EN ENDA SIKRERE PC:

Beskyttelse mot endringer

Programmet S.O.S Security Suite er en effektiv sikring mot at andre enn deg selv kan foreta større endringer på maskinen og gjøre den usikker.

Register-databasen

Registerdatabasen, eller bare "registeret", i Windows er en slags digital katalog som holder orden på de viktigste innstillingene og informasjonen om Windows og programmene du installerer. Tenk på det som en godt organisert notisbok, der Windows lagrer informasjon om hvordan pc-en skal fungere, om preferansene dine og om innstillingene som får alt til å virke optimalt.

Journalist
Niklas Ernst

En av de største farene når du setter deg ved datamaskinen, er at hackere og andre døgenikter gjør endringer i det skjulte på pc-en. De kan eksempelvis starte programmer som registrerer tastetrykkene dine automatisk og sender dem tilbake til hackerne. På den måten kan de få tak i passordene dine. Eller de kan installere små programmer som filmer deg via nettkameraet, eller som automatisk kopierer alle filene dine og sender dem til sin egen datamaskin. Derfor gjelder det å holde ganske streng kontroll med hvilke programmer som skal få lov til å kjøre. Slik kontroll får du med programmet S.O.S Security Suite, som blant annet inneholder funksjonen Execute Prevent. Tanken bak den er å hindre at skadelige filer i det hele tatt får sjansen til å kjøre.

Execute Prevent legger til spesielle begrensninger direkte i Windows-registeret, og disse begrensningene hindrer at bestemte filtyper kan kjøres i utvalgte mapper og eventuelt i undermapper. Det kan være kjørbare filer som .exe, eller det kan være skript som .bat eller .vb, og til og med snarveier (.lnk). Altså nettopp den slags filer som hackere gjerne benytter for å infisere og skaffe seg tilgang til maskinen din.

Fordelen med Execute Prevent er at det gir en ekstra beskyttelse, også mot trusler som ikke fanges opp av antivirusprogrammet. Hvis et virus skulle havne i en av de blokkerte mappene, vil det ganske enkelt ikke kunne kjøre og dermed vil det heller ikke gjøre skade. Infeksjonen vil med andre ord være isolert og ute av stand til å gjøre skade, selv om viruset skulle ha kommet seg inn på maskinen.

S.O.S Security Suite

Sett en effektiv stopper for at andre kan gjøre endringer i nettleseren eller på maskinen.

Språk
Engelsk

Virker med
Windows 10 og 11

Programmet laster du ned fra:
komputer.no/2419

Bli kjent med programmet

Her får du en kort introduksjon til programmet S.O.S Security Suite og noen av de nyttige verktøyene det inneholder.

Dashboard
På Dashboard-fanen får du raskt oversikt over hele maskinen. Du ser blant annet prosessoren og om Windows Defender er aktivert.

Execute Prevent
Her kan du angi at bestemte filtyper ikke skal kunne startes fra visse mapper. Dermed gir du maskinen ekstra beskyttelse.

System Immunization
Disse innstillingene definerer hvilke endringer som skal kunne gjøres på maskinen.

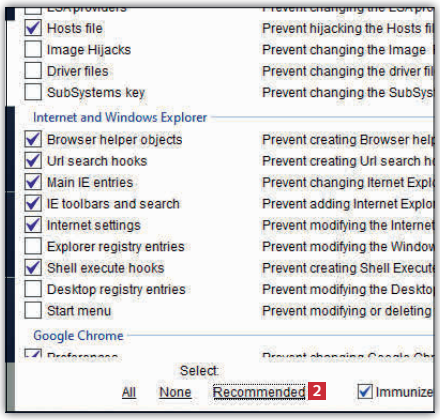
Aktiveringer
Til høyre ser du raskt om funksjonene System Immunization og Execute Prevent er aktivert.

Foto: fridaydsgn/Shutterstock.com

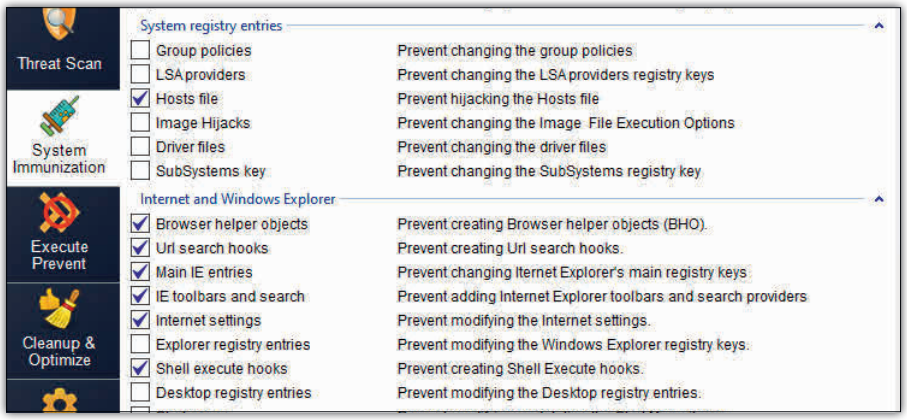
Unngå at andre gjør endringer på maskinen

Det første skrittet når du vil sørge for at det ikke kan gjøres endringer på maskinen, er å gå til fanen System Immunization. Der er det særlig nettleseren som beskyttes. Du kan alltid tilbakestille innstillingene hvis du opplever problemer.

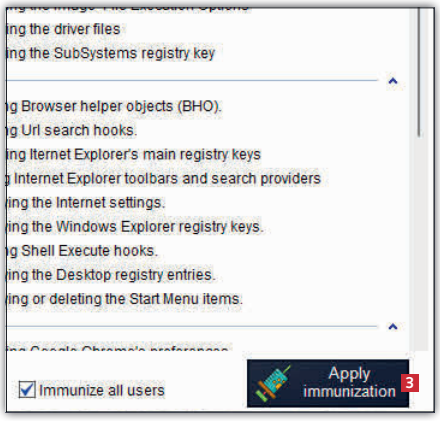
1 Last ned og installer S.O.S Security Suite fra nettsiden vår. I programmets hovedmeny klikker du på **System Immunization** 1.



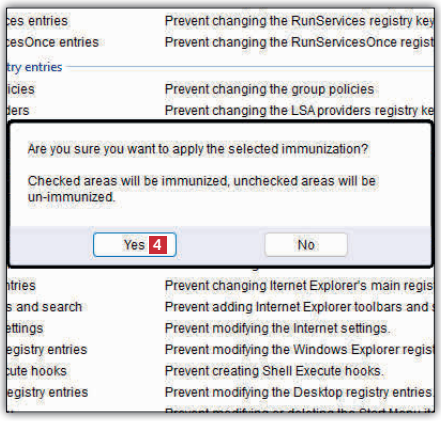
2 I oversikten som vises, klikker du på **Recommended** 2 nederst i vinduet.



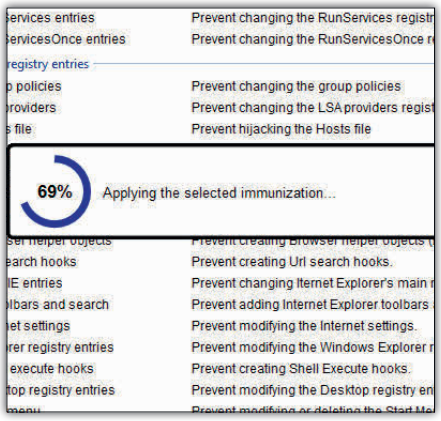
3 Deretter markeres en rekke forskjellige innstillinger. Det er programmets egne anbefalinger, og de er ganske fornuftige, så la dem være som de er.



4 Klikk på **Apply immunization** 3.



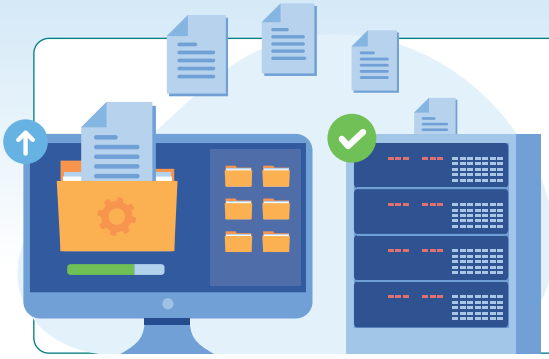
5 I vinduet som åpnes, klikker du på **Yes** 4 for å lagre de valgte innstillingene.



6 Dermed lagres innstillingene. Det tar ikke mer enn et par sekunder. Deretter er maskinen beskyttet og klar til bruk.

Disse truslene blokkeres

Med de anbefalte innstillingene i System Immunization treffer programmet en rekke kloke valg for sikkerheten på maskinen. Her ser du en nærmere beskrivelse av hva som foregår.

