EN REN OG SIKKER PC:

Fjern alle skjulte trusler

Skadevare som er skjult på maskinen kan gjøre mye ugagn, men nå kan du raskt og effektivt fjerne alle trusler – også de antivirusprogrammet har oversett.

Malware

Malware, skadevare på godt norsk, er som navnet antyder programvare som er utviklet for å ødelegge, stjele data eller utnytte enheter som pc-er, nettbrett og mobiltelefoner, nettverk og andre IT-systemer. Det omfatter forskjellige virus og trojanske hester. Skadevaren kan stjele data, kryptere filer, overvåke brukere og gi angripere kontroll over systemer. Skadevare spres via e-post, filer fra nettet eller via sårbarheter i utstyr og operativsystemer.

Journalist
Martin Lorentsen

Det finnes mange former for små og skadelige programmer som hver dag spres til datamaskiner over hele verden, uten at ofrene aner uråd. Noen former for skadevare blir installert sammen med tilsynelatende legitime og ufarlige programmer, mens andre lastes ned til maskinen i det skjulte, for eksempel fordi du ved et uhell klikker på en annonse på en nettside.

Som regel er de eneste symptomene på en infeksjon at maskinen blir tregere eller fryser i ny og ne. Slike hendelser kan imidlertid også skyldes en rekke andre forhold, som feil på harddisken eller i det fysiske minnet, altså i ram-modulene. Derfor oppdager mange ofre virusinfeksjonen først når det er for sent og bankkontoen er tømt, eller når umistelige filer har gått tapt.

Det skjer ikke hvis du har installert Malwarebytes på maskinen. Med dette programmet kan du nemlig raskt og enkelt finne den skjulte skadevaren som har tatt seg inn på maskinen, og fjerne problemet.

Enkel fjerning av skadevare

Hackerne har blitt gode til å lage virus som opererer i det skjulte, men Malwarebytes finner og eliminerer selv det best kamuflerte viruset. Med dette programmet, som du kan laste ned gratis fra nettsiden vår, kan du sette i gang en dyp skanning av både selve operativsystemet og av alle de øvrige filene på maskinen. Etter et par minutter gir programmet klar og tydelig beskjed hvis det har oppdaget mulige trusler.

Er derimot maskinen fri for skjult skadevare, får du vite at alt er i sin skjønneste orden og at du ikke behøver å foreta deg noe mer. Hvis det oppdages trusler, viser Malwarebytes først et varsel i nederste høyre hjørne på skrivebordet. I selve programmet åpnes deretter en liste der de mistenkelige filene beskrives i detalj. Fra denne listen er det lett å få programmet til å slette de potensielt skadelige filene én gang for alle.

Malwarebytes

Finn all skjult skadevare og virus som måtte finnes på maskinen, og fjern alt på få minutter.

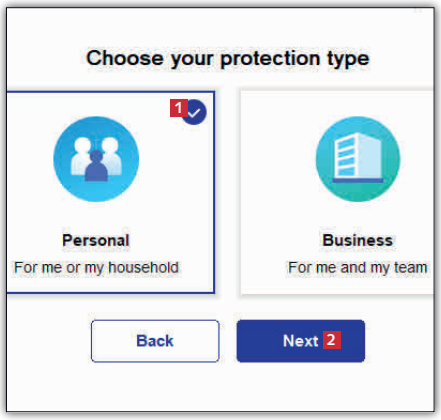
Språk
Engelsk

Virker med
Windows 10 og 11

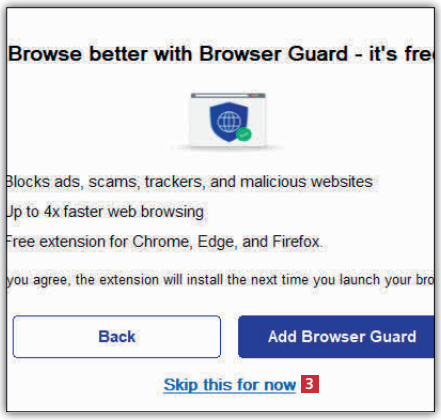
Programmet laster du ned fra:
komputer.no/2419

