidtas när Arbetsprofil används:

1. Klicka på **Verktyg** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fliken **Profiler** klickar du på **Inställningar**.
3. Klicka på knappen **KONFIGURERA** från området Arbetsprofil.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
 - Ökar prestanda på arbetsappar
 - Optimera produktinställningar för arbetsprofil
 - Skjut upp bakgrundsprogram och underhållsuppgifter
 - Skjut upp Windows automatiska uppdateringar
5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.



Lägga till appar manuellt till arbetsprofilen

Om Bitdefender inte automatiskt laddar Jobbprofil när du startar en viss jobbapp, kan du manuellt lägga till appen till **listan Jobbappar**.

Lägga till appar i listan Jobbprogram i Jobbprofil manuellt:

1. Klicka på **Verktyg** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fliken **Profiler** klickar du på **Inställningar**.
3. Klicka på knappen **KONFIGURERA** från området Arbetsprofil.
4. I fönstret **Inställningar av jobbprofil** klickar du på **Programlista**.
5. Klicka på **LÄGG TILL**.

Ett nytt fönster visas. Bläddra till appens exekveringsfil, välj den och klicka på **OK** för att lägga till den till listan.

23.2. Filmprofil

Att visa högkvalitativt videoinnehåll, som HD-filmer, kräver mycket systemresurser. Filmprofil justerar system- och produktinställningar så att du kan njuta av en oavbruten och smidig filmupplevelse.

Konfigurera filmprofil

Konfigurera de åtgärder som ska vidtas när filmprofil används:

1. Klicka på **Verktyg** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fliken **Profiler** klickar du på **Inställningar**.
3. Klicka på knappen **KONFIGURERA** från området filmprofil.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
 - Öka prestanda på videospelare
 - Optimera produktinställningar för filmprofil
 - Skjut upp bakgrundsprogram och underhållsuppgifter
 - Skjut upp Windows automatiska uppdateringar
 - Justera energiplansinställningar för filmer
5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.



Lägga till videospelare till listan Filmprofil manuellt

Om Bitdefender inte automatiskt laddar Filmprofil när du startar en viss videospelare, kan du manuellt lägga till appen till **listan Filmappar**.

Lägga till videospelare till listan Filmappar i Filmprofil manuellt:

1. Klicka på **Verktyg** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fliken **Profiler** klickar du på **Inställningar**.
3. Klicka på knappen **KONFIGURERA** från området filmprofil.
4. I fönstret **Inställningar av filmprofil** klickar du på **Spelarlista**.
5. Klicka på **LÄGG TILL**.

Ett nytt fönster visas. Bläddra till appens exekveringsfil, välj den och klicka på **OK** för att lägga till den till listan.

23.3. Spelprofil

Att njuta av en oavbruten spelupplevelse handlar om att minska spelbelastningen och minska nedgångar. Genom att använda beteendemässig heuristik tillsammans med en lista med kända spel kan Bitdefender automatiskt upptäcka spel som körs och optimera dina systemresurser så att du kan njuta av din spelstund.

Konfigurera spelprofil

Konfigurera de åtgärder som ska vidtas när spelprofil används:

1. Klicka på **Verktyg** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fliken **Profiler** klickar du på **Inställningar**.
3. Klicka på knappen **Konfigurera** från området Spelprofil.
4. Välj de systemjusteringar du vill ska tillämpas genom att markera följande alternativ:
 - Öka prestanda på spel
 - Optimera produktinställningar för spelprofil
 - Skjut upp bakgrundsprogram och underhållsuppgifter
 - Skjut upp Windows automatiska uppdateringar
 - Justera energiplansinställningar för spel



5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Lägga till spel manuellt till spellistan

Om Bitdefender inte automatiskt laddar Spelprofil när du startar ett visst spel eller app, kan du manuellt lägga till appen till **listan Spelappar**.

Lägga till spel i listan Spelappar i Spelprofil manuellt:

1. Klicka på **Verktyg** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fliken **Profiler** klickar du på **Inställningar**.
3. Klicka på knappen **KONFIGURERA** från området spelprofil.
4. I fönstret **Inställningar av spelprofil** klickar du på **Spellista**.
5. Klicka på **LÄGG TILL**.

Ett nytt fönster visas. Bläddra till spelets exekveringsfil, välj den och klicka på **OK** för att lägga till den till listan.

23.4. Publik Wi-Fi-profil

Att skicka e-post, skriv in känsliga personuppgifter eller shoppa online medan du är ansluten till osäkra trådlösa nätverk kan utsätta din personliga information för risk. Publik Wi-Fi-profil justerar produktinställningar för att ge dig möjlighet att göra betalningar online och använda känslig information i en skyddad miljö.

Konfigurera publik Wi-Fi-profil

För att konfigurera Bitdefender att använda produktinställningar när du är ansluten till ett osäkert trådlöst nätverk:

1. Klicka på **Verktyg** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fliken **Profiler** klickar du på **Inställningar**.
3. Klicka på knappen **KONFIGURERA** från området Publik Wi-Fi-profil.
4. Låt kryssrutan **Justerar produktinställningar för att öka skyddet när du är ansluten till ett osäkert publikt Wi-Fi-nätverk** vara markerad.
5. Klicka **Spara**.



23.5. Batterilägesprofil

Batterilägesprofil är specialdesignad för användare av bärbar dator och surfplatta. Dess syfte är att minimera både system- och Bitdefender-inverkan på strömförbrukning när batteriladdningsnivån är lägre än standard eller den du valt.

Konfigurera Batterilägesprofil

Konfigurera batterilägesprofil:

1. Klicka på **Verktyg** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fliken **Profiler** klickar du på **Inställningar**.
3. Klicka på knappen **Konfigurera** från området Batterilägesprofil.
4. Välj de systemjusteringar som ska tillämpas genom att markera följande alternativ:
 - Optimera produktinställningar för batteriläge.
 - Skjut upp bakgrundsprogram och underhållsuppgifter.
 - Skjut upp Windows automatiska uppdateringar.
 - Justera energiplansinställningar för batteriläge.
 - Inaktivera externa enheter och nätverksportar.
5. Klicka på **SPARA** för att spara ändringarna och stänga fönstret.

Skriv in ett giltigt läge i listrutan eller välj ett med upp- och nedpilarna för att ange när systemet ska gå över till batteriläge. Som standard aktiveras läget när batteriladdningsnivån faller lägre än 30 %.

Följande produktinställningar tillämpas när Bitdefender drivs av batterilägesprofilen:

- Bitdefender Automatisk uppdatering skjuts upp.
- Schemalagda skanningar skjuts upp.

Bitdefender upptäcker när din bärbara dator har växlat till batterikraft och utifrån batteriladdningsnivån går den automatiskt över till batteriläge. På samma sätt går Bitdefender automatiskt ur Batteriläge när det upptäcker att den bärbara datorn inte längre körs på batteri.



23.6. Realtidsoptimering

Bitdefender Realtidsoptimering är ett insticksprogram som förbättrar systemprestanda tyst, i bakgrunden, och ser till att du inte blir avbruten när du är i ett profilläge. Beroende på CPU-belastningen övervakar insticksprogrammet alla processer, med fokus på dem som tar upp en högre belastning, för att justera dem efter dina behov.

Aktivera eller inaktivera realtidsoptimering:

1. Klicka på **Verktyg** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I fliken **Profiler** klickar du på **Inställningar**.
3. Bläddra ned tills du ser alternativet Realtidsoptimering och använd sedan motsvarande omkopplare för att aktivera eller inaktivera.



24. DATASKYDD

24.1. Radera filer permanent

När du raderar en fil kan den inte längre nås på normalt sätt. Filen är dock fortfarande lagrad på hårddisken tills den skrivs över, då du kopierar nya filer.

Bitdefender File Shredder hjälper dig att radera data och fysiskt ta bort dem från din hårddisk permanent.

Du kan snabbt strimla filer eller mappar från enhet med Windows-kontextmenyn genom att följa de här stegen:

1. Högerklicka på den fil eller mapp du vill ta bort permanent.
2. Välj **Bitdefender** > **File Shredder** i kontextmenyn som visas.
3. Klicka på **Ta bort permanent** och bekräfta sedan att du vill fortsätta med processen.

Vänta medan Bitdefender slutför filborttagning.

4. Resultaten visas. Klicka på **Slutför** för att lämna guiden.

Alternativt kan du strimla filer från Bitdefender-gränssnittet enligt följande:

1. Klicka på **Verktyg** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **Dataskydd** klickar du på **File Shredder**.
3. Följ File Shredder-guiden:
 - a. Klicka på knappen **Lägg till mappar** för att lägga till filer och mappar du vill ta bort permanent.

Alternativt drar du dessa filer eller mappar till det här fönstret.

- b. Klicka på **Ta bort permanent** och bekräfta sedan att du vill fortsätta med processen.

Vänta medan Bitdefender slutför filborttagning.

- c. **Sammanfattning resultat**

Resultaten visas. Klicka på **Slutför** för att lämna guiden.



FELSÖKNING



25. LÖSA VANLIGA PROBLEM

Det här kapitlet presenterar några problem du kan stöta på när du använder Bitdefender och tillhandahåller dig med möjliga lösningar till dessa problem. De flesta av dessa problem kan lösas genom passande konfigurering av produktinställningarna.

- *"Mitt system verkar vara långsamt" (p. 134)*
- *"Skanningen startar inte" (p. 135)*
- *"Jag kan inte längre använda en app" (p. 138)*
- *"Vad du ska göra när Bitdefender blockerar en webbplats, en domän, en IP-adress eller en onlineapp som är säker." (p. 139)*
- *"Så här uppdaterar du Bitdefender på en långsam Internet-anslutning" (p. 140)*
- *"Tjänsterna för Bitdefender svarar inte" (p. 140)*
- *"Funktionen Autofill i min plånbok fungerar inte" (p. 141)*
- *"Bitdefender-borttagning misslyckades" (p. 142)*
- *"Mitt system startar inte efter att ha installerat Bitdefender" (p. 143)*

Om du ej kan finna ditt problem här eller om den valda lösningen inte fungerar kan du kontakta Bitdefender representanter för teknisk support som visat i kapitlet *"Be om hjälp"* (p. 154).

25.1. Mitt system verkar vara långsamt

Vanligtvis när man installerat ett säkerhetsprogram, kan det förekomma en liten sänkning av systemhastigheten, detta är i viss grad normalt.

Om du märker en betydande försämring av hastigheten kan bero på något av följande:

- **Bitdefender är inte det enda installerade säkerhetsprogrammet på systemet.**

Även om Bitdefender söker och tar bort funna säkerhetsprogram under installationen, rekommenderas det att man tar bort alla andra säkerhetslösningar du använder innan du installerar Bitdefender. Mer information finns på *"Hur tar jag bort andra säkerhetslösningar?"* (p. 65).

- **Systemkraven för att köra Bitdefender är inte uppfyllda.**



Om din maskin inte uppfyller systemkraven kommer enhet att bli trög, särskilt när flera olika appar körs samtidigt. Mer information finns på "[Systemkrav](#)" (p. 3).

● Du har installerat appar du inte använder.

Alla enheter har program eller appar som du inte använder. Och många oönskade program körs i bakgrunden vilket tar upp diskutrymme och minne. Om du inte använder ett program, avinstallera det. Det gäller även för annan förinstallerad programvara eller utvärderingsappar du glömt att ta bort.



Viktigt

Om du misstänker att ett program eller en app är en viktig del av ditt operativsystem tar du inte bort det och kontaktar Bitdefenders kundtjänst för att få hjälp.

● Ditt system kan vara infekterat.

Systemets hastighet och allmänna beteende kan också påverkas av hot. Spionprogramvara, skadlig kod, trojaner och adware belastar alla enhetens prestanda. Se till att du skannar systemet regelbundet, minst en gång i veckan. Vi rekommenderar att du använder Bitdefender Systemskanning eftersom den skannar efter alla typer av hot som riskerar säkerheten för ditt system.

Starta systemskanningen:

1. Klicka på **Skydd** på navigeringsmenyn i [Bitdefender-gränssnittet](#).
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**
3. I fönstret **Skanningar** klickar du på **Kör skanning** bredvid **Systemskanning**.
4. Följ guidestegen.

25.2. Skanningen startar inte

Denna typ av problem kan ha två huvudsakliga orsaker:

● En tidigare Bitdefenderinstallation som inte var helt borttagen eller en felaktig Bitdefenderinstallation.

I det här fallet installerar du om Bitdefender:



● I Windows 7:

1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
3. Klicka på **INSTALLERA OM** i det fönster som visas.
4. Vänta tills ominstallationens slutförts och starta sedan om ditt system.

● I Windows 8 och Windows 8.1:

1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **INSTALLERA OM** i det fönster som visas.
5. Vänta tills ominstallationens slutförts och starta sedan om ditt system.

● I Windows 10:

1. Klicka på **Start**, därefter på **Inställningar**.
2. Klicka på **System**-ikonen i området **Inställningar** och välj sedan **Installerade appar**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
5. Klicka på **INSTALLERA OM** i det fönster som visas.
6. Vänta tills ominstallationens slutförts och starta sedan om ditt system.



Notera

Genom att följa den här ominstallationsproceduren sparas anpassade inställningar och är tillgängliga i den nyinstallerade produkten. Andra inställningar kan växlas tillbaka till sin standardkonfiguration.

- **Bitdefender är inte den enda installerade säkerhetslösningen på ditt system.**

I det här fallet:



1. Ta bort den andra säkerhetslösningen. Mer information finns på "*Hur tar jag bort andra säkerhetslösningar?*" (p. 65).
2. Installera om Bitdefender:
 - **I Windows 7:**
 - a. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
 - b. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
 - c. Klicka på **INSTALLERA OM** i det fönster som visas.
 - d. Vänta tills ominstallationens slutförts och starta sedan om ditt system.
 - **I Windows 8 och Windows 8.1:**
 - a. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
 - b. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
 - c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
 - d. Klicka på **INSTALLERA OM** i det fönster som visas.
 - e. Vänta tills ominstallationens slutförts och starta sedan om ditt system.
 - **I Windows 10:**
 - a. Klicka på **Start**, därefter på **Inställningar**.
 - b. Klicka på **System**-ikonen i området **Inställningar** och välj sedan **Installerade appar**.
 - c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
 - d. Klicka på **Avinstallera** igen för att bekräfta ditt val.
 - e. Klicka på **INSTALLERA OM** i det fönster som visas.
 - f. Vänta tills ominstallationens slutförts och starta sedan om ditt system.



Notera

Genom att följa den här ominstallationsproceduren sparas anpassade inställningar och är tillgängliga i den nyinstallerade produkten. Andra inställningar kan växlas tillbaka till sin standardkonfiguration.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion "*Be om hjälp*" (p. 154).

25.3. Jag kan inte längre använda en app

Detta problem inträffar när du försöker använda ett program som fungerade normalt innan du installerade Bitdefender.

När du har installerat Bitdefender kan du stöta på någon av följande situationer:

- Du kan få ett meddelande från Bitdefender om att programmet försöker göra en ändring av systemet.
- Det kan hända att du får ett felmeddelande från programmet du försöker använda.

Detta inträffar när Advanced Threat Defense av misstag anger vissa appar som skadliga.

Advanced Threat Defense är en Bitdefender-funktion som hela tiden övervakar de program som körs på ditt system och rapporterar de med potentiellt skadligt beteende. Eftersom den här funktion baseras på ett heuristiskt system kan det finnas fall då legitima appar rapporteras av Advanced Threat Defense.

När den här situationen kan du undanta respektive app från att övervakas av Advanced Threat Defense.

Lägga till en app i undantagslistan:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **ADVANCED THREAT DEFENSE** klickar du på **Öppna**.
3. I fönstret **Inställningar** klickar du på **Hantera undantag**.
4. Klicka på **+Lägg till undantag**.
5. Ange sökvägen till filen du vill undanta från skanning i motsvarande fält.



Du kan även navigera till program genom att klicka på bläddra-knappen till höger i gränssnittet, välja den och klicka på **OK**.

6. Aktivera reglaget bredvid **Advanced Threat Defense**.

7. Klicka **Spara**.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion "*Be om hjälp*" (p. 154).

25.4. Vad du ska göra när Bitdefender blockerar en webbplats, en domän, en IP-adress eller en onlineapp som är säker.

Bitdefender erbjuder en säker surfupplevelse genom att filtrera all webbttrafik och blockera skadligt innehåll. Det är dock möjligt att Bitdefender ser en webbplats, en domän, en IP-adress eller onlineapp som är säker som osäker, vilket gör att Bitdefender HTTP-trafikskanning blockerar dem felaktigt.

Om samma sida, domän, IP-adress eller app blockeras flera gånger kan de läggas till i undantagen så att de inte skannas av Bitdefender-motorerna, och därmed säkerställa en smidig surfupplevelse.

Lägg till en webbplats till **Undantag**:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **FÖREBYGGANDE AV ONLINEHOT** klickar du på **Inställningar**.
3. Klicka på **Hantera undantag**.
4. Klicka på **+Lägg till undantag**.
5. Skriv namnet på webbplatsen, domänen eller IP-adressen du vill lägga till i undantagen i motsvarande fält.
6. Klicka på reglaget bredvid **Onlinehotskydd**.
7. Klicka **Spara** för att spara ändringarna och stänga fönstret.

Endast webbsidor, domäner IP-adresser och appar du litar på helt ska läggas till i den här listan. Dessa undantas från skanning av följande motorer: hot, nätfiske och bedrägeri.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion "*Be om hjälp*" (p. 154).



25.5. Så här uppdaterar du Bitdefender på en långsam Internet-anslutning

Om du har en långsam Internet-anslutning (som uppringd) kan fel inträffa under uppdateringsprocessen.

För att se till att systemet är uppdaterat med den senaste Bitdefender-hotinformationsdatabasen:

1. Klicka på **Inställningar** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. Välj fliken **Uppdatera**.
3. Inaktivera omkopplaren **Tyst uppdatering** switch.
4. Nästa gång en uppdatering är tillgänglig uppmanas du att välja vilken uppdatering du vill ladda ner. Välj endast **Uppdatering av signaturer**.
5. Bitdefender hämtar och installerar bara hotinformationsdatabasen.

25.6. Tjänsterna för Bitdefender svarar inte

Denna artikel hjälper dig att felsöka felet **Bitdefender Tjänster svarar inte**. Du kan få det här problemet på följande sätt:

- Bitdefender-ikonen i **systemfältet** är utgråad och du informeras om att Bitdefender-tjänsterna inte svarar.
- Bitdefenderfönstret visar att Bitdefenders tjänster inte svarar.

Felet kan vara orsakat av något av följande:

- temporära kommunikationsfel mellan Bitdefendertjänsterna.
- några av Bitdefender tjänster har stoppats
- andra säkerhetslösningar körs på din enhet samtidigt som Bitdefender.

För att felsöka detta fel, testa dessa lösningar:

1. Vänta en stund och se om något förändras. Felet kan vara temporärt.
2. Starta om enheten och vänta ett tag tills Bitdefender har laddats. Öppna Bitdefender för att se om felet kvarstår. Omstart av enheten löser oftast problemet.
3. Kontrollera om du har en annan säkerhetslösning installerad då den i så fall kan störa Bitdefender normala aktivitet. Om så är fallet rekommenderar



vi dig att ta bort alla andra säkerhetslösningar och sedan installera Bitdefender igen.

Mer information finns på "*Hur tar jag bort andra säkerhetslösningar?*" (p. 65).

Om felet kvarstår kontaktar du våra supportmedarbetare för hjälp, såsom beskrivs i avsnitt "*Be om hjälp*" (p. 154).

25.7. Funktionen Autofill i min plånbok fungerar inte

Du har sparat dina onlineuppgifter i din Bitdefender Password Manager och du märker att automatisk ifyllnad inte fungerar. Oftast dyker det här problemet upp när Bitdefender-plånbokstilläget inte är installerat i din webbläsare.

Följ de här stegen för att lösa den här situationen:

● I Internet Explorer:

1. Öppna Internet Explorer.
2. Klicka på Verktyg.
3. Klicka på Hantera tillägg.
4. Klicka på Verktygsfält och tillägg.
5. Peka på **Bitdefender-plånbok** och klicka på **Aktivera**.

● I Mozilla Firefox:

1. Öppna Mozilla Firefox.
2. Klicka på knappen **Öppna meny** i det övre högra hörnet av skärmen.
3. Klicka på Tilläggsprogram.
4. Klicka på Tillägg.
5. Peka på **Bitdefender Wallet** och klicka på reglaget bredvid den.

● I Google Chrome:

1. Öppna Google Chrome.
2. Gå till Meny-ikonen.
3. Klicka på Fler verktyg.
4. Klicka på Tillägg.
5. Peka på **Bitdefender Wallet** och klicka på dess motsvarande reglage.



Notera

Tillägget aktiveras när du startat om webbläsaren.

Kontrollera nu om funktionen för automatisk ifyllnad i plånboken fungerar för dina onlinekonton.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion "*Be om hjälp*" (p. 154).

25.8. Bitdefender-borttagning misslyckades

Om du vill ta bort din Bitdefender-produkt och märker att processen hänger sig eller systemet fryser, så klickar du på **Avbryt** för att avbryta åtgärden. Om det inte fungerar startar du om systemet.

När borttagning misslyckas kan vissa Bitdefender-registernycklar och filer vara kvar i systemet. Sådana rester kan förhindra en ny installation av Bitdefender. De kan även påverka systemets prestanda och stabilitet.

Gör så här för att helt ta bort Bitdefender från systemet:

● I Windows 7:

1. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
2. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
3. Klicka på **TA BORT** i det fönster som visas.
4. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

● I Windows 8 och Windows 8.1:

1. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
2. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **TA BORT** i det fönster som visas.
5. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

● I Windows 10:

1. Klicka på **Start**, därefter på **Inställningar**.



2. Klicka på **System**-ikonen i området Inställningar och välj sedan **Installerade appar**.
3. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
4. Klicka på **Avinstallera** igen för att bekräfta ditt val.
5. Klicka på **TA BORT** i det fönster som visas.
6. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

25.9. Mitt system startar inte efter att ha installerat Bitdefender

Om du precis har installerat Bitdefender och inte kan starta om systemet i normalt läge längre kan det finns flera olika orsaker till det här problemet.

Mest troligt är att det orsakas av en tidigare Bitdefender-installation, som inte togs bort korrekt eller av en annan säkerhetslösning som fortfarande finns kvar på systemet.

Så här kan du ta hand om varje situation:

● Du hade Bitdefender tidigare och du tog inte bort det ordentligt.

För att lösa det:

1. Starta om ditt system och gå in i felsäkert läge. Se i "*Hur startar jag om i Felsäkert läge?*" (p. 66) hur du gör det.
2. Ta bort Bitdefender från ditt system:
 - **I Windows 7:**
 - a. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
 - b. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
 - c. Klicka på **TA BORT** i det fönster som visas.
 - d. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
 - e. Starta om systemet i normalt läge.
 - **I Windows 8 och Windows 8.1:**



- a. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.
- b. Klicka på **Avinstallera ett program** eller **Program och funktioner**.
- c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
- d. Klicka på **TA BORT** i det fönster som visas.
- e. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
- f. Starta om systemet i normalt läge.

● **I Windows 10:**

- a. Klicka på **Start**, därefter på **Inställningar**.
- b. Klicka på **System**-ikonen i området **Inställningar** och välj sedan **Installerade appar**.
- c. Hitta **Bitdefender Antivirus Plus** och välj **Avinstallera**.
- d. Klicka på **Avinstallera** igen för att bekräfta ditt val.
- e. Klicka på **TA BORT** i det fönster som visas.
- f. Vänta tills avinstallationen slutförts och starta sedan om ditt system.
- g. Starta om systemet i normalt läge.

3. Installera om din Bitdefender-produkt.

● **Du hade en annan säkerhetslösning tidigare och du tog inte bort den ordentligt.**

För att lösa det:

1. Starta om ditt system och gå in i felsäkert läge. Se i "*Hur startar jag om i Felsäkert läge?*" (p. 66) hur du gör det.
2. Ta bort den andra säkerhetslösningen från systemet:

● **I Windows 7:**

- a. Klicka **Starta**, för att gå till **Kontrollpanelen** och dubbelklicka **Program och Funktioner**.
- b. Hitta namnet på det program du vill ta bort och välj **Ta bort**.



c. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

● **I Windows 8 och Windows 8.1:**

a. Från startskärmen i Windows letar du upp **Kontrollpanelen** (du kan till exempel börja skriva "Kontrollpanel" direkt på startskärmen) och sedan klicka på ikonen.

b. Klicka på **Avinstallera ett program** eller **Program och funktioner**.

c. Hitta namnet på det program du vill ta bort och välj **Ta bort**.

d. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

● **I Windows 10:**

a. Klicka på **Start**, därefter på **Inställningar**.

b. Klicka på **System**-ikonen i området **Inställningar** och välj sedan **Installerade appar**.

c. Hitta namnet på det program du vill ta bort och välj **Avinstallera**.

d. Vänta tills avinstallationen slutförts och starta sedan om ditt system.

För att korrekt avinstallera den andra programvaran går du till deras webbplats och kör deras avinstallationsverktyg eller kontaktar dem direkt så att de kan ge dig riktlinjer för avinstallationen.

3. Starta om systemet i normalt läge och installera om Bitdefender.

Du har redan följt stegen ovan och situationen är inte löst.

För att lösa det:

1. Starta om ditt system och gå in i felsäkert läge. Se i "*Hur startar jag om i Felsäkert läge?*" (p. 66) hur du gör det.

2. Använd alternativet Systemåterställning från Windows för att återställa enheten till ett tidigare datum innan du installerade Bitdefender-produkten.

3. Starta om systemet i normalt läge och kontakta vår support för hjälp såsom beskriv i avsnitt "*Be om hjälp*" (p. 154).



26. TA BORT HOT FRÅN DITT SYSTEM

Hot kan påverka ditt system på många olika sätt och Bitdefender tillvägagångssätt beror på typen av hotattack. Eftersom hota ofta ändrar sitt beteende är det svårt att bestämma ett mönster för deras beteenden och handlingar.

Det finns situationer när Bitdefender inte automatiskt kan ta bort hotinfektionen från ditt system. I sådana fall krävs en åtgärd av dig.

- *"Räddningsmiljön" (p. 146)*
- *"Vad ska du göra när Bitdefender hittar hot på enheten?" (p. 147)*
- *"Hur rensar jag bort ett hot i ett arkiv?" (p. 148)*
- *"Hur rensar jag ett e-postarkiv från hot?" (p. 149)*
- *"Vad gör jag om jag misstänker att en fil är farlig?" (p. 150)*
- *"Vad är de lösenordsskyddade filerna i skanningsloggen?" (p. 151)*
- *"Vad är de överhoppade posterna i skanningsloggen?" (p. 151)*
- *"Vad är de överkomprimerade filerna i skanningsloggen?" (p. 151)*
- *"Varför raderade Bitdefender en infekterad fil automatiskt?" (p. 152)*

Om du ej kan finna ditt problem här eller om den valda lösningen inte fungerar kan du kontakta Bitdefender representanter för teknisk support som visat i kapitlet *"Be om hjälp"* (p. 154).

26.1. Räddningsmiljön

Räddningsmiljö är en Bitdefender-funktion som gör att du kan skanna och desinfektera alla befintliga hårddiskpartitioner inuti och utanför ditt operativsystem.

Bitdefender Räddningsmiljö är integrerad med Windows RE,

Startar ditt system i Räddningsmiljö

Du kan endast komma in i räddningsmiljön från din Bitdefender-produkt enligt följande:

1. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
2. I panelen **VIRUSSKYDD** klickar du på **Öppna**



3. Klicka på **Öppna** bredvid **Räddningsmiljö**.
4. Klicka på **STARTA OM** i det fönster som visas.
Bitdefender Rescue Environment laddas på några minuter.

Skannar ditt system i Räddningsmiljö

För att skanna ditt system i Räddningsmiljö:

1. Öppna räddningsläget såsom beskrivs i "**Startar ditt system i Räddningsmiljö**" (p. 146).
2. Bitdefender-skanningsprocessen startar automatiskt så fort systemet laddas i räddningsmiljön.
3. Vänta tills skanningen är klar. Om ett hot upptäcks följer du instruktionerna för att ta bort det.
4. Avsluta Räddningsmiljö genom att klicka på knappen **Stäng** i fönstret med skanningsresultaten.

26.2. Vad ska du göra när Bitdefender hittar hot på enheten?

Du kan få reda på att det finns hot på enheten på något av följande sätt:

- Du skannade din enhet och Bitdefender fann infekterade objekt på den.
- En hotvarning meddelar dig om att Bitdefender blockerat ett eller flera hot på din enhet.

I dessa situationer uppdaterar du Bitdefender för att försäkra dig om att du har den senaste hotinformationsdatabasen och kör en systemskanning för att analysera systemet.

Så fort systemskanningen är avslutad, väljer du önskad åtgärd för de infekterade objekten (desinficera, radera, flytta till karantän).

- ⊗ **Varning**
Om du misstänker att en fil är en del av Windows operativsystem eller att det inte är en infekterad fil, följ inte dessa steg utan kontakta Bitdefender kundtjänst så snart som möjligt.

Om vald handling inte kunde utföras och att loggen för skanning visar att en smitta inte kunde tas bort, måste filen (-erna) tas bort manuellt.



Den första metoden kan användas i normalt läge:

1. Slå av Bitdefenders realtidsskydd:
 - a. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
 - b. I panelen **VIRUSSKYDD** klickar du på **Öppna**
 - c. I fönstret **Avancerat** stänger du av **Bitdefender Shield**.
2. Visa dolda objekt i Windows. Se i "*Hur visar jag dolda objekt i Windows?*" (p. 65) hur du gör det.
3. Bläddra till den infekterade filens plats (sök igenom skanningsloggen) och radera den.
4. Slå på Bitdefender realtids-antiviruskydd.

Om den första metoden misslyckas med att ta bort infektionen:

1. Starta om ditt system och gå in i felsäkert läge. Se i "*Hur startar jag om i Felsäkert läge?*" (p. 66) hur du gör det.
2. Visa dolda objekt i Windows. Se i "*Hur visar jag dolda objekt i Windows?*" (p. 65) hur du gör det.
3. Bläddra till den infekterade filens plats (sök igenom skanningsloggen) och radera den.
4. Starta om ditt system och gå in i normalt läge.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion "*Be om hjälp*" (p. 154).

26.3. Hur rensar jag bort ett hot i ett arkiv?

En komprimerad fil innehåller en eller flera filer som packats ihop till ett speciellt format för att spara på diskutrymmet.

Vissa av dessa format är öppna format, och tillhandahåller såvida Bitdefender möjligheten att skanna dem på insidan för att sen vidta passande åtgärder för att ta bort dem.

Andra komprimerade format är delvis eller helt stängda och Bitdefender kan endast hitta hot inuti dem, men kan inte vidta andra åtgärder.

Om Bitdefender meddelar dig om att ett hot upptäckts inuti ett arkiv och att ingen åtgärd är tillgänglig, betyder detta att det inte är möjligt att ta bort hotet på grund av begränsningar av arkivets inställningar för behörigheter.



Så här kan du rensa bort ett hot som lagrats i ett arkiv:

1. Identifiera arkivet som innehåller hotet genom att utföra en Systemskanning av systemet.
2. Slå av Bitdefenders realtidsskydd:
 - a. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
 - b. I panelen **VIRUSSKYDD** klickar du på **Öppna**
 - c. I fönstret **Avancerat** stänger du av **Bitdefender Shield**.
3. Gå till arkivets plats och dekomprimera det genom att använda en arkiveringsapp, som WinZip.
4. Identifiera den infekterade filen och radera den.
5. Radera det ursprungliga arkivet för att vara säker på att infektionen är fullständigt borttagen.
6. Komprimera filerna i ett nytt arkiv med hjälp av en arkiveringsapp, som WinZip.
7. Slå igång Bitdefenders realtidsskydd och kör en systemskanning för att försäkra dig om att det inte finns någon mer infektion på systemet.



Notera

Det är viktigt att notera, att ett hot som är lagrat i ett arkiv inte utgör ett omedelbart hot mot ditt system eftersom hotet måste expanderas och verkställas för att kunna infektera ditt system.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 154).

26.4. Hur rensar jag ett e-postarkiv från hot?

Bitdefender kan också identifiera hot i e-postdatabaser och e-postarkiv lagrade på en disk.

Ibland är det nödvändigt att identifiera det infekterade meddelandet, genom att använda den information du fått i skanningsrapporten, och radera det manuellt.

