ETT EXTRA SKYDDSLAGER

Skydda datorn mot ändringar

Programmet S.O.S Security Suite är ett effektivt skydd mot att någon annan än du själv ska kunna göra stora ändringar i datorn och göra den osäker.

Journalist
Niklas Ernst

En av de största farorna när du sitter vid datorn och surfar är att hackare och cyberbrottslingar i hemlighet kan göra ändringar i din dator. De kan till exempel automatiskt starta program som registrerar tangenttryckningar och skickar dem till hackarna, så att de på så sätt kan stjäla dina lösenord. Eller så kan de installera program som filmar dig med din webbkamera eller automatiskt kopierar alla dina filer och skickar dem till hackarens dator. Därför är det viktigt att hålla mycket noggrann uppsikt över vilka program som får köras på datorn.

Det kan du göra med programmet S.O.S Security Suite, som innehåller en bra funktion som kallas Execute Prevent. Tanken med funktionen är att förhindra att skadliga filer körs. Execute Prevent lägger till speciella begränsningar i systemregistret som ser till att vissa specifika typer av filer inte kan köras i utvalda mappar samt eventuellt också deras undermappar. Det kan handla om körbara filer som .exe, skript som .bat eller .vb, till och med genvägar till hemsidor (.lnk). Det är nämligen den här typen av filer som hackare och andra cyberbrottslingar behöver använda för att infektera din dator.

Fördelen med att använda Execute Prevent är att det skapar ett extra lager av skydd även om antivirusprogrammet inte upptäcker något hot. Om ett virus skulle hamna i någon av de blockerade mapparna kommer det helt enkelt inte att kunna köras och därmed inte heller kunna skada datorn. Det innebär i sin tur att även om systemet blir infekterat kommer infektionen att vara "förlamad" och inte kunna göra skada.

Registrerings-databasen

Registreringsdatabasen, eller systemregistret, i Windows är ett slags digitalt lagringssystem som håller reda på alla inställningar och all information om både Windows och program du installerar. Tänk på det som en organiserad anteckningsbok som Windows använder för att lagra information om hur datorn ska fungera, dina inställningar och alla detaljer som gör att allt fungerar optimalt.

S.O.S Security Suite

Sätt effektivt stopp för andra från att kunna göra ändringar i din webbläsare eller på din dator.

Språk
Engelska

Fungerar med
Windows 10 och 11

Hämta programmet på vår hemsida:
pctidningen.se/2419

Lär känna programmet

Här följer en kort introduktion till programmet S.O.S Security Suite och några av de praktiska verktyg som det innehåller.

Dashboard
Dashboard ger en överblick över din dator, bland annat vilken processor datorn har och om Windows Defender är aktiverat.

Execute Prevent
Här kan du ange att vissa typer av filer (inte) kan startas i specifika mappar. Det ger ett extra lager av säkerhet till din dator.

System Immunization
Här hittar du de inställningar som definierar de ändringar som kan göras på datorn.

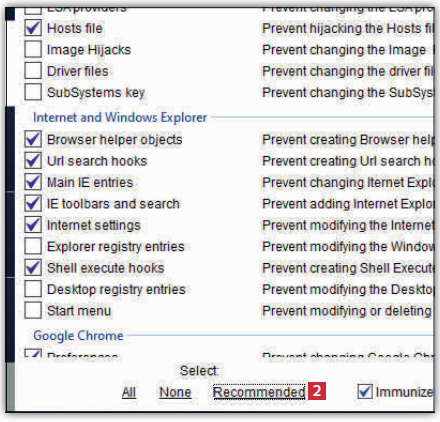
Aktivering
Till höger kan du snabbt se om System Immunisation och Execute Prevent är aktiverade.

Foto: fridaydsgn/Shutterstock.com

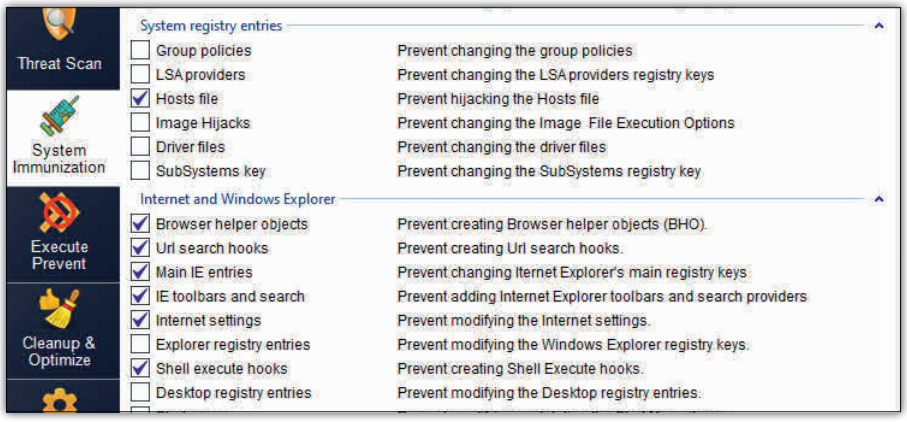
Hindra andra från att ändra i datorn

Det första steget mot att se till att inga ändringar kan göras på din dator är fliken System Immunisation. Här skyddas framför allt din webbläsare. Du kan alltid ändra inställningarna igen om du får problem.

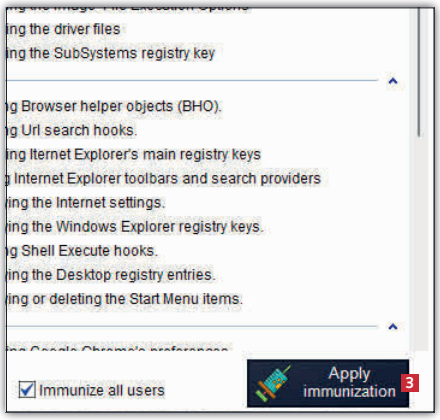
1 Hämta S.O.S Security Suite från vår webbplats och installera programmet. I programmets huvudmeny klickar du på fliken som heter **System Immunization** 1.



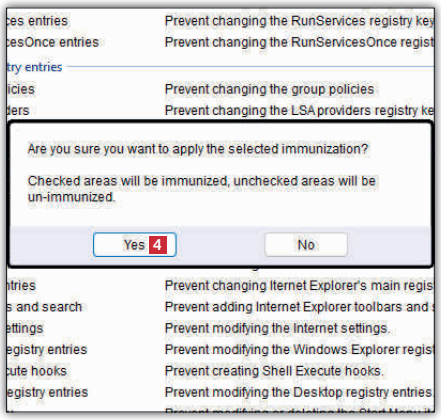
2 I översikten som öppnas klickar du på **Recommended** 2 längst ner i fönstret.



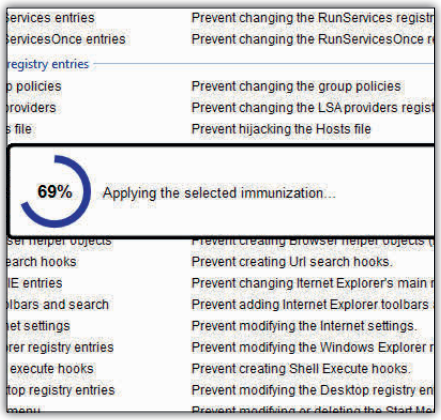
3 Då kommer en massa olika inställningar att markeras. Det här är programmets rekommendationer, som är ganska rimliga, så det är bara att låta dem vara kvar.



4 Klicka på **Apply immunization** 3.



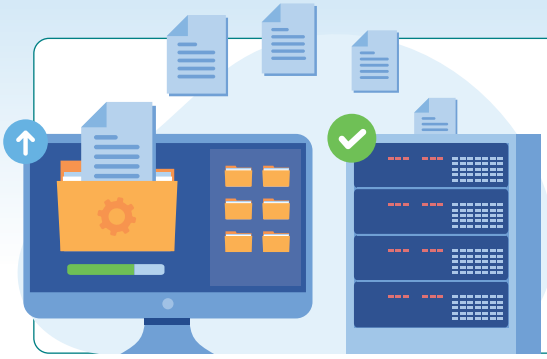
5 I fönstret som öppnas klickar du på **Yes** 4 för att spara de valda inställningarna.



6 Inställningarna sparas. Det tar inte mer än några sekunder, och din skyddade dator är redo att användas direkt.

Dessa hot stoppas av programmet

Med de rekommenderade inställningarna i System Immunisation gör programmet ett antal smarta val för din dators säkerhet. Här följer en detaljerad beskrivning av vad som händer.