Klargjør programmet for bruk

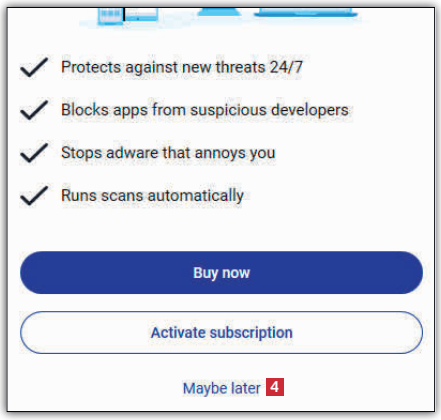
Når du har lastet ned Malwarebytes fra nettsiden vår, må du sette opp programmet slik at det kan skanne maskinen for skjulte trusler. Her viser vi de viktigste trinnene i installeringen.



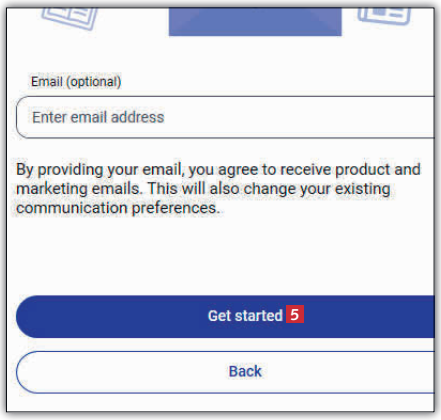
1 Først laster du ned Malwarebytes fra komputer.no og starter installeringen av programmet. Underveis ser du vinduet over. Velg **Personal** 1, og klikk på **Next** 2.



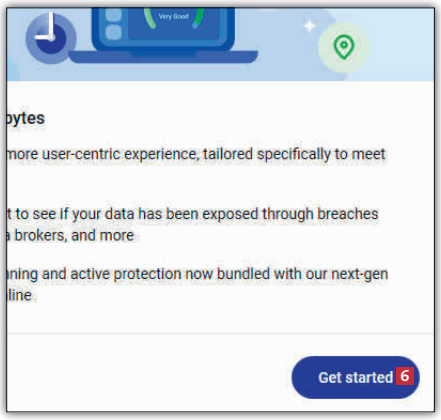
2 Programmet foreslår å installere en nettleserutvidelse. Det er ikke nødvendig, og du kan trygt klikke på **Skip this for now** 3.



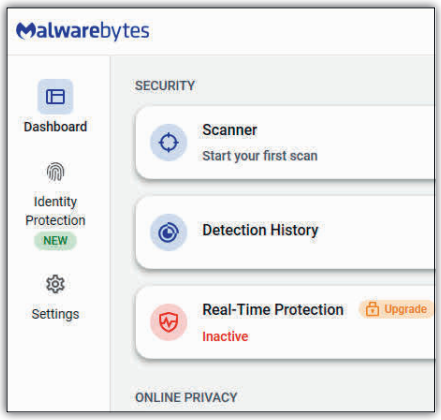
3 Ved dette punktet i installeringen blir du spurt om du vil kjøpe betalingsversjonen av Malwarebytes. Klikk på **Maybe later** 4.



4 Malwarebytes spør også om du vil abonnere på produsentens nyhetsbrev. Det behøver du heller ikke. Bare klikk på **Get started** 5 uten å fylle ut noe.