Så här kan du rensa bort ett hot som lagrats i ett e-postarkiv:

1. Skanna e-postdatabasen med Bitdefender.
2. Slå av Bitdefenders realtidsskydd:



- a. Klicka på **Skydd** på navigeringsmenyn i **Bitdefender-gränssnittet**.
 - b. I panelen **VIRUSSKYDD** klickar du på **Öppna**
 - c. I fönstret **Avancerat** stänger du av **Bitdefender Shield**.
3. Öppna skanningsrapporten och använd identifieringsinformationen (ämne, från, till) från de infekterade meddelandena för att hitta dem i din e-postklient.
 4. Radera de infekterade meddelandena. De flesta e-postklienter flyttar även det raderade meddelandet till en återställningsmapp, från vilken meddelandet kan återställas. Du bör försäkra dig om att meddelandet även är raderat från denna återställningsmapp.
 5. Komprimera mappen som innehåller det infekterade meddelandet.
 - I Microsoft Outlook 2007: I filmenyn, klicka datafilshantering. Välj de personliga mappar-filerna (.pst) du har tänkt komprimera och klicka sen på inställningar. Klicka på Packa nu.
 - I Microsoft Outlook 2010/2013/2016: På menyn Arkiv klickar du på Info och därefter på Kontoinställningar (Lägg till eller ta bort konton eller ändra befintliga anslutningsinställningar). Klicka sedan på Dataarkiv, välj de personliga mappfiler (.pst) du avser att komprimera och klicka på Inställningar. Klicka på Packa nu.
 6. Slå på Bitdefender realtids-antiviruskydd.

Om inte denna information var hjälpsam kan du kontakta Bitdefender för support som beskrivet i sektion *"Be om hjälp"* (p. 154).

26.5. Vad gör jag om jag misstänker att en fil är farlig?

Du kan misstänka att en fil från ditt system är farlig, även om din Bitdefender-produkt inte upptäckte den.

För vara säker på att ditt system är skyddat:

1. Kör en **Systemskanning** med Bitdefender. Se i *"Hur skannar jag mitt system?"* (p. 51) hur du gör det.
2. Om skanningsresultatet visar sig vara rent, men du fortfarande är tveksam och vill vara säker på filen, kontaktar du vår support så att vi kan hjälpa dig.

Se i *"Be om hjälp"* (p. 154) hur du gör det.



26.6. Vad är de lösenordsskyddade filerna i skanningsloggen?

Det här är bara ett meddelande som visar att Bitdefender har upptäckt att dessa filer antingen skyddas med ett lösenord eller någon form av kryptering.

De vanligaste lösenordsskyddade posterna är:

- Filer som tillhör en annan säkerhetslösning.
- Filer som hör till operativsystemet.

För att verkligen kunna skanna innehållet, skulle dessa filer behöva antingen extraheras eller på annat sätt avkrypteras.

Skulle dessa innehåll extraheras, skulle Bitdefenders realtidsskanner automatiskt skanna dem för att hålla din enhet skyddad. Om du vill skanna de filerna med Bitdefender måste du kontakta tillverkaren av produkten så att de kan ge dig fler detaljer om filerna.

Vår rekommendation till dig är att ignorera dessa filer då de ej utgör något hot mot ditt system.

26.7. Vad är de överhoppade posterna i skanningsloggen?

Alla filer som visas som överhoppade i skanningsrapporten är rena.

För bättre prestanda skannar inte Bitdefender filer som inte har ändrats sedan den senaste skanningen.

26.8. Vad är de överkomprimerade filerna i skanningsloggen?

De överkomprimerade posterna är delar som inte kunde extraheras av skanningsmotorn, eller delar som det skulle ta för lång tid att dekryptera vilket skulle göra systemet instabilt.

Överkomprimerad betyder att Bitdefender hoppade över skanning av det arkivet eftersom det skulle krävas för stora systemresurser för att packa upp det. Innehållet kommer att skannas i realtid vid behov.



26.9. Varför raderade Bitdefender en infekterad fil automatiskt?

Om en infekterad fil upptäcks, kommer Bitdefender automatiskt att försöka desinficera den. Om desinficering misslyckas flyttas filen till karantän för att innesluta infektionen.

För vissa typer av hot är desinfektion inte möjligt, eftersom den upptäckta filen är helt och hållet skadlig. Vid sådana tillfällen raderas den infekterade filen från enheten.

Detta är vanligtvis fallet med installationsfiler som hämtas från opålitliga webbsidor. Om du hamnar i en sådan situation, hämta installationsfilen från tillverkarens webbsida eller annan betrodd webbsida.



CONTACT US



27. BE OM HJÄLP

Bitdefender erbjuder sina kunder en överträffad nivå av snabb och korrekt support. Om du upplever några problem med, eller om du har några frågor om din Bitdefender-produkt kan du använda flera resurser på nätet för att hitta en lösning eller ett svar. Samtidigt kan du kontakta Bitdefenders kundtjänst. Våra supportmedarbetare besvarar dina frågor snabbt och ger dig den hjälp du behöver.

Avsnitt "*Lösa vanliga problem*" (p. 134) innehåller den nödvändiga informationen avseende de vanligaste problemen du kan stöta på när du använder den här produkten.

Om du inte svaret på din fråga med de resurser du fått kan du kontakta oss direkt:

- "*Kontakta oss direkt från Bitdefender Antivirus Plus*" (p. 154)
- "*Kontakta oss via vårt onlinesupportcenter*" (p. 155)

Kontakta oss direkt från Bitdefender Antivirus Plus

Om du har en fungerande Internet-anslutning kan du kontakta Bitdefender för hjälp direkt från produktgränssnittet.

Följ dessa steg:

1. Klicka på knappen **Support**, som motsvaras av ett **frågetecken** i den övre delen av **Bitdefender-gränssnittet**.
2. Du har följande alternativ:

- **ANVÄNDARGUIDE**

Gå till vår databas och sök efter nödvändig information.

- **SUPPORTCENTER**

Gå till våra onlineartiklar och videohandledningarna.

- **KONTAKTA SUPPORT**

Klicka på **KONTAKTA SUPPORT** för att starta Bitdefender-supportverktyget och kontakta kundtjänsten.

- a. Fyll i formuläret med nödvändig information:
 - i. Välj vilken typ av problem du upplever.



- ii. Skriv en beskrivning av det problem du stötte på.
 - iii. Klicka på **FÖRSÖK ATT ÅTERSKAPA DET HÄR PROBLEMET** ifall du stöter på ett produktproblem. Återskapa problemet och klicka därefter på **SLUTFÖR** i ramen ÅTERSKAPA PROBLEMET.
 - iv. Klicka på **BEKRÄFTA ÄRENDE**.
- b. Fortsätt fylla i formuläret med nödvändig information.
- i. Skriv ditt fullständiga namn.
 - ii. Ange din e-postadress.
 - iii. Markera avtalskryssrutan.
 - iv. Klicka **SKAPA FELSÖKNINGSPAKET**.
- Vänta en stund medan Bitdefender samlar in produktrelaterad information. Denna information kommer att hjälpa våra tekniker att finna en lösning på ditt problem.
- c. Klicka på **STÄNG** för att lämna guiden. Du kommer att bli kontaktad så fort som möjligt av en av våra medarbetare.

Kontakta oss via vårt onlinesupportcenter

Om du inte kommer åt nödvändig information via Bitdefender-produkten, gå till vårt onlinesupportcenter:

1. Gå till <https://www.bitdefender.com/support/consumer.html>.

Bitdefender Support Center har flera artiklar som innehåller lösningar på Bitdefender-relaterade frågor.

2. Använd sökfältet längst upp i fönstret för att hitta artiklar som kan ge en lösning på ditt problem. För att söka skriver du bara in en term i sökfältet och klickar på **Sök**.
3. Läs de relevanta artiklarna och dokumenten, och prova de föreslagna lösningarna.
4. Om lösningen inte löser ditt problem går du till

<https://www.bitdefender.com/support/contact-us.html> och kontaktar våra supportmedarbetare.



28. ONLINERESURSER

Flera på nätet-resurser finns tillgängliga för att hjälpa dig med att lösa dina Bitdefender-relaterade problem och frågor.

- Bitdefenders supportcenter:

<https://www.bitdefender.com/support/consumer.html>

- Bitdefender Supportforum:

<https://forum.bitdefender.com>

- Datorsäkerhetsportalen HOTforSecurity:

<https://www.hotforsecurity.com>

Du kan även använda din favoritsökmotor för att hitta mer information om datorsäkerhet, Bitdefenderprodukter och företaget.