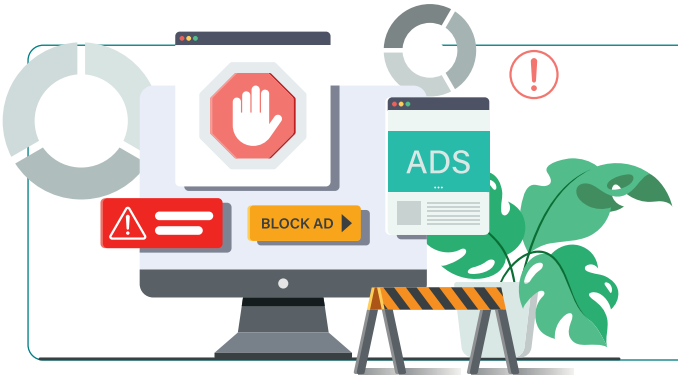


Undviker ändringar i host-filen

En host-fil är en liten textfil som Windows använder för att dirigera dig till rätt webbplatser när du surfar på webben. Värdfilen kopplar ihop domännamn med IP-adresser, så när du till exempel skriver google.se i webbläsaren kommer du till Googles sökmotor. Men om värdfilen ändras kan trafiken dirigeras någon annanstans, till exempel till en falsk webbplats. Med S.O.S Security Suite kan du förhindra att host-filen ändras.

Stoppar webbläsartillägg

En metod som hackare ofta använder för att få tillgång till datorer är via så kallade webbläsartillägg. Det är små program som ger webbläsaren extra funktionalitet, men som i vissa fall också innehåller skadlig kod. S.O.S Security Suite ser till att de inte kan installeras dolt i bakgrunden. Om du vill installera ett tillägg själv kan du tillfälligt inaktivera funktionen genom att avmarkera kryssrutan Extensions.



Blockera automatiska startprogram

I Windows kan du välja att vissa program ska starta tillsammans med datorn. Det finns dock risk för att man oavsiktligt installerar skadliga program som också startar med Windows för att sedan köras i bakgrunden. Med den här inställningen kan du hindra nya program på datorn från att starta automatiskt. För att aktivera denna funktion, markera rutan bredvid **Autorun entries** som inte är en del av de rekommenderade inställningarna.

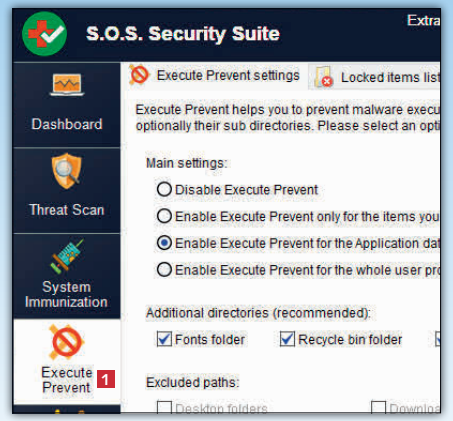
Inget krångel med säkerhetsinställningar

Om du inte vill att obehöriga ska kunna ändra säkerhets-inställningarna i din webbläsare, oavsett om du använder Chrome, Edge eller Firefox, kan du i S.O.S Security Suite välja att inställningarna inte ska kunna ändras. Allt du behöver göra är att markera rutan Secure preferences, som är en del av de rekommenderade inställningarna.

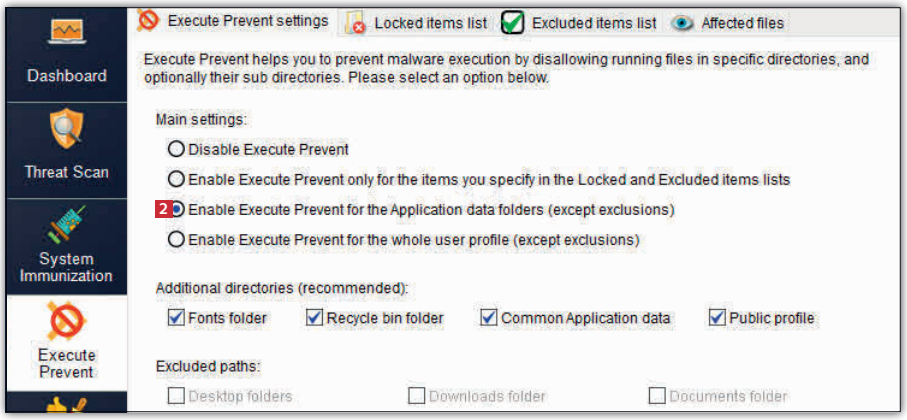
Foto: yelosmiley, Visual Generation, NiceDayKorn, Overearth/Shutterstock.com

