GÖR DATORN REN OCH SÄKER

Ta bort alla dolda hot

Dold malware kan orsaka allvarliga problem, men nu kan du enkelt och effektivt ta bort hot som ditt antivirusprogram har missat.

Malware

Malware är en form av skadlig programvara utformad att förstöra, stjäla eller i det fördolda utnyttja datorer, surfplattor och mobiler, nätverk och IT-system. Programmen inkluderar olika typer av virus och trojaner. Malware kan stjäla data, låsa filer, spionera på användare och även ge hackare kontroll över hela datorsystem. Programmen sprids vanligtvis via mejl, filer som hämtas från internet eller genom säkerhetshål i operativsystem och utrustning.

Journalist
Martin Lorentsen

Det finns många olika typer av små men skadliga program som sprids till datorer över hela världen dygnet runt varje dag utan att offren vet om det. Vissa skadliga program installeras tillsammans med till synes legitima program, medan andra hämtas och installeras i hemlighet, till exempel när du råkar klicka på en annons på en webbplats.

Vanligtvis är de enda symptomen på att datorn har infekterats med skadlig kod att det känns som att den arbetar långsammare eller fryser ibland. Det kan dock även bero på många andra saker, till exempel fel på hårddisken eller i minnet. Många offer inser därför inte att de har blivit infekterade förrän det är för sent och deras bankkonto har tömts eller deras datafiler har gått förlorade.

Men det kommer inte att hända dig om du har Malwarebytes installerat på datorn. Med programmet kan du snabbt hitta dold malware som har smugit sig in i datorn och ta bort de skadliga programmen.

Få bort malware från datorn

Hackare har blivit väldigt skickliga på att skapa virus som arbetar i det fördolda, men även väl kamouflerad malware kan upptäckas och raderas med Malwarebytes. Programmet, som du kan hämta på vår webbplats, låter dig genomföra en djupgående genomsökning av både Windows och alla filer på din dator. Efter några minuter meddelar programmet om det har hittat några potentiella hot på datorn.

Om datorn är fri från dold skadlig kod säger programmet att allt är bra och att du inte behöver vidta några ytterligare åtgärder.

Om det däremot upptäcks några hot kommer Malwarebytes först att tala om det för dig med en avisering i det nedre högra hörnet i Windows. Därefter öppnas i programmet en lista med de misstänkta filerna. Från den listan kan du enkelt låta programmet radera de potentiellt skadliga filerna från datorn.

Malwarebytes

Hitta dold malware och virus som finns installerade på datorn och ta bort dem på bara några minuter.

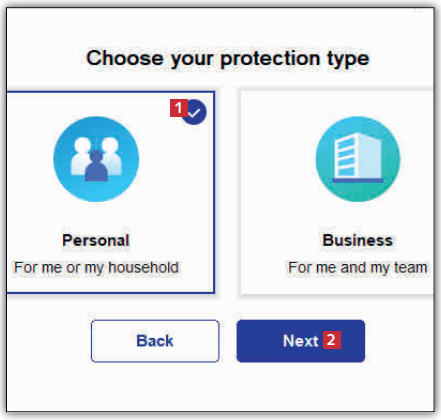
Språk
Engelska

Fungerar med
Windows 10 och 11

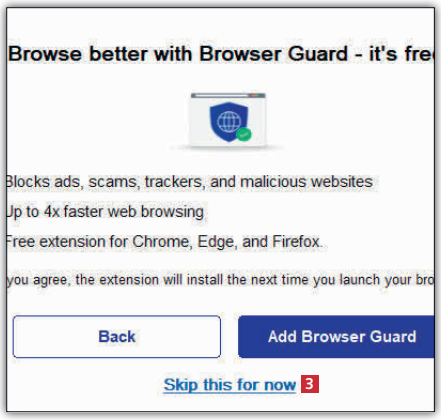
Hämta programmet på vår hemsida:
pctidningen.se/2419

Gör programmet klart för användning

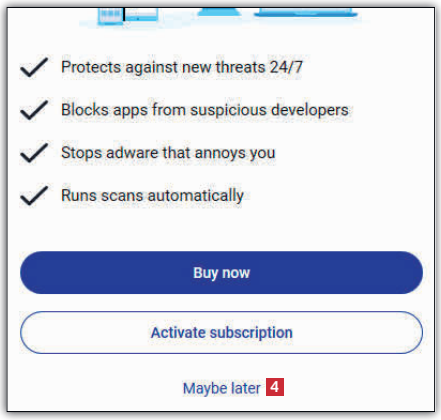
När du har hämtat Malwarebytes från vår webbplats måste du konfigurera programmet att genomsöka datorn efter dolda hot. Här visar vi de viktigaste stegen i installationen.