28.1. Bitdefenders supportcenter

Bitdefenders supportcenter är en databas med information om Bitdefenderprodukter på nätet. Den lagrar, i ett lättåtkomligt format, rapporter om resultaten för utgående teknisk support och felkorrigeringsåtgärder för Bitdefenders support- och utvecklingsteam, tillsammans med mer allmänna artiklar om hotförebyggande, hantering av Bitdefender-lösningar med detaljerade förklaringar och många andra artiklar.

Bitdefenders supportcenter är öppet för allmänheten och gratis att söka igenom. Den omfattande information den innehåller är ännu ett sätt att förse Bitdefenders kunder med den tekniska kunskap och insikt de behöver. Alla giltiga begäran om information eller buggrapporter som kommer från Bitdefender-klienter hittar till slut in i Bitdefenders supportcenter, som felkorrigeringsrapporter, workaroundsbeskrivningar eller informationsartiklar som tillägg till produkthjälpfiler.

Bitdefendera supportcenter är alltid tillgängligt på

<https://www.bitdefender.com/support/consumer.html>.

28.2. Bitdefender Supportforum

Bitdefender Supportforum tillhandahåller Bitdefender användare med ett enkelt sätt att få hjälp samt att hjälpa andra.



Om din Bitdefenderprodukt inte fungerar som den ska, om den inte kan ta bort särskilda hot från din enhet eller om du har frågor om hur den fungerar, posta dina problem eller frågor i forumet.

Bitdefenders supporttekniker söker i forumet efter nya poster för att kunna hjälpa dig. Du kan även få svar eller en lösning från en mer van Bitdefenderanvändare.

Innan du skickar ditt problem eller din fråga, sök igenom forumet efter ett liknande eller relaterat ämne.

Bitdefenders supportforum är tillgängligt på <https://forum.bitdefender.com>, på 5 olika språk: Engelska, Tyska, Franska, Spanska och Rumänska. Klicka länken **Hemma & Hemma Kontor Skydd** för att öppna sektionen som är avsedd för konsumentprodukter.

28.3. HOTforSecurity Portal

HOTforSecurity är en rik källa till datorsäkerhetsinformation. Här kan du lära dig om olika hot din enhet utsätts för när den är ansluten till Internet (skadlig kod, nätfiske, spam, cyberbrottslingar).

Nya artiklar postas regelbundet för att hålla dig uppdaterad med de senaste hot som upptäckts, de nuvarande säkerhetstrenderna och annan information om branschen för datorsäkerhet.

Webbsidan HOTforSecurity är <https://www.hotforsecurity.com>.



29. CONTACT INFORMATION

Effektiv kommunikation är nyckeln till en framgångsrik affärsverksamhet. Sedan 2001 har BITDEFENDER etablerat ett obestriddigt anseende genom att hela tiden sträva efter bättre kommunikation för att överträffa våra klienters och partners förväntningar. Om du har frågor, tveka inte att kontakta oss.

29.1. Webbadresser

Försäljningsavdelning: sales@bitdefender.com

Supportcenter: <https://www.bitdefender.com/support/consumer.html>

Dokumentation: documentation@bitdefender.com

Lokala återförsäljare: <https://www.bitdefender.com/partners>

Partnerprogram: partners@bitdefender.com

Mediarelationer: pr@bitdefender.com

Jobbmöjligheter: jobs@bitdefender.com

Virusinlagor: virus_submission@bitdefender.com

Skräppostinlagor: spam_submission@bitdefender.com

Rapportera missbruk: abuse@bitdefender.com

Webbsida: <https://www.bitdefender.com>

29.2. Lokala återförsäljare

Bitdefenders lokala återförsäljare är redo att svara på alla frågor rörande deras uppgiftsområde, både i kommersiella allmänna ärenden.

För att finna en återförsäljare av Bitdefender i ditt land:

1. Gå till <https://www.bitdefender.com/partners/partner-locator.html>.
2. Välj ditt land och din ort genom att använda motsvarande alternativ.
3. Om du inte hittar någon Bitdefender-återförsäljare i ditt land får du gärna kontakta oss via e-post på sales@bitdefender.com. Skriv ditt e-postmeddelande på engelska så att vi kan hjälpa dig så snart som möjligt.

29.3. Bitdefender-kontor

Bitdefenders kontor är redo att svara på alla frågor rörande deras verksamhetsområde, både i kommersiella och allmänna ärenden. Deras respektive adresser och kontakter finns listade nedanför.



U.S.A

Bitdefender, LLC

6301 NW 5th Way, Suite 4300

Fort Lauderdale, Florida 33309

Telefon (office&sales): 1-954-776-6262

Försäljning: sales@bitdefender.com

Tekniskt stöd: <https://www.bitdefender.com/support/consumer.html>

Webb: <https://www.bitdefender.com>

UK och Irland

BITDEFENDER LTD

C/O Howsons Winton House, Stoke Road, Stoke on Trent

Staffordshire, United Kindon, ST4 2RW

Email: info@bitdefender.co.uk

Phone: (+44) 2036 080 456

Försäljning: sales@bitdefender.co.uk

Tekniskt stöd: <https://www.bitdefender.co.uk/support/>

Webb: <https://www.bitdefender.co.uk>

Tyskland

Bitdefender GmbH

TechnoPark Schwerte

Lohbachstrasse 12

D - 58239 Schwerte

Office: +49 2304 9 45 - 162

Fax: +49 2304 9 45 - 169

Försäljning: vertrieb@bitdefender.de

Tekniskt stöd: <https://www.bitdefender.de/support/consumer.html>

Webb: <https://www.bitdefender.de>

Danmark

Bitdefender APS

Agern Alle 24, 2970 Hørsholm, Denmark

Office: +45 7020 2282

Tekniskt stöd: <http://bitdefender-antivirus.dk/>

Webb: <http://bitdefender-antivirus.dk/>



Spanien

Bitdefender España, S.L.U.

C/Bailén, 7, 3-D

08010 Barcelona

Fax: +34 93 217 91 28

Phone: +34 902 19 07 65

Försäljning: comercial@bitdefender.es

Tekniskt stöd: <https://www.bitdefender.es/support/consumer.html>

Webbsida: <https://www.bitdefender.es>

Rumänien

BITDEFENDER SRL

Orhideea Towers Building, 15A Orhideelor Street, 11th floor, district 6

Bucharest

Fax: +40 21 2641799

Försäljning Telefon: +40 21 2063470

Försäljnings-e-post: sales@bitdefender.ro

Tekniskt stöd: <https://www.bitdefender.ro/support/consumer.html>

Webbsida: <https://www.bitdefender.ro>

Förenade Arabemiraten

Dubai Internet City

Building 17, Office # 160

Dubai, UAE

Försäljning Telefon: 00971-4-4588935 / 00971-4-4589186

Försäljnings-e-post: mena-sales@bitdefender.com

Tekniskt stöd: <https://www.bitdefender.com/support/consumer.html>

Webbsida: <https://www.bitdefender.com>



Ordlista

Abonnemang

Köpeavtal som ger användaren behörighet att använda en viss produkt eller tjänst på ett visst antal enheter och för en viss tidsperiod. En utgången prenumeration kan automatiskt förnyas med den information som användaren uppger vid det första köpet.

ActiveX

ActiveX är ett sätt att skriva program på så att andra program kan anropa dem. ActiveX-teknik används med Microsoft Internet Explorer för att skapa interaktiva webbsidor som ser ut och uppför sig som datorprogram mer än statiska sidor. med ActiveX kan användare ställa eller besvara frågor, använda knappar och interagera på andra sätt med webbsidan. ActiveX-kontroller är ofta skrivna i Visual Basic.

Active X är känt för total avsaknad av säkerhetskontroller; experter på datorsäkerhet avråder från att använda det på Internet.

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.

Annonsprogram

Annonsprogram kombineras ofta med ett världprogram som är gratis så länge som användaren går med på att tillåta annonsprogrammet. Eftersom sådana program oftast installeras efter att användaren gått med på licensavtalet, har inget brott begåtts.

Popup-reklam kan dock bli ett irritationsmoment, och i vissa fall försämra systemets prestanda. Även den privata information som vissa av dessa program samlar in kan vara oroande för användare som inte var fullt medvetna om villkoren i licensavtalet.

Arkiv

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



En fil som innehåller en eller flera komprimerade filer.

Avancerat kvarstående hot

APT (Advanced persistent threat) exploaterar säkerhetsrisker i system för att stjäla viktig information att leverera till källan. Stora grupper som organisationer, företag eller myndigheter, är måltavlor för detta hot.

Målet med ett APT är att förbli oupptäckt under en lång tid för att kunna övervaka och samla in viktig information utan att skada målmaskinerna. Den metod som används är att injicera hotet i nätverket via en PDF-fil eller ett Office-dokument som ser ofarligt ut så att alla användare kan köra filerna.

Bakdörr

Ett hål i säkerhetssystemet som avsiktligen lämnats av de som utformat och underhåller systemet. Meningen med sådana hål är inte alltid ondskefull, till exempel, "come out of the box with privileged accounts" är menat för fälttekniker eller för försäljarens underhållsprogrammerare.

Boot sector

En sektor i början av varje enhet som identifierar enhetens arkitektur (sektorstorlek, klusterstorlek osv). För startenheter innehåller boot-sektorn även ett program laddar operativsystemet.

Boot virus

Ett hot som infekterar startsektorn på en fast eller flyttbar disk. Ett försök att starta från en diskett infekterad med ett startsektorvirus gör att viruset blir aktivt i minnet. Varje gång du startar ditt system från och med nu innebär att du har hotet aktivt i minnet.

Botnet

Termen "botnet" är sammansatt av orden "robot" och "nätverk". Botnets är Internet-anslutna enheter infekterade med hot och som kan användas för att skicka skräppost, stjäla data, fjärrstyra sårbara enheter eller sprida spionprogramvara, ransomware och andra typer av hot. Deras mål är att infektera så många anslutna enheter som möjligt, som datorer, servrar, mobil- eller IoT-enheter som tillhör stora företag eller industrier.

E-post

Elektronisk post. En tjänst som sänder datormeddelanden via lokala eller globala nätverk.



E-postklient

En e-postklient är en app som låter dig sända och ta emot e-postmeddelanden.

Eponeringar

Ett sätt att utnyttja olika buggar eller sårbarheter som finns i en dator (programvara eller hårdvara). På så sätt kan hackare ta kontroll över datorer eller nätverk.

Falska positiva

Inträffar när en skanning identifierar en fil som ett hot när den i själva verket inte är det.

Filändelse

Den del av ett filnamn, som kommer efter sista punkten, som visar vilken typ av data som finns lagrad på filen.

Många operativsystem använder sig av filändelser, t.ex. Unix, VMS, och MS-DOS. De består oftast av en till tre bokstäver (vissa sorgliga gamla operativsystem har inte stöd för mer än tre). Exempel inkluderar "c" för C-källkod, "ps" för PostScript, "txt" för godtycklig text.

Hämta

För att kopiera data (vanligtvis en hel fil) från en huvudkälla till en fjärrenhet. Termen används ofta för att beskriva processen att kopiera en fil från en tjänst på nätet till sin egen dator. Hämta kan även hänvisa till att kopiera en fil från en nätverksfilserver till en dator på nätverket.

Händelser

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 få slut minnesutrymme.

Hårddisk

Det är en maskin som läser data från, och skriver data till en skiva.

En hårdisk skriver och läser hårddiskar.

En diskettenhet har tillgång till disketter.

Diskar kan antingen vara interna (inuti ett datorchassi) eller externa (inuti en mindre extern låda som ansluts till en dator).



Heuristiskt

En regelbaserad metod för att identifiera nya hot. Den här skanningsmetoden förlitar sig inte på en specifik hotinformationsdatabas. Fördelen med den heuristiska skanningen är att den inte luras av en ny variant av ett befintligt hot. Det kan dock hända att den ibland rapporterar misstänkta koder i vanliga program, genererar de så kallade "falsk positiv".

Honungsfälla

Ett lockbetessystem som konfigureras för att locka hackare för att studera hur de agerar och identifiera vilka metoder de använder för att samla in systeminformation. Företag och koncerner är mer intresserade av att implementera och använda honungsfällor för att förbättra sin allmänna säkerhetsstatus.

Hot

Ett program eller en kod som utan din vetskap laddas upp till din dator mot din vilja. De flesta virus kan även kopiera sig själva. Alla datorvirus är tillverkade av människor. Ett simpelt virus som kan kopiera sig själv om och om igen är relativt lätt att tillverka. Även ett sådant simpelt virus är farligt eftersom det snabbt kommer att använda upp allt ledigt minnesutrymme och orsaka en systemkrasch. Ett ännu farligare typ av virus är ett virus som kan sända sig själv via nätverk och ta sig förbi säkerhetssystem.

Icke-heuristiskt

Den här skanningsmetoden förlitar sig på en specifik hotinformationsdatabas. Fördelen med icke-heuristisk skanning är att den inte låter sig luras av vad som kan se ut som ett hot och genererar inte falska alarm.

IP

Internetprotokoll - Ett routabelt protokoll i TCP/IP som ansvarar för IP-adressering, routing, och fragmenteringen och återmonteringen av IP-paket.

Java-applet

Ett Java-program som är konstruerat för att endast köras på en webbsida. För att använda en applet på en webbsida måste du ange namnet på appleten och storleken (längd och bredd, i pixlar) som appleten kan



använda. När webbsidan öppnas laddar webbläsaren ner appleten från en server och kör den på användarens maskin (klienten). Appletar skiljer sig från appar eftersom de styrs av ett strikt säkerhetsprotokoll.

Till exempel, fastän applets körs på klienten kan de inte läsa eller skriva data till klientens maskin. Dessutom är applets mer begränsade till att endast kunna läsa och skriva data från samma domän de kommer ifrån.

Kaka

I Internet-branschen beskrivs cookies som små filer som innehåller information om individuella datorer, som kan analyseras och användas av annonsörer för att följa vad du gör och dina intressen på nätet. Inom detta område utvecklas cookie-teknologin fortfarande, och målet är att kunna rikta annonser direkt mot vad du sagt att du är intresserad av. För många är det ett tveeggat svärd då det å ena sidan är effektivt och relevant eftersom man bara ser annonser om sådant man är intresserad av. Å andra sidan handlar det faktiskt om att "spåra" och "följa" dina aktiviteter. Förståeligt nog så finns det en debatt om privatliv, och många människor känner sig kränkta av känslan att de behandlas som en EAN-kod (du vet streckkoden på baksidan av förpackningar som skannas i matbutiken). Även om detta sätt att se på saken kan vara extremt, så är det i vissa fall sant.

Keylogger

En keylogger är en app som loggar allt du skriver.

Keyloggers är inte skadliga till sin natur. De kan användas i legitima syften, som att övervaka anställdas eller barns aktivitet. De används dock mer och mer av cyberbrottslingar för skadliga syften (till exempel för att samla in privat information, som inloggningsuppgifter och personnummer).

Kommandorad

I ett kommandorads-gränssnitt skriver användaren kommandon i utrymmet som finns direkt på skärmen genom att använda kommandospråk.

Komprimerade program

En fil i komprimerat format. Många operativsystem och appar innehåller kommandon som gör att du kan komprimera en fil så att den tar upp mindre minne. Till exempel, säg att du har en textfil som innehåller tio



blanksteg på varandra. Detta skulle normalt kräva tio bytes lagringsutrymme.

Dock skulle ett program som komprimerar filer ersätta blankstegen med ett speciellt tecken för blanksteg följt av hur många blanksteg som ersätts. I detta fall kommer de tio stegen endast kräva två bytes utrymme. Detta är bara en komprimeringsmetod - det finns många fler.

Makrovirus

En typ av datorhot som är kodat som ett makro inbäddat i ett dokument. Många appar, som Microsoft Word och Excel, har stöd för kraftfulla makrospråk.

Dessa appar tillåter dig att bädda in ett makro i ett dokument samt låter makrot köras varje gång dokumentet öppnas.

Mask

Ett program som sprider sig själv över ett nätverk och reproducerar sig självt efter hand. Det kan inte fästa sig till andra program.

Minne

Interna lagringsytor på datorn. Med termen minne menas lagring av information i kretsar, och ordet lagring används för minne som finns på band eller diskar. Till varje dator följer det en viss mängd fysiskt minne, vilket brukar kallas för internminne eller RAM-minne.