5 I neste vindu klikker du på knappen **Get started** 6 igjen. Dermed tas du videre til programmet.

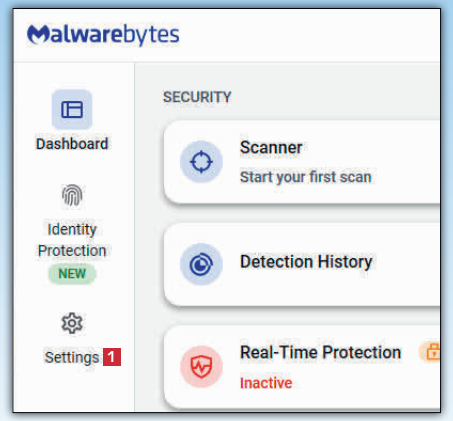


6 Malwarebytes er installert, og du er klar til å gjennomsøke maskinen på jakt etter skjult skadevare.

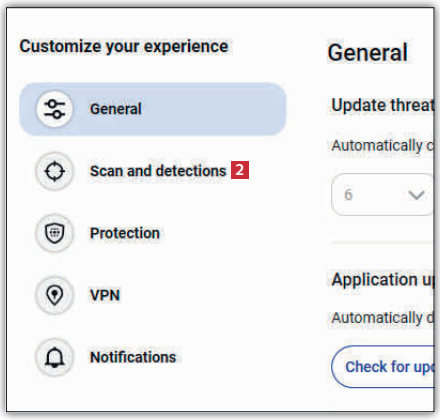
Foto: Nick Graphic/Shutterstock.com

Skann maskinen for skadevare

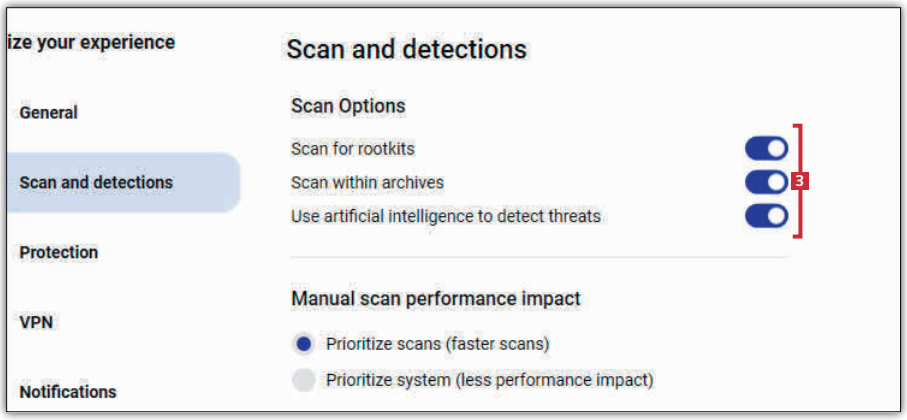
Med Malwarebytes er det lett å skanne operativsystemet for på den måten oppdage og fjerne skadevare som ligger skjult på maskinen.



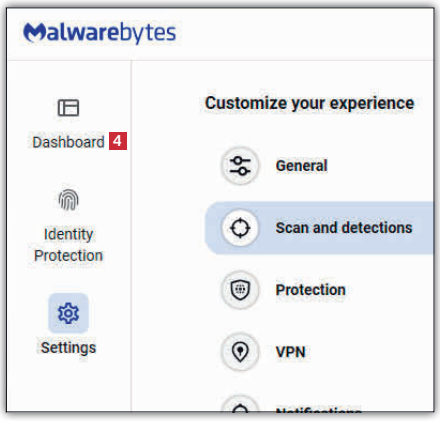
1 Når du har lastet ned og installert Malwarebytes, må du først åpne programmet. I hovedmenyen velger du **Settings** 1 for å komme til programinnstillingene.



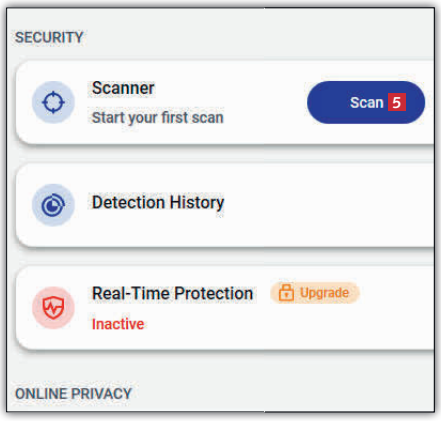
2 Velg **Scan and detections** 2.



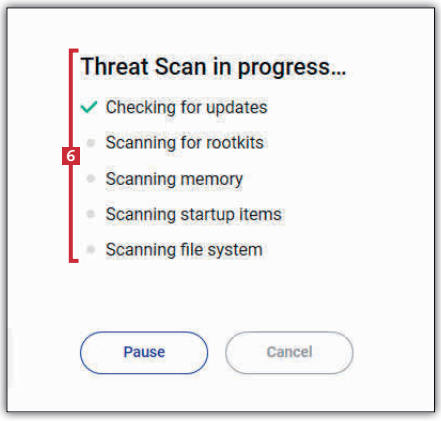
3 Klikk på skyveknappene 3 ved **Scan for rootkits**, **Scan within archives** og **Use artificial intelligence to detect threats**, slik at alle de tre knappene er blå og dermed aktivert. Deretter foretar programmet en grundig gjennomgang av hele maskinen.