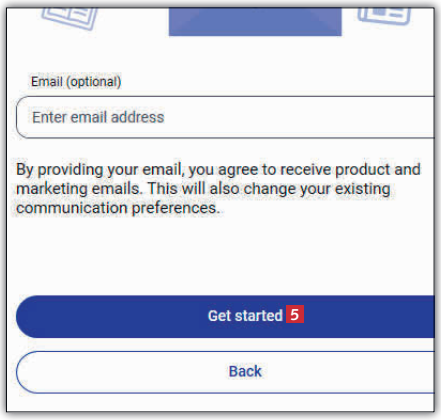
1 Hämta Malwarebytes från pctidningen.se och starta installationen. Du kommer att se rutan här ovan. Välj **Personal** 1 och klicka på **Next** 2.



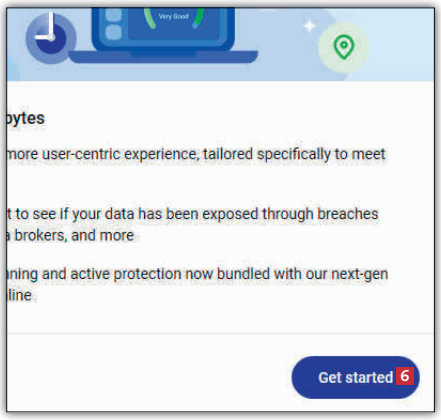
2 Programmet kommer att föreslå att du installerar ett webbläsartillägg. Du behöver inte göra det, så klicka bara på **Skip this for now** 3.



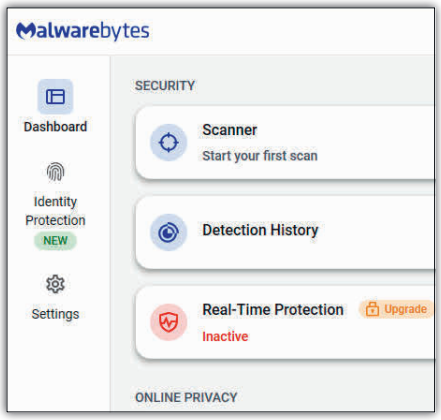
3 Här får du frågan om du vill köpa betalversionen av Malwarebytes. Klicka på **Maybe later** 4.



4 Malwarebytes frågar också om du vill registrera dig för deras nyhetsbrev. Det är inte nödvändigt. Klicka därför bara på **Get started** 5 utan att fylla i något.