Onlineförövare

Personer som försöker locka minderåriga eller tonåringar till konversationer i syfte att involvera dem i illegala sexuella aktiviteter. Sociala nätverk är den perfekta platsen där sårbara barn kan sökas upp och lockas att begå sexuella aktiviteter, online eller ansikte mot ansikte.

Onlinemobbning

När kollegor eller främlingar begår oegentliga handlingar mot barn i syfte att fysiskt skada. För att skada emotionellt skickas förövarna elaka meddelanden eller osmickrande foton, för att därmed isolera sina offer från andra eller få dem att känna sig frustrerade.

Ordlisteattack

Lösenordsgissningsattacker som 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



avkrypteringsnycklar för krypterade meddelanden eller dokument. Ordlisteattacker lyckas eftersom många människor tenderar att använda korta lösenord och lösenord med ett ord som är enkla att gissa.

Phishing

Att skicka ett e-postmeddelanden till en användare och utge sig för att vara ett legitimt företag i ett försök att lura användaren att uppge privat information som kan användas för identitetsstöld. E-postmeddelandet skickar användaren till en webbsida där de ombes uppdatera personlig information, som lösenord och kreditkort, personnummer och bankkontonummer, som den legitima organisationen redan har. Webbplatsen är dock falsk och endast uppsatt för att stjäla användarens information.

Photon

Photon är en innovativ, ej störande Bitdefender-teknik, konstruerat för att minimera prestandainverkan för din säkerhetslösning. Genom att övervaka din dators aktivitet i bakgrunden skapar den ett användningsmönster som bidrar till att optimera start- och skanningsprocesser.

Polymorfa Virus

Ett virus som ändrar form med varje fil det smittar. Eftersom det inte har något konsekvent binärt mönster är sådana virus svåra att identifiera.

Port

En dators gränssnitt till vilket du kan ansluta en enhet. Hemdatorer har olika sorters portar. Internt finns flera portar för anslutning av diskenheter, skärmar och tangentbord. Externt finn portar för anslutning av modem, skrivare, möss och andra externa enheter.

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 från användarna genom att låsa deras sårbara system. CryptoLocker, CryptoWall och TeslaWall är några varianter som jagar personliga användarsystem.



Infektionen kan spridas genom att öppna skräppostmeddelanden, hämta e-postbilagor eller installera appar, utan att låta användaren vet vad som händer på deras system. Varje dag utsätts användare och företag för ransomwarehackare.

Rapportera fil

En fil som listar inträffade åtgärder. Bitdefender underhåller en rapportfil som listar den skannade sökvägen, de mappar, antal filer och arkiv som skannats, hur många infekterade och misstänkta filer som hittats.

Råstyrkeattack

Lösenordsgissningsattack använd för att bryta sig in i ett datorsystem genom att ange möjliga lösenordskombinationer, oftast genom att börja med de som är lättast att gissa.

Script

En annan term för makro eller batch-fil, ett script är en lista med kommandon som kan utföras utan användarens medverkan.

Skräppost

Elektronisk skräppost eller skräp nyhetsgruppsinlägg. Generellt känt som oönskade e-postmeddelanden.

Sökväg

Exakt anvisning till en fil på en dator. Dessa anvisningar är vanligtvis beskrivna i ett hierarkiskt katalogsystem uppifrån och nedåt.

Vägen mellan två punkter, exempelvis vägen för kommunikation mellan två datorer.

Spionprogram

All programvara som i hemlighet samlar in användarinformation via användarens Internetuppkoppling utan hans eller hennes vetande, vanligen ur reklamsyfte. Spionprogram är vanligtvis paketerat som en dold komponent i gratisprogram eller delningsprogram som kan laddas ner från Internet; det bör dock noteras att majoriteten av gratisprogrammen och delningsprogrammen inte bär på spionprogram. När det väl installerats så övervakar spionprogrammet användarens aktiviteter på Internet och skickar i bakgrunden denna information till någon annan. Spionprogram kan även samla information om e-postadresser och till och med lösenord och kreditkortsnummer.



Spionprogramms likhet med Trojanska hästar är att användare ovetande installerar produkten när de installerar något annat. Ett vanligt sätt att falla offer för spionprogram är att hämta vissa pir till pir fildelningsprodukter som finns tillgängliga idag.

Förutom frågorna om etik och sekretess stjälar spionprogram från användaren genom att använda datorns minnesresurser och ta upp bandbredd när den sänder tillbaka information till sin hemmabas via användarens Internetanslutning. Eftersom spionprogram använder minnes- och systemresurser kan de program som körs i bakgrunden leda till systemkrasch eller generell systeminstabilitet.

Spökprogram

Ett rootkit är en uppsättning programvaruverktyg som erbjuder administratörsnivååtkomst till ett system. Termen användes från början av operativsystemet UNIX och refererade till ombyggnadsverktyg som gav inkräktare administrativa rättigheter och lät dem dölja sin närvaro för att inte upptäckas av systemadministratörerna.

Den huvudsakliga uppgiften för spökprogram är att gömma processer, filer, inloggningsuppgifter och loggar. De kan även snappa upp information från terminaler, nätverksanslutningar och externa enheter om de lyckas nästla sig in i "rätt" program.

Spökprogram är inte naturligt skadliga. Till exempel gömmer system och även vissa program kritiska filer genom att använda spökprogram. De används dock oftast för att dölja hot eller för att dölja närvaron av en inkräktare i systemet. När de kombineras med hot utgör rootkits ett stort hot till systemets integritet och säkerhet. De kan övervaka trafik, skapa bakdörrar in i system, ändra filter och loggar för att undgå upptäckt.

Startposter

Alla filer som placeras i denna mapp kommer att öppnas när datorn startas. Till exempel, en startskärm, en ljudfil som ska spelas upp när datorn först startar, en påminnelsekalender eller appar kan vara uppstartsobjekt. Vanligen placeras ett alias för filen i mappen istället för den aktuella filen.

Systemfältet

Introducerat med Windows 95, finns systemfältet i Windows aktivitetsfält (vanligtvis längst ner vid klockan) och innehåller miniatyrikoner för enkel



tillgång till systemfunktioner såsom fax, skrivare, modem, volym och mer. Dubbelklicka eller högerklicka en ikon för att visa och komma åt detaljerna och kontrollerna.

TCP/IP

Överföringskontroll/Internetprotokoll - En uppsättning nätverksprotokoll som ofta används på Internet och erbjuder kommunikation över sammankopplade datornätverk med diverse maskinvaruarkitekturer och operativsystem. TCP/IP omfattar standard för hur datorer kommunicerar och konvent för anslutna nätverk och routing-trafik.

Trojansk

Ett destruktivt program som maskerar sig som ett godartat. Till skillnad från skadliga program och maskar kan inte trojaner kopiera sig själva, men de kan vara minst lika destruktiva. Ett av de mest försåtliga typerna av trojaner är ett program som gör anspråk på att rensa datorn från hot, men istället inför hot på datorn.

Termen kommer från en berättelse i Homeros Illiaden där Grekerna ger en enorm trähäst till sina fiender Trojanerna, skenbart en fredsgåva. Men när Trojanerna dragit hästen innanför murarna så smyger Grekiska soldater ut ur hästens mage och öppnar porten till staden så deras kamrater kan välla in och ta över Troja.

Uppdatera

En ny version av programvara eller maskinvara utformad för att ersätta äldre versioner av samma produkt. Dessutom kontrollerar ofta installations-rutinerna för uppdatering, din dator för att vara säker på att en äldre version redan finns installerad på din dator; om inte, kan du installera uppdateringen.

Bitdefender har sin egen uppdateringsmodul som låter dig manuellt kontrollera efter uppdateringar, eller automatiskt låter den uppdatera produkten.

Uppdatering av hotinformation

Det binära mönstret för ett hot, som används av säkerhetslösningen för att hitta och ta bort hotet.

Utforskaren

Kort för webbläsare, en programvaruapp som används för att hitta och visa webbsidor. Populära webbläsare omfattar Microsoft Internet



Explorer, Mozilla Firefox och Google Chrome. Dessa är grafiska webbläsare vilket betyder att de kan visa både grafik och text. Dessutom kan de flesta moderna webbläsare visa multimediaminformation som inkluderar ljud och bild, även om det för vissa format krävs insticksprogram.

Virtual Private Network (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.