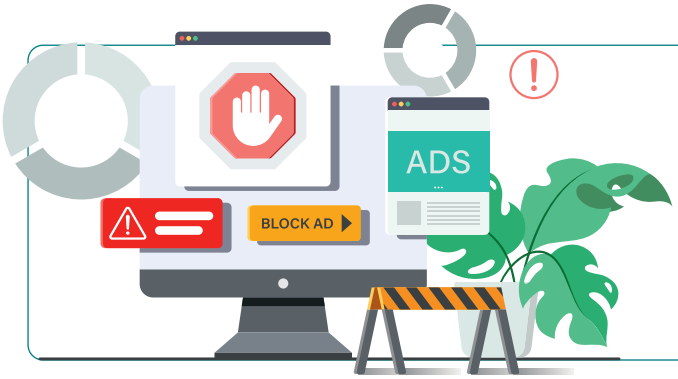


Unngå endringer i vertsfilen

En ”host-file”, altså vertsfil på norsk, er en liten tekstfil Windows benytter til å åpne de riktige nettsidene når du bruker nettleseren. Vertsfilen kobler sammen domenenavn og IP-adresser, slik at du for eksempel kommer til Googles søkemotor når du skriver google.com i adresselinjen. Endres vertsfilen, kan du havnet et helt annet sted, for eksempel på en falsk nettside. Med S.O.S Security Suite unngår du at vertsfilene kan endres.

Stopper nettleserutvidelser

En metode hackerne ofte benytter seg av for å få tilgang til andres maskiner, er å bruke nettleserutvidelser. Det er små programmer som gir nettleseren en ekstra funksjon, men som noen ganger også inneholder ondsinnet kode. S.O.S Security Suite gjør at de ikke kan installeres i bakgrunnen. Vil du selv vil installere en utvidelse, må du deaktivere funksjonen midlertidig ved at du fjerner haken ved Extensions.



Blokker automatiske oppstartsprogrammer

I Windows kan du velge å la visse programmer starte sammen med maskinen, men du risikerer også at du uforvarende får installert skadelige programmer som starter sammen med operativsystemet og kjører i bakgrunnen. Med denne innstillingen unngår du at nye programmer kan starte sammen med Windows. Funksjonen aktiveres når du setter hake ved **Autorun entries**, og er ikke en del av de anbefalte innstillingene.

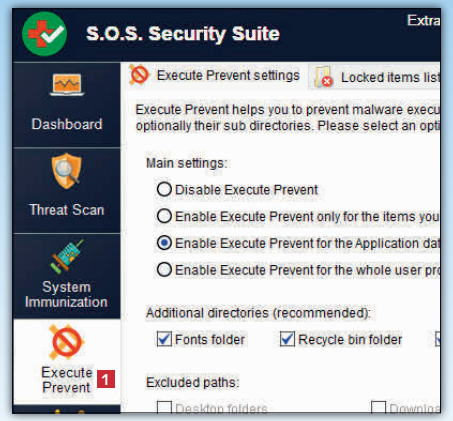
Lås sikkerhetsinnstillingene

Hvis vil unngå at uvedkommende endrer sikkerhetsinnstillingene i nettleseren, enten du bruker Chrome, Edge eller Firefox, kan du velge å låse disse innstillingene i S.O.S Security Suite. Alt som skal til er at du setter hake ved feltet Secure preferences, som er en del av de anbefalte innstillingene.

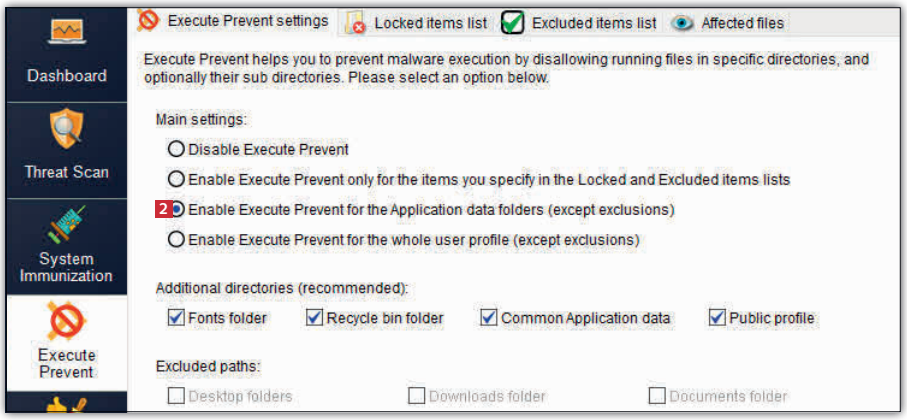
Foto: yelosmiley, Visual Generation, NiceDayKorn, Overearth/Shutterstock.com