5 I nästa fönster klickar du på knappen **Get started** 6. Nu kommer du till programmet.

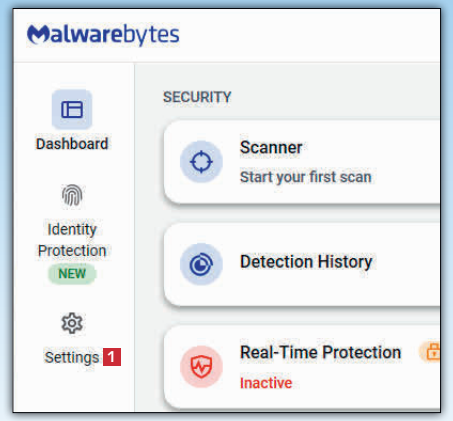


6 Malwarebytes är nu installerat och du är redo att genomsöka din dator efter dold malware.

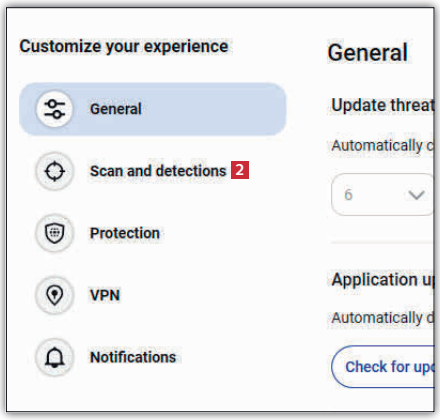
Foto: Nick Graphic/Shutterstock.com

Genomsök datorn efter malware

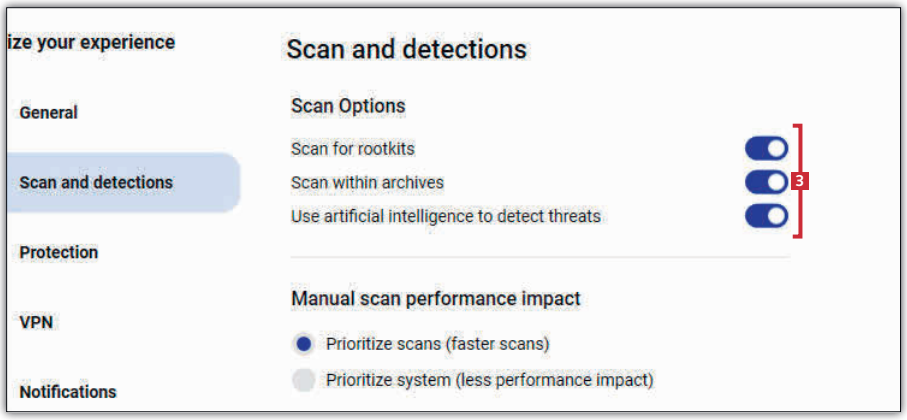
Med Malwarebytes kan du med hjälp av en grundlig genomsökning upptäcka och ta bort skadlig kod som gömmer sig i datorn.



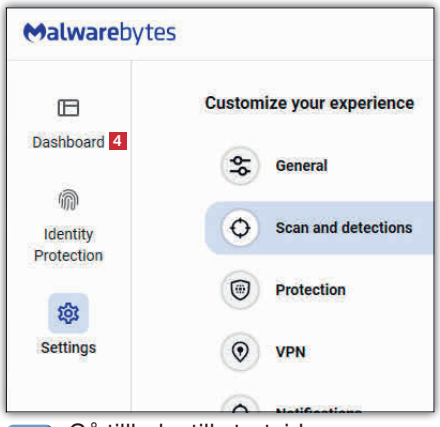
1 När du har hämtat och installerat Malwarebytes på datorn öppnar du programmet. I huvudmenyn väljer du **Settings** 1 för att komma till programmets inställningar.



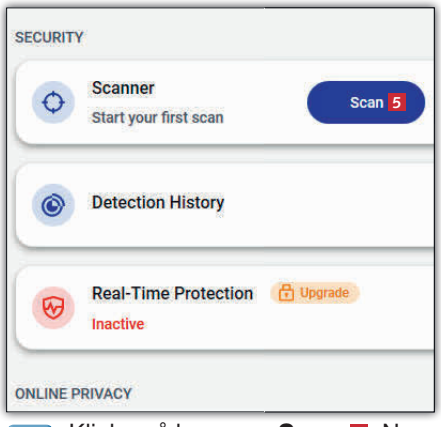
2 Klicka på kategorin som heter **Scan and detections** 2.



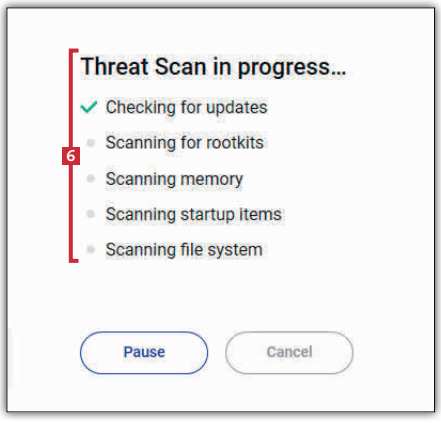
3 Klicka på reglagen 3 vid **Scan for rootkits**, **Scan within archives** och **Use artificial intelligence to detect threats**, så att alla tre reglagen är aktiverade och lyser blått. Programmet kommer nu att kunna undersöka hela datorn grundligt.