Sätt stopp för farliga program

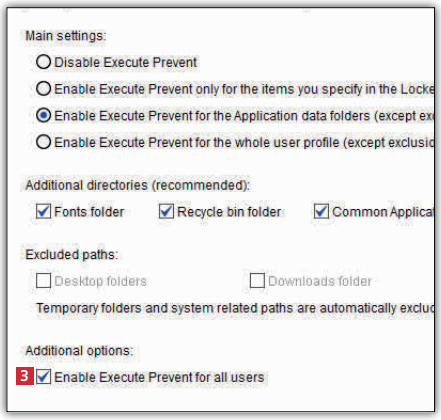
Funktionen Execute Prevent ger dig extra skydd mot virus. Den lägger till särskilda begränsningar direkt i systemregistret, vilket förhindrar att filer kan köras i specifika mappar och undermappar.



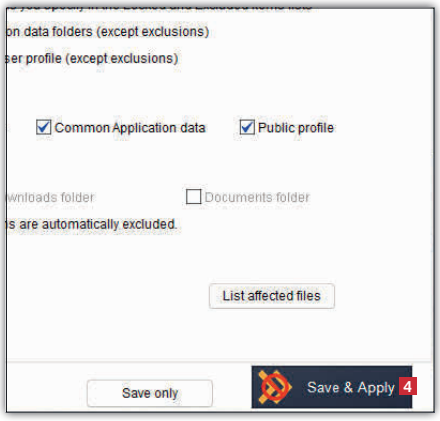
1 Klicka på fliken **Execute Prevent** 1 i huvudfönstret.



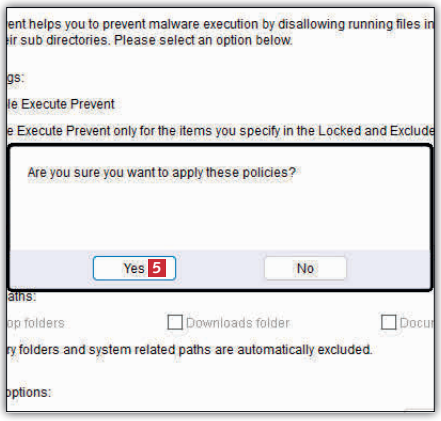
2 Vi rekommenderar att du väljer alternativet **Enable Execute Prevent for the Application data folders (except exclusions)** 2. På så sätt säkerställer du att det sätts begränsningar för program i systemregistret, men du kan också välja att de program du litar på inte kommer att påverkas av begränsningarna.



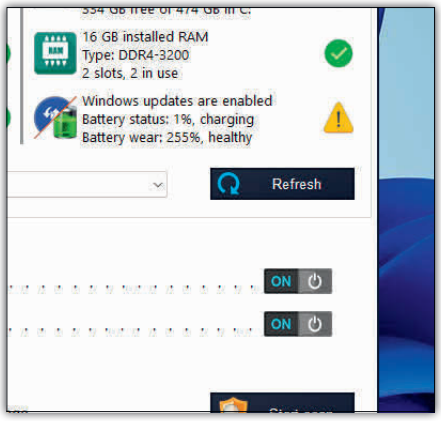
3 Se också till att det finns en markering vid **Enable Execute Prevent for all users** 3. Då omfattas alla användare av inställningen.



4 Klicka slutligen på knappen **Save & Apply** 4 längst ner i programmet.



5 I rutan som öppnas klickar du på **Yes** 5.

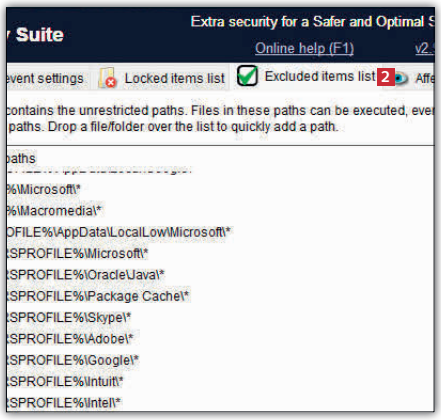


6 Inställningen är nu aktiverad och datorn är skyddad av S.O.S Security Suite.

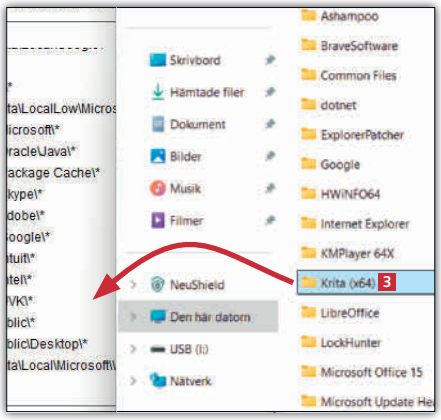
Gör undantag för program du litar på

Du har nu kraftigt begränsat både program och processer från att ändra i registreringsdatabasen. Om du har problem med betrodda program kan du låta dem slippa begränsningarna.

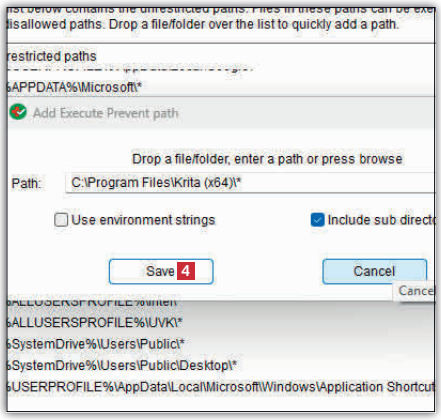
1 Öppna S.O.S Security Suite och klicka på **Execute Prevent** 1.



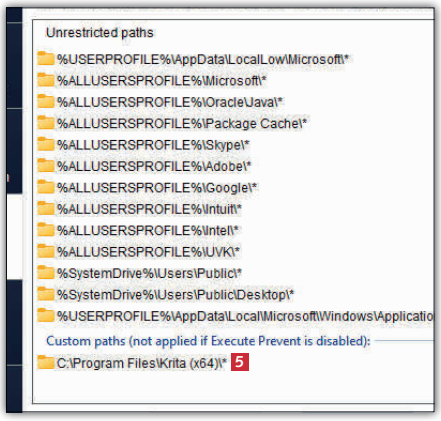
2 Välj **Excluded items list** 2. Det öppnar ett fönster där du kan välja det program du vill ska kunna köras utan begränsningar.



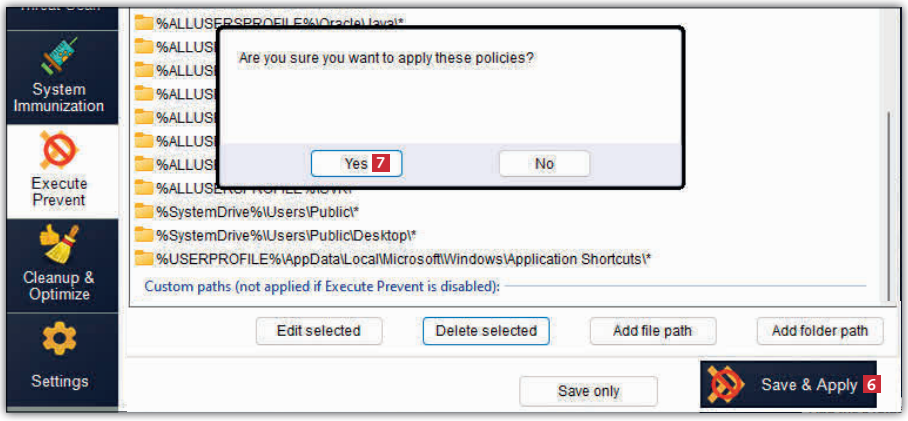
3 I Utforskaren letar du upp det program som du vill skapa ett undantag för. Dra applikationens mapp, till exempel **Krita (x64)** 3, till översikten i S.O.S Security Suite.



4 Klicka på **Save** 4 i fönstret som öppnas.



5 Nu visas programmet 5 längst ner i listan över program som inte begränsas av S.O.S Security Suite.



6 Klicka på **Save & Apply** 6 för att spara ändringarna, och därefter på **Yes** 7 i rutan som öppnas. Ändringarna sparas på datorn som nu mycket väl skyddad.