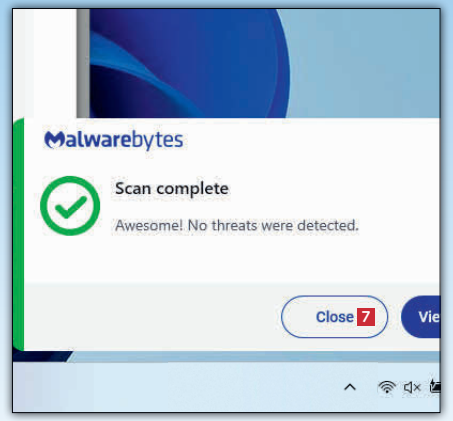
4 Gå tilbake til startsiden ved å klikke på **Dashboard** 4 i øverste venstre hjørne av vinduet.



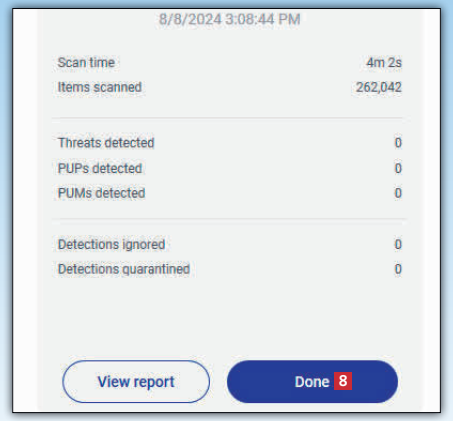
5 Klikk på knappen **Scan** 5, slik at Malwarebytes begynner å skanne pc-en. Det kan ta litt tid hvis du har mange filer som skal skannes.



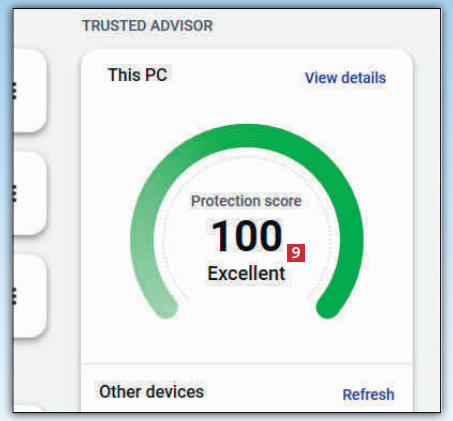
6 Skanningen er i gang, og du kan følge prosessen her 6.



7 Når skanningen er fullført uten at det er oppdaget noen trusler, ser du dette vinduet nederst til høyre på skrivebordet. Klikk på **Close** 7.



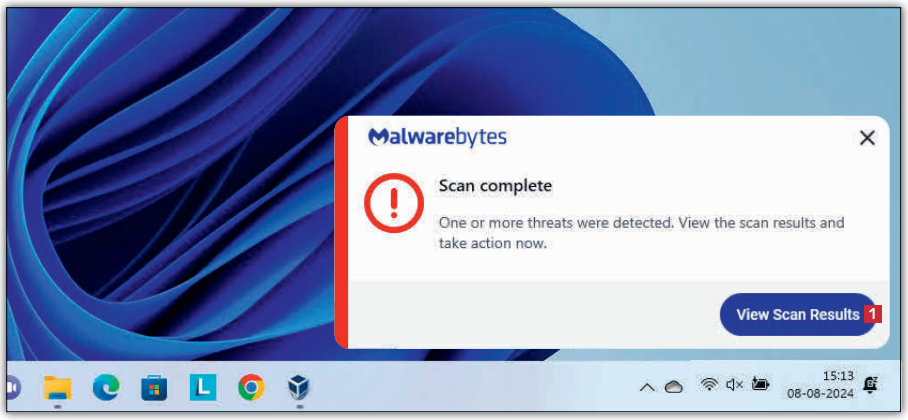
8 I programmet ser du en oversikt over resultatet av skanningen. Her er det bare å klikke på **Done** 8.



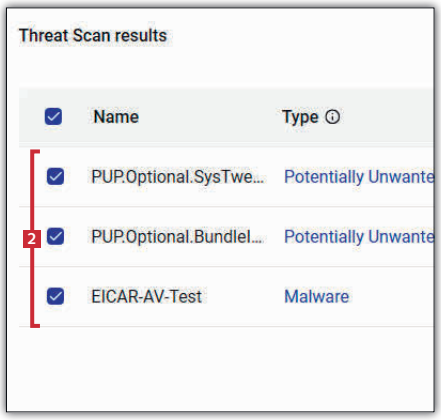
9 Hovedmenyen i Malwarebytes åpnes og viser at maskinen er fri for skadevare 9. Vi anbefaler at du kjører en skanning med programmet en gang hver 14. dag.

Fjern trusler fra maskinen

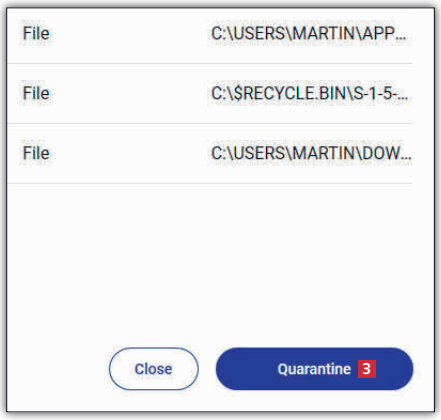
Meldingen er ikke til å misforstå hvis programmet oppdager trusler under skanningen. Deretter kan du fjerne de skadelige filene med et par museklikk.



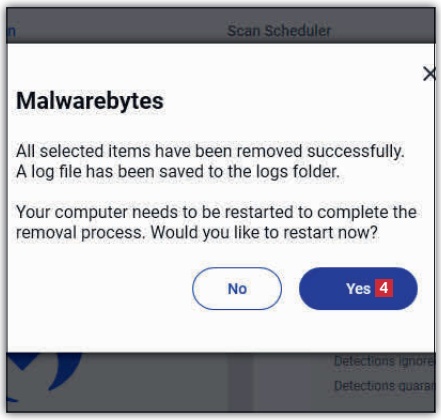
1 Hvis det oppdages mulige trusler i løpet av skanningen, ser du en advarsel nederst til høyre på skrivebordet. Klikk på **View Scan Results** 1 i sprett-opp-vinduet. Du får også beskjed inne i selve programmet.



2 Deretter vises en liste med de mulige truslene 2. Hvis du av en eller annen grunn er sikker på at en bestemt fil *ikke* er farlig, fjerner du haken ved den. Ellers lar du alle haker stå.



3 Klikk på knappen **Quarantine** 3 nederst til høyre i vinduet. Dermed fjernes alle trusler.

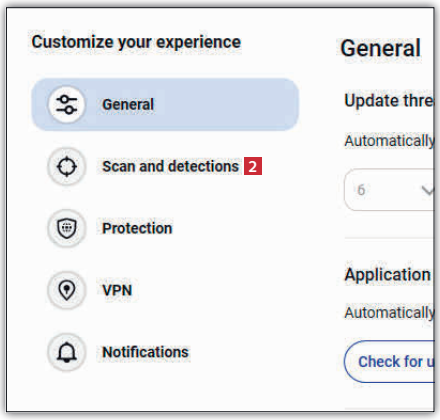


4 Når de farlige filene er fjernet, må maskinen startes på nytt. Klikk på **Yes** 4 for å gjøre det med samme.

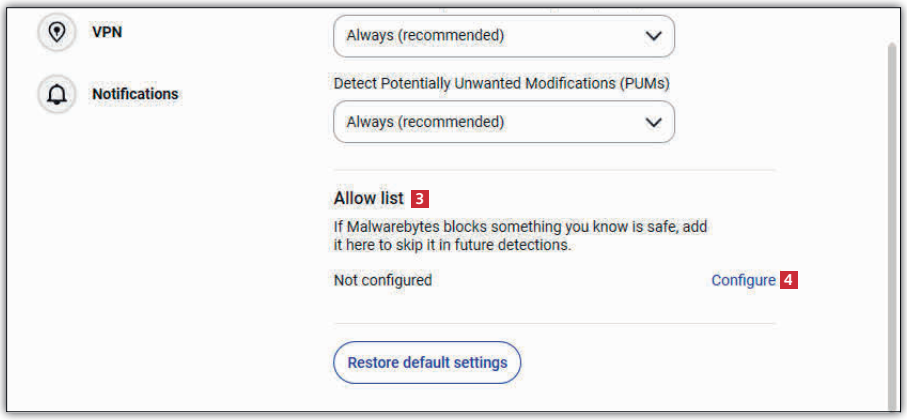
Sett opp unntak for enkeltfiler

Det hender at Malwarebytes tror at en fil er farlig, selv om den ikke er det. Da markeres filen som en trussel som kan fjernes under hver skanning, og du risikerer å slette den. Det kan du unngå ved å legge til filen i en unntaksliste.

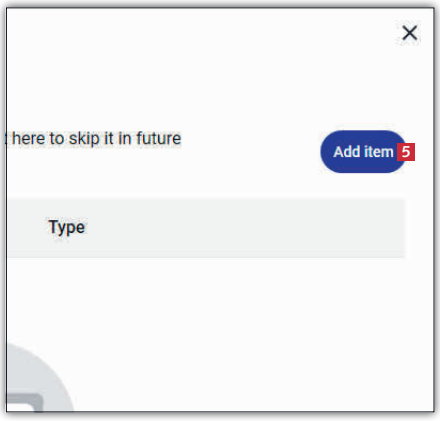
1 Åpne Malwarebytes. I hovedmenyen klikker du på **Settings** 1 til venstre for å åpne innstillingene.



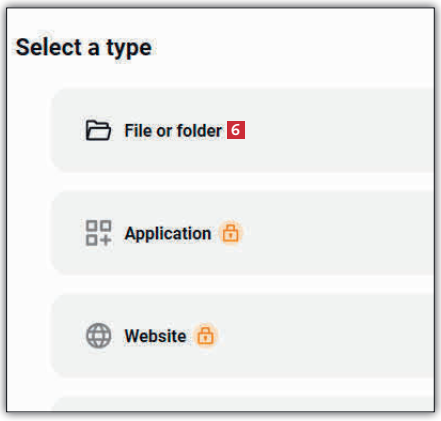
2 I innstillingene for Malwarebytes klikker du på **Scan and detections** 2.



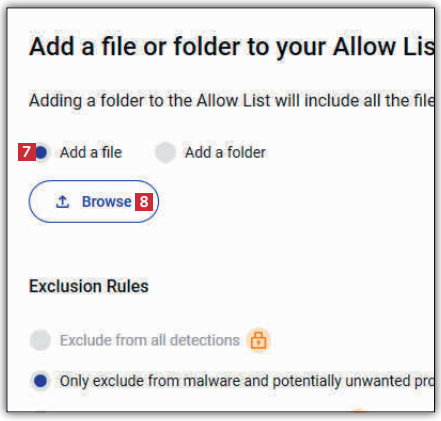
3 Bruk musehjulet til å bla helt ned i vinduet til feltet **Allow list** 3. Deretter klikker du på **Configure** 4 til høyre.



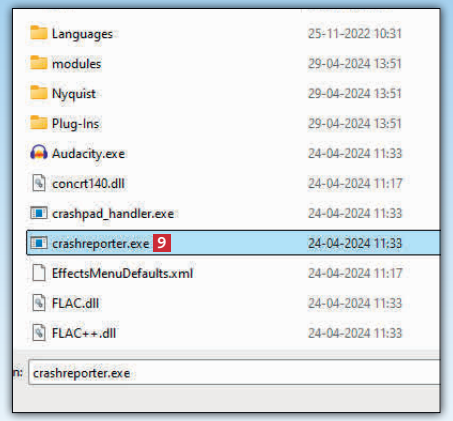
4 Et nytt vindu åpnes. Klikk på knappen **Add item** 5.



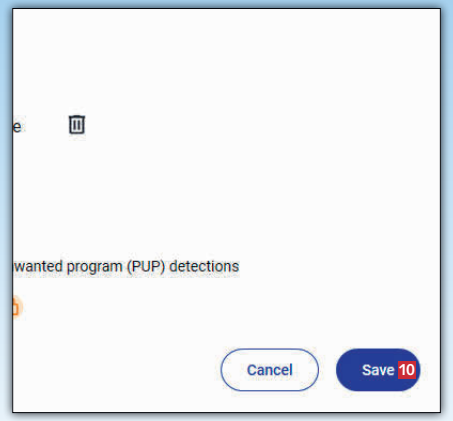
5 Velg **File or folder** 6 fra listen med valgmuligheter. De øvrige alternativene kan ikke velges i gratisversjonen av Malwarebytes.