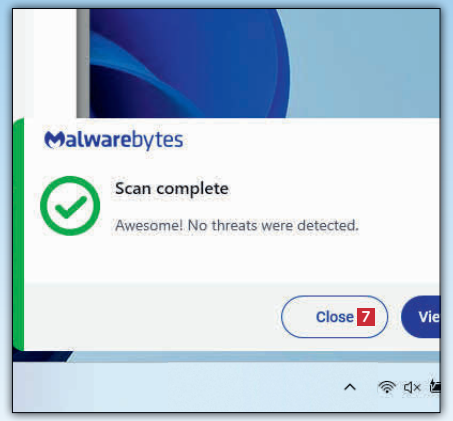
4 Gå tillbaka till startsidan genom att klicka på **Dashboard** 4 i det övre vänstra hörnet.



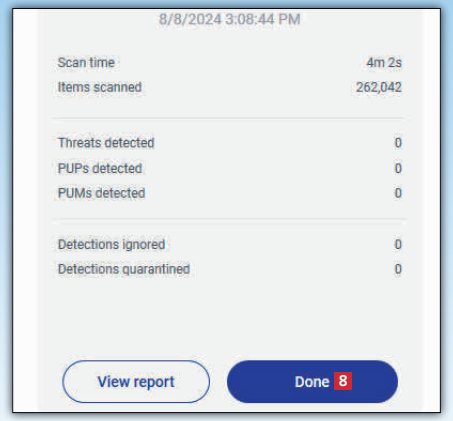
5 Klicka på knappen **Scan** 5. Nu börjar Malwarebytes undersöka datorn. Det kan ta ganska lång tid om det är många filer som ska skannas.



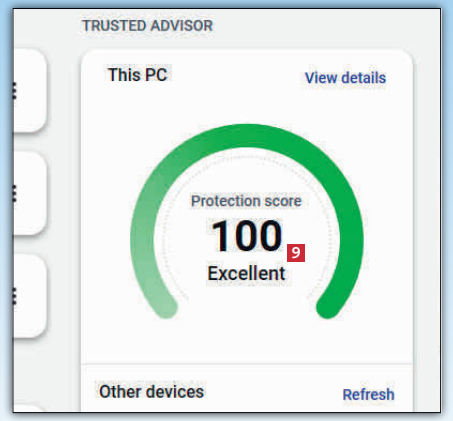
6 Arbetet med skanningen har påbörjats och du kan följa processen här 6.



7 När skanningen är klar och inga faror har hittats visas det här fönstret i det nedre högra hörnet av Windows. Klicka på **Close** 7.



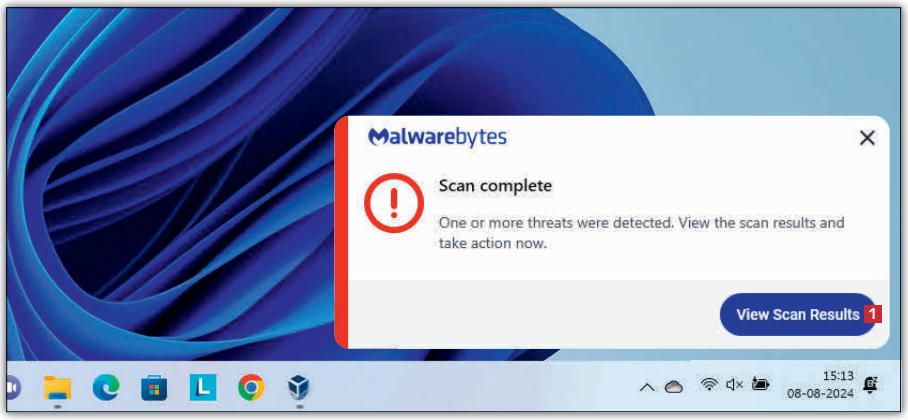
8 Programmet visar en översikt över skanningen och du klickar helt enkelt på knappen **Done** 8.



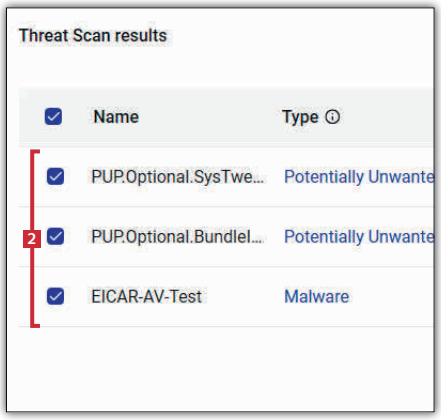
9 Huvudmenyn öppnas och visar att datorn är fri från skadlig programvara 9. Vi rekommenderar att du gör en ny skanning var 14:e dag.