Stopp farlige programmer

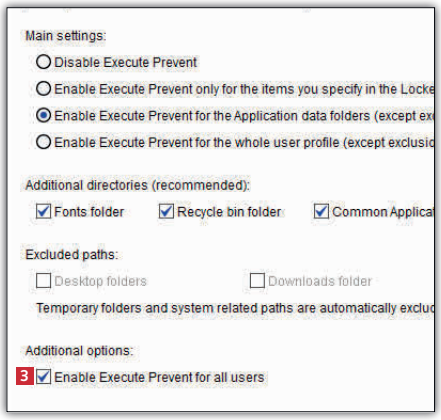
Execute Prevent-funksjonen gir en tilleggsbeskyttelse mot virus. Det gjør den ved å legge inn spesielle begrensninger direkte i Windows-registeret og hindrer på den måten filer i å kjøres fra bestemte mapper og undermapper.



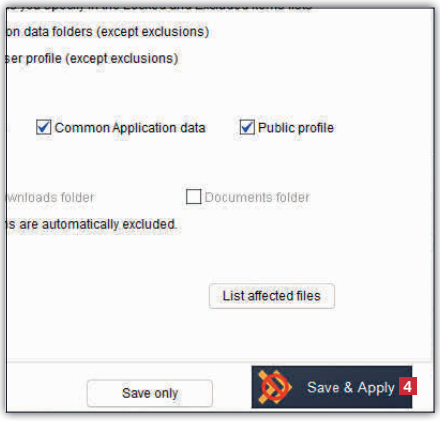
1 Klikk på feltet **Execute Prevent** 1 i hovedvinduet.



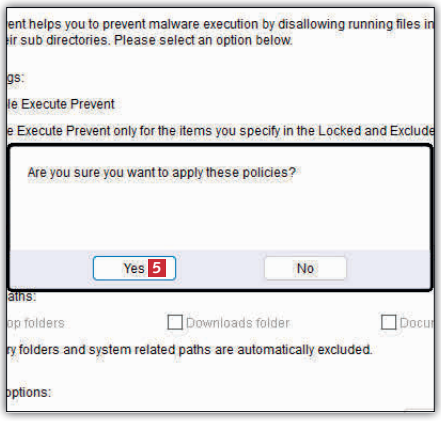
2 Vi anbefaler at du velger innstillingen **Enable Execute Prevent for the Application data folders (except exclusions)** 2. På den måten sørger du for at det settes begrensninger for programmer i Windows-registeret, men at du også kan velge at de programmene du stoler på, ikke berøres av begrensningene.



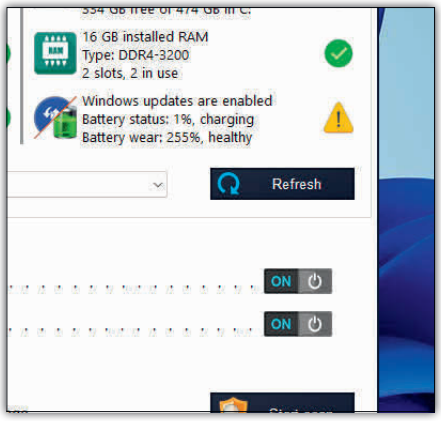
3 Pass også på at det er satt hake ved **Enable Execute Prevent for all users** 3. Da gjelder innstillingen for alle brukere.



4 Til slutt klikker du på **Save & Apply** 4 lengst ned i vinduet.



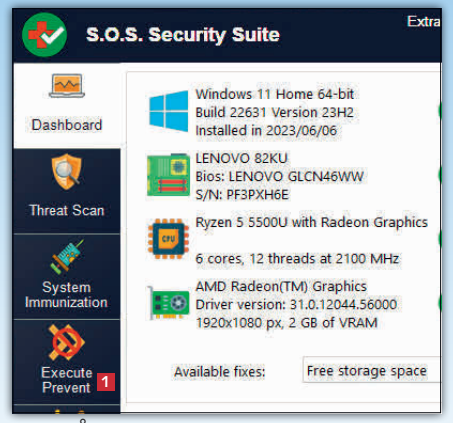
5 Klikk på **Yes** 5 i vinduet som åpnes.



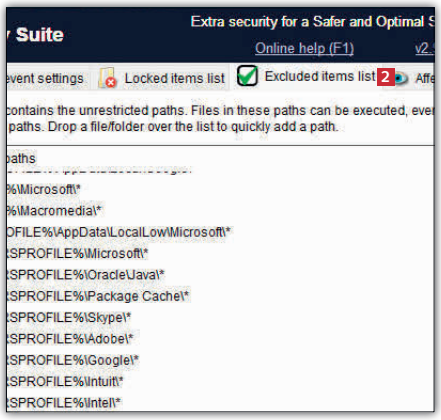
6 Nå er innstillingen aktivert, og maskinen er beskyttet av programmet S.O.S Security Suite.

Lag unntak for programmer du stoler på

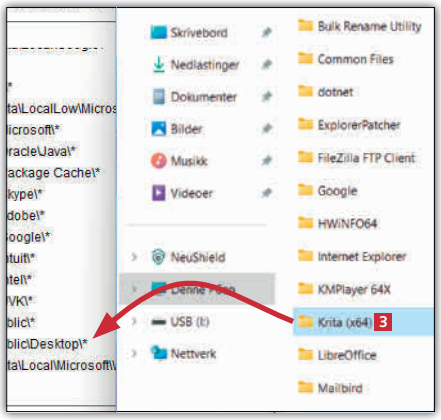
Nå har du satt kraftige begrensninger for å hindre både programmer og prosesser i å endre noe i registeret. Får du problemer med programmer du stoler på, kan du opprette unntak for disse.



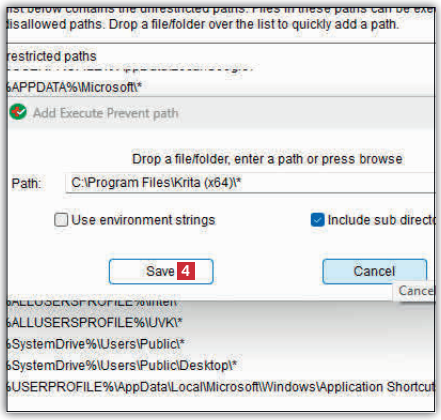
1 Åpne S.O.S Security Suite, og klikk på **Execute Prevent** 1.



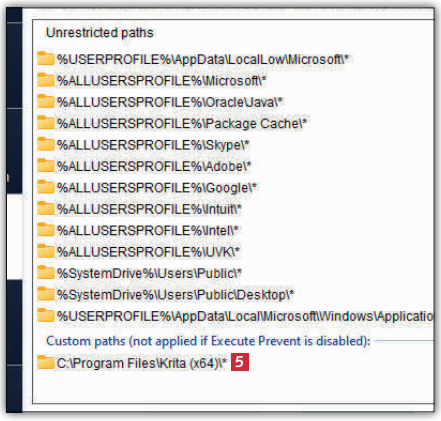
2 Klikk på **Excluded items list** 2. Deretter åpnes et vindu på skjermen der du kan velge programmet du vil gjøre unntak for.



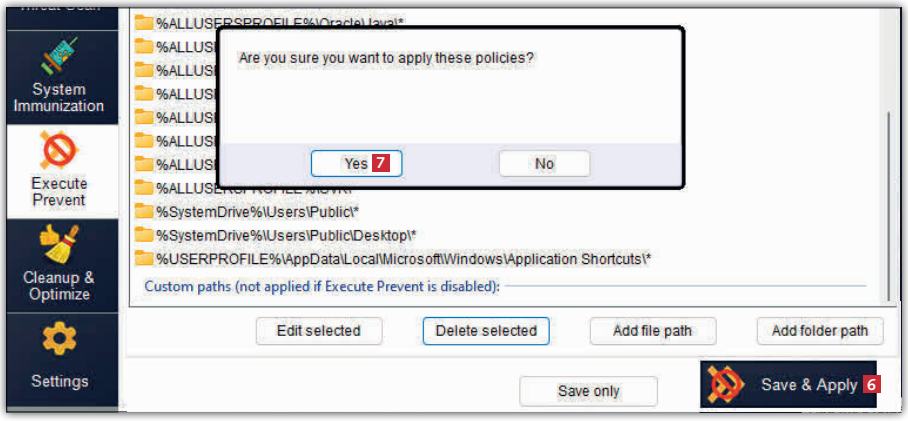
3 Du finner programmet du vil gjøre unntak for via Filutforsker. Dra programmappen, for eksempel **Krita (x64)**, 3 over til oversikten i S.O.S Security Suites.



4 Klikk på **Save** 4 i vinduet som åpnes.



5 Nå ser du programmet 5 nederst i listen over programmer som ikke er begrenset av S.O.S Security Suite.



6 Klikk på **Save & Apply** 6 for å lagre endringene, og klikk på **Yes** 7 i vinduet som åpnes. Da lagres endringene på maskinen, som nå er særdeles godt beskyttet.