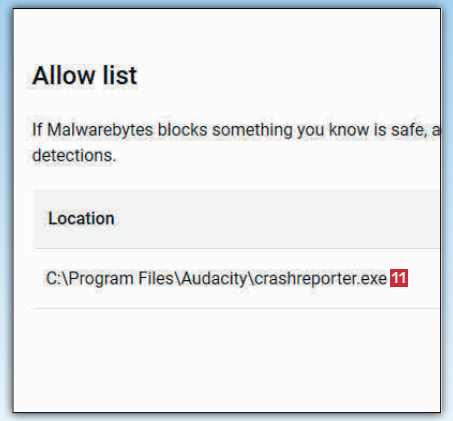
6 Velg **Add a file** 7, og klikk på **Browse** 8. Du kan også velge en hel mappe ved å klikke i feltet ved **Add a folder**.



7 Finn den filen på maskinen du vil legge til i listen over unntak, og dobbeltklikk på den 9.



8 Når du har valgt filen, klikker du på **Save** 10 nederst til høyre i Malwarebytes-vinduet.



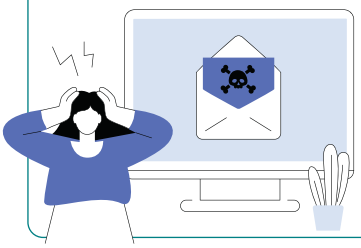
9 Den valgte filen er lagt til i unntakslisten 11 og vil ikke inngå i de fremtidige skanningene du gjør med programmet.

Slik unngår du å laste ned skadevare

For å holde maskinen fri for skadevare i tiden fremover, anbefaler vi at du følger de fire tipsene under.

Bruk et antivirusprogram

Du må ha et godt antivirusprogram, slik at du kan fange opp de farlige filene som prøver å ta seg inn på maskinen. Malwarebytes er effektivt til å finne skjulte trusler som allerede ligger på maskinen, og du kan godt ha det installert sammen med et vanlig antivirusprogram, som er bedre til å fange opp farlige filer *før* de lastes ned.



På komputer.no/2419 kan du laste ned det gratis antivirusprogrammet Avast One Essential med en tilhørende veiledning.

Ikke alle hjemmesider er til å stole på

Skadevare ligger ofte skjult på tvilsomme hjemmesider, og derfor må du være ekstra kritisk med hvilke sider du laster ned filer fra. Last bare ned fra nettsider du stoler på, for eksempel siden til Komputer for alle.

Det kan kanskje være fristende å laste ned en gratisversjon av et ellers dyrt program som Photoshop eller Microsoft Office, men "gratisversjoner" av dyre programmer kan bli en kostbar fornøyelse. Ni av ti ganger er det snakk om svindel når dyre programmer plutselig kan lastes ned fra en obskur hjemmeside. Av samme grunn bør du unngå å installere piratkopierte programmer, som ofte er infisert med skadevare.

Forsiktig med vedlagte filer

Du bør alltid være på vakt hvis du får e-post fra en ukjent avsender, eller hvis meldingen av en annen grunn virker mistenkelig. Alarmlampene bør lyse iltert hvis meldingen også inneholder en vedlagt fil som du blir bedt om å åpne. Hackere pleier nemlig å sende e-post med vedlagt skadevare som kan ligge skjult i for eksempel pdf-filer, kamuflert som regninger eller andre viktige dokumenter som mottakeren nødig vil gå glipp av.

Er du i tvil, skal du *ikke* åpne filen. Er det en mulighet for at det faktisk er en legitim e-post, kontakter du avsenderen på annet vis og spør. Det samme gjelder hvis du får en uventet faktura eller lignende fra et firma.

Klikk aldri på sprett-opp-annonser

Annonser som plutselig åpnes mens du er på nettet, kan være en kilde til skadelige filer. Ikke klikk på dem. Sprett-opp-annonser lokker ofte med gode tilbud eller påstår at du har vunnet penger, og at du bare må klikke på en knapp for å bekrefte at du vil motta premien.

Klikker du på knappen, risikerer du å laste ned skadevare. Du må heller ikke klikke på lukkekrysset i hjørnet av annonsen. Det kan nemlig også føre til at det lastes ned skadelige filer. I stedet lukker du ganske enkelt hele nettleseren.

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