Ta bort hot från datorn

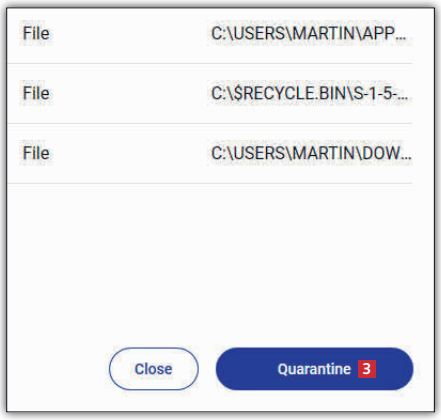
Om några hot upptäcks på datorn under skanningen kommer du att få en tydlig varning. Du kan därefter ta bort de skadliga filerna med några få musklick.



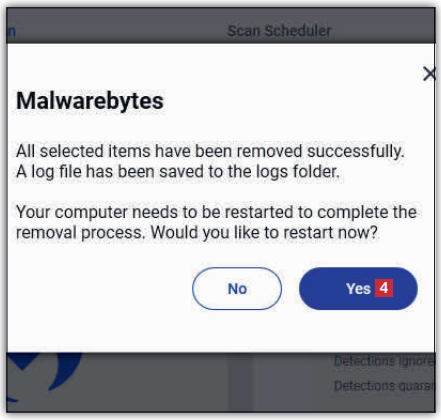
1 Om det upptäcks några potentiella hot under skanningen kommer du att få en varning i det nedre högra hörnet av Windows. Klicka på **View Scan Results** 1 i aviseringen. Du kommer också att få ett meddelande i själva programmet.



2 Nu visas en lista med upptäckta möjliga hot 2. Om du av någon anledning är säker på att en viss fil inte är farlig, avmarkera den. I annat fall lämnar du alla markeringar orörda.



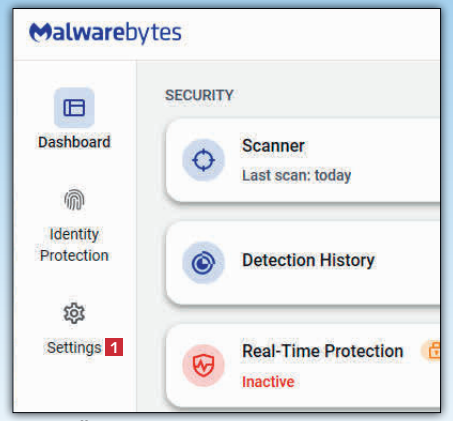
3 Klicka på **Quarantine** 3 nere till höger i fönstret. Alla upptäckta hot kommer då att tas bort.



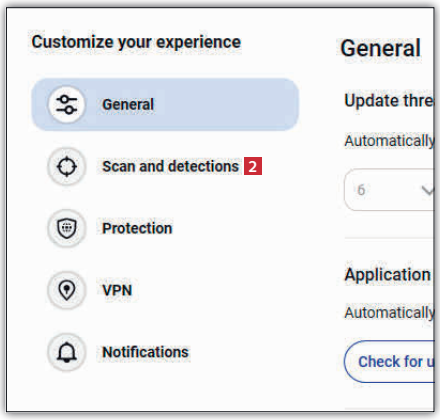
4 När de farliga filerna är borta startar du om datorn. Klicka på **Yes** 4 för att göra det direkt.

Tillåt att en fil körs på datorn

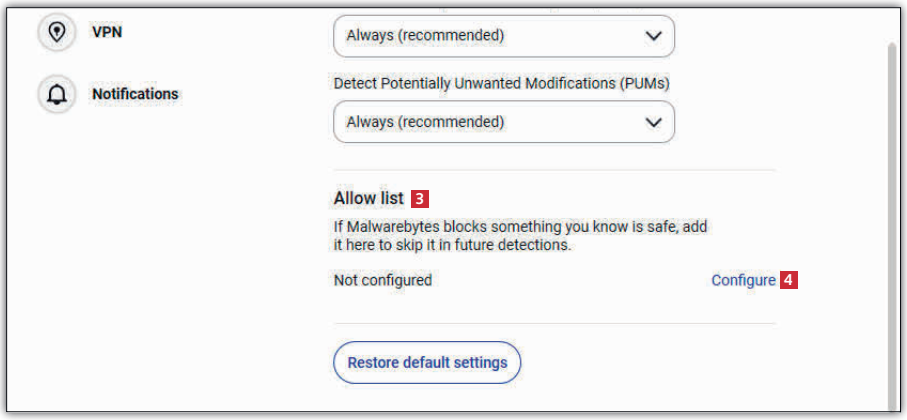
Malwarebytes kan tro att en fil är farlig fast den inte är det. I så fall kommer varje skanning att markera filen som ett hot som ska tas bort, och du riskerar att radera den. Du kan undvika detta genom att lägga till filen i en särskild lista.



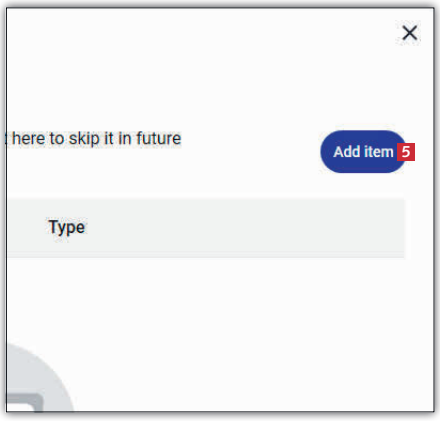
1 Öppna Malwarebytes. I huvudmenyn klickar du på punkten **Settings** 1 till vänster för att öppna Malwarebytes inställningar.



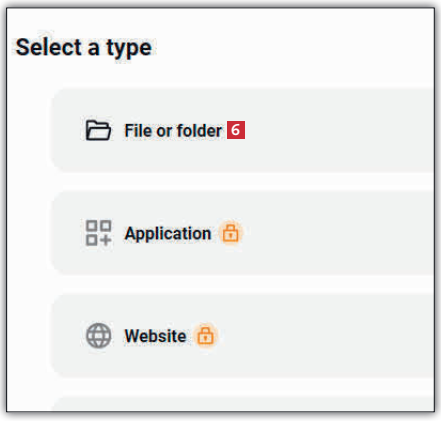
2 I Malwarebytes inställningar klickar du på menyalternativet **Scan and detections** 2.



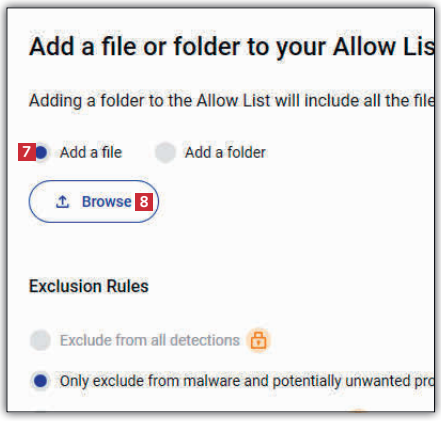
3 Bläddra sedan till botten av fönstret och avsnittet **Allow list** 3. Klicka sedan på **Configure** 4 till höger.



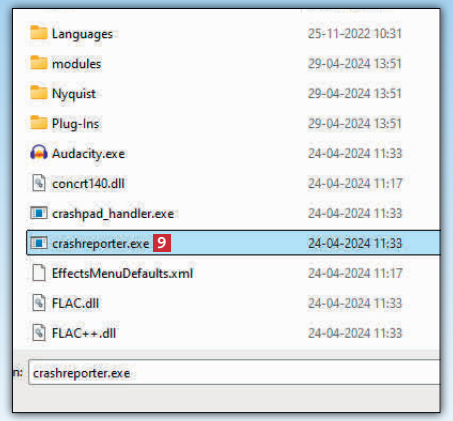
4 Ett nytt fönster öppnas. Klicka på knappen **Add item** 5.



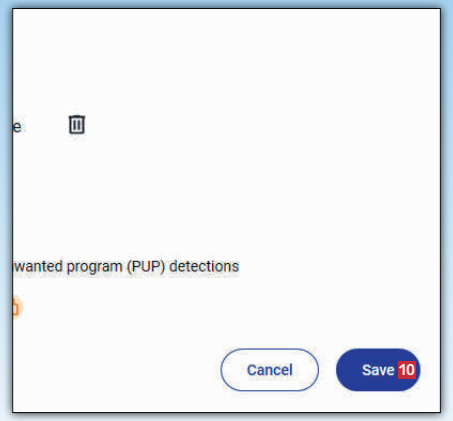
5 Välj **File or folder** 6 i listan med valmöjligheter. De andra alternativen är inte tillgängliga i gratisversionen av Malwarebytes.



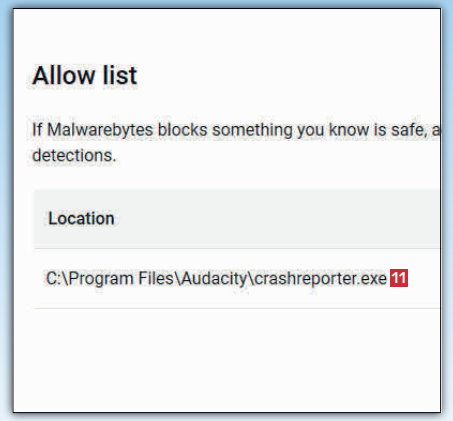
6 Välj **Add a file** 7 och klicka på knappen **Browse** 8. Observera att du även kan välja en hel mapp genom att markera **Add a folder**.



7 Leta upp den fil på datorn som du vill lägga till i undantagslistan och dubbelklicka på den 9.



8 När du har valt filen klickar du på knappen **Save** 10 nere till höger i Malwarebytes.



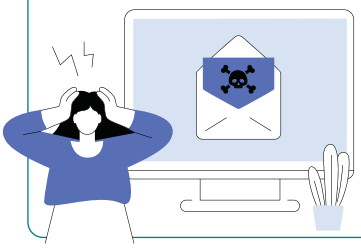
9 Den valda filen har lagts till i undantagslistan 11 och kommer inte att ingå i kommande skanningar du gör med programmet.

Så undviker du att hämta malware

För att hålla din dator fri från malware i framtiden rekommenderar vi att du följer de fyra råden nedan.

Använd ett antivirusprogram

Först och främst behöver du ett bra antivirusprogram för att fånga upp farliga filer som försöker smyga sig in på din dator. Malwarebytes är bra på att hitta faror som redan *finns* på datorn. Du kan ha det tillsammans med ett riktigt antivirusprogram som är bättre på att fånga hot *innan* de hämtas till datorn.



På pctidningen.se/2419 kan du hämta det kraftfulla och kostnadsfria antivirusprogrammet Avast One Essential med en tillhörande guide.

Lita inte på alla webbplatser

Skadlig programvara finns ofta dold på tvivelaktiga webbplatser, så du måste vara extra kritisk till var du hämtar filer. Hämta bara från webbplatser som du litar på, till exempel PC-tidningen.

Det kan vara frestande att hämta en gratisversion av ett dyrt program som Photoshop eller Microsoft Office, men gratisversioner av dyra program kan i slutändan bli en kostsam historia. Nio gånger av tio är det en bluff när dyra program plötsligt finns tillgängliga utan kostnad från en mystisk webbplats. Av samma anledning bör du undvika att installera piratkopierade program eftersom dessa ofta kan vara infekterade med malware.

Se upp för bifogade filer

Om du får ett mejl från en okänd avsändare, eller om mejlet av någon annan anledning verkar misstänkt, finns det alltid anledning att vara uppmärksam. Varningsklockorna bör ringa extra högt om det finns en bifogad fil som du uppmanas att öppna. Hackare älskar att skicka mejl med bifogad malware som kan vara dold i PDF-filer förklädda till räkningar eller andra viktiga dokument som mottagaren inte vill missa.

Om du är det *minsta* osäker ska du inte öppna filen. Om det finns en möjlighet att det handlar om ett legitimt mejl, kontakta avsändaren på annat sätt och fråga. Det gäller även om du helt plötsligt får en konstig faktura.

Klicka inte på popup-reklam

Annonser som plötsligt dyker upp när du är online kan vara en källa till malware. Håll dig borta från dem. Popup-reklam lockar ofta med ofattbart bra erbjudanden eller säger att du har vunnit något dyrt, och att du bara behöver klicka på en knapp för att bekräfta att du vill ha priset.

Om du klickar på knappen riskerar du att hämta malware. Stäng emellertid inte annonsen genom att klicka på krysset i hörnet, eftersom detta också kan leda till att de skadliga filerna hämtas. Stäng bara webbläsaren istället.

Foto: John k studio, Visual Generation/Shutterstock.com