

## EKSTRA SIKKERHED TIL DIN COMPUTER:

# Beskyt pc'en mod ændringer

Programmet S.O.S Security Suite er et effektivt bolværk mod, at andre end dig selv kan lave større ændringer på din computer og gøre den usikker.



Journalist  
Niklas Ernst

En af de største farer, når du sætter dig ved din computer, er at hackere og it-kriminelle i det skjulte laver ændringer på din pc. De kan eksempelvis automatisk få startet programmer, som optager dine tastetryk, og sender dem tilbage til hackerne. På den måde kan de tiltuske sig dine kodeord. Eller de kan installere små programmer, som filmer dig med dit webkamera, eller som automatisk kopierer alle dine filer og sender dem afsted

til hackerens computer. Det gælder derfor om at føre ganske stram kontrol med, hvilke programmer der må køre på pc'en. Til det formål kan du bruge programmet S.O.S Security Suite, som blandt andet rummer funktionen Execute Prevent. Hovedideen med denne funktion er at forhindre, at skadelige filer overhovedet kan køre. Execute Prevent tilføjer specielle begrænsninger direkte til Windows' registreringsdatabase, og disse begrænsninger blokerer for, at bestemte typer filer kan blive kørt i udvalgte mapper og eventuelt i deres undermapper. Det kan være eksekverbare

filer som .exe, scripts som .bat eller .vb, og endda genveje (.lnk). Altså netop den type filer, som hackere og it-kriminelle skal bruge for at inficere din computer.

Fordelen ved at bruge Execute Prevent er, at det skaber en ekstra beskyttelseslag, selv hvis antivirusprogrammet ikke opdager en trussel. Hvis en virus skulle ende i en af de blokerede mapper, vil den ganske enkelt ikke kunne køre og dermed ikke kunne skade computeren. Det betyder, at selv hvis systemet bliver inficeret, vil infektionen være "lammet" og ude af stand til at udføre sin skade.

### Registreringsdatabasen

Registreringsdatabasen i Windows er et slags digitalt opslagssystem, der holder styr på de vigtigste indstillinger og oplysninger om både selve Windows og om de programmer, som du installerer. Tænk på det som en slags organiseret notesbog, hvor Windows gemmer oplysningerne om, hvordan din pc skal fungere, om dine præferencer og om de indstillinger, der gør, at alting kører optimalt.





## S.O.S Security Suite

Sæt en effektiv stopper for, at andre kan lave ændringer i din browser eller på din computer.

**Sprog**  
Engelsk

**Virker med**  
Windows 10 og 11

**Hent programmet på vores hjemmeside:**

[komputer.dk/2419](http://komputer.dk/2419)



# Lær programmet at kende

Du får her en kort introduktion til programmet S.O.S Security Suite og nogle af de nyttige værktøjer, som programmet indeholder.

**S.O.S. Security Suite** Extra security for a Safer and Optimal System  
Online help (F1) v2.9.3.0

**Dashboard**

- Windows 11 Home 64-bit  
Build 22631 Version 23H2  
Installed in 2023/06/06
- LENOVO 82KU  
Bios: LENOVO GLCN46WW  
S/N: PF3PXH6E
- Ryzen 5 5500U with Radeon Graphics  
6 cores, 12 threads at 2100 MHz
- AMD Radeon(TM) Graphics  
Driver version: 31.0.12044.56000  
1920x1080 px, 2 GB of VRAM

**Security Status:**

- Windows Defender: ON
- Windows firewall: ON
- UAC: ON | System Restore: ON
- 509GB NVMe SSD  
Status: OK  
334 GB free of 474 GB in C:
- 16 GB installed RAM  
Type: DDR4-3200  
2 slots, 2 in use
- Windows updates are enabled
- Battery status: 1%, charging
- Battery wear: 255%, healthy

Available fixes: Free storage space

System immunization is ON

Execute Prevent is ON

Last threat scan was 4 days, 7 hours and 25 minutes ago

Start scan

### Dashboard

På fanen Dashboard får du et hurtigt overblik over din computer. Her kan du fx se CPU'en og om Windows Defender er slået til.

### Execute Prevent

Her kan du angive, at bestemte typer filer (ikke) kan blive startet i specifikke mapper. Dermed tilføjer du et ekstra lag af sikkerhed til din computer.

### System Immunization

Her finder du indstillingerne, som definerer de ændringer, der kan laves på din pc.

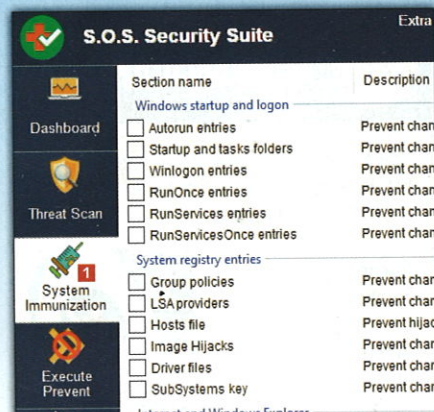
### Aktiveringer

Til højre kan du hurtigt se, om funktionerne System Immunization og Execute Prevent er aktiveret.

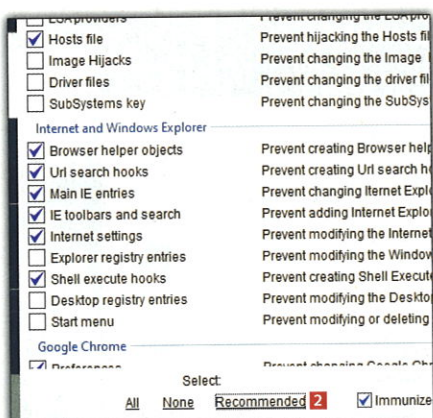


# Undgå at andre laver ændringer på din pc

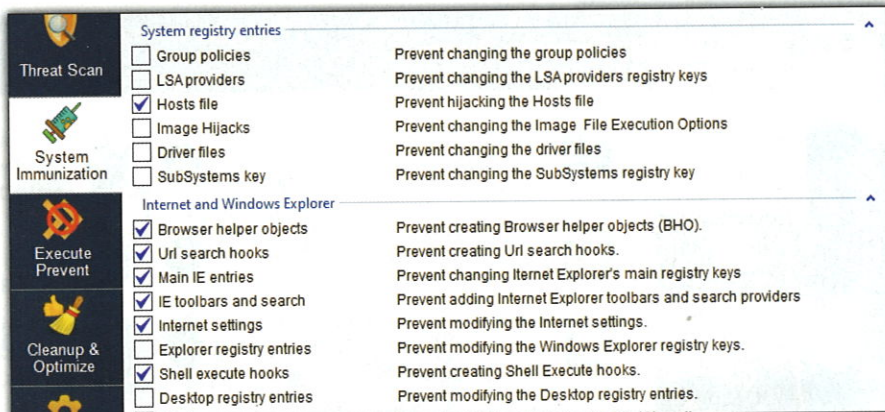
Det første skridt mod at sikre, at der ikke kan laves ændringer på din computer, er fanen System Immunization. Her er det særligt din browser, der bliver beskyttet. Du kan altid ændre indstillingerne tilbage igen, hvis du oplever problemer.



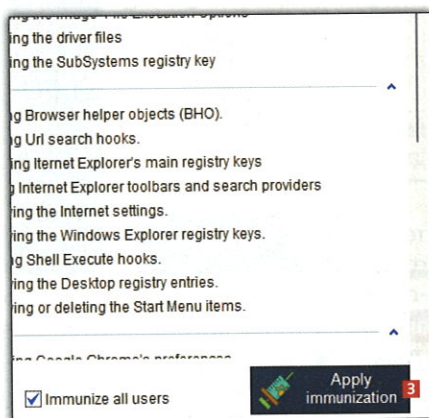
**1** Hent S.O.S Security Suite på vores hjemmeside og installer programmet. I programmets hovedmenu skal du klikke på knappen **System Immunization** **1**.



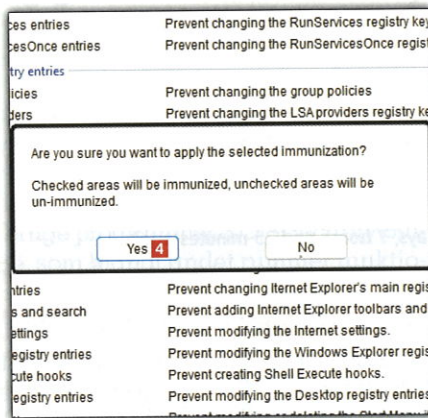
**2** I oversigten, der åbner, skal du klikke på **Recommended** **2** nederst i vinduet.



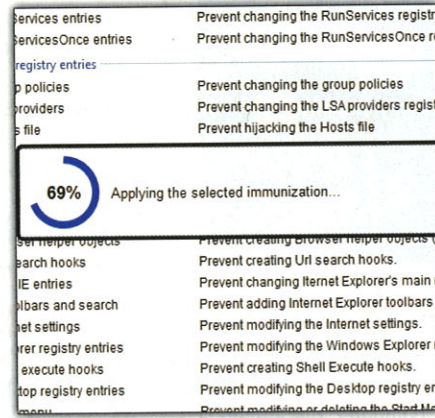
**3** Derefter bliver en masse forskellige indstillinger markeret. Det er programmets anbefalinger, som er ganske fornuftige, så lad bare dem stå.



**4** Klik så på **Apply immunization** **3**.



**5** I vinduet, der åbner, skal du klikke på **Yes** **4** for at gemme de valgte indstillinger.

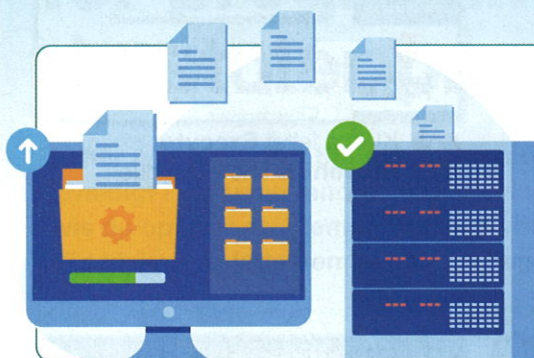


**6** Herefter gemmes indstillingerne. Det tager ikke mere end et par sekunder og din beskyttede computer er klar til brug umiddelbart efter.



# Disse trusler stoppes af programmet

Med de anbefalede indstillinger i System Immunization træffer programmet en række kloge valg for sikkerheden på din pc. Her kan du få en nærmere beskrivelse af, hvad der sker.

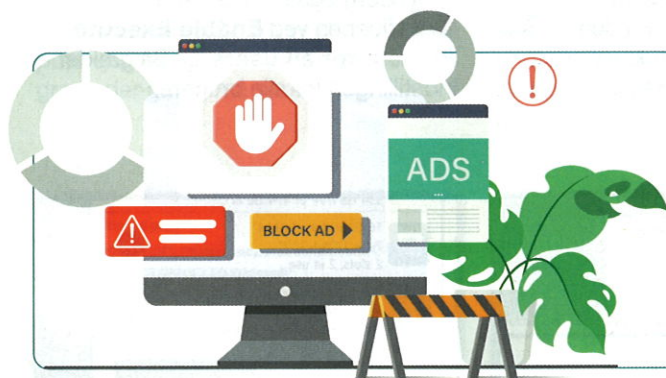


## Undgå ændringer i host-filen

En host-file er en lille tekstfil, som Windows bruger til at lede dig hen til de rette hjemmesider, når du er på nettet med din browser. Host-filen forbinder domænenavne til IP-adresser, så når du fx indtaster google.com i browseren, bliver du ledt til Googles søgemaskine. Bliver der ændret i host-filen, kan trafikken dog ledes et andet sted hen, fx en falsk hjemmeside. Med S.O.S Security Suite undgår du, at der kan ændres i host-filerne.

## Stopper tilføjelser til browseren

En metode, hackerne ofte bruger til at få adgang til din computer, er såkaldte tilføjelser til browseren. Det er små programmer, der giver browseren en ekstra funktion, men som i nogle tilfælde også indeholder ondsindet kode. S.O.S Security Suite sørger for, at de ikke kan installeres i baggrunden. Vil du selv installere en tilføjelse, skal du deaktivere funktionen midlertidigt ved at fjerne fluebenet ved punktet **Extensions**.

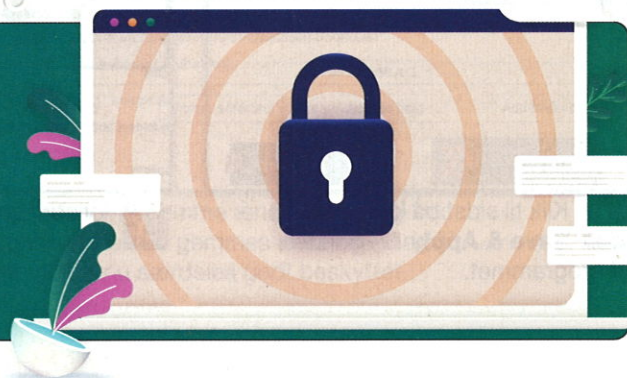


## Bloker automatiske opstartsprogrammer

I Windows kan du vælge, at visse programmer starter sammen med pc'en. Men du kan også risikere, at du uforvarende får installeret skadelige programmer, som starter med Windows og kører i baggrunden. Med denne indstilling blokerer du for, at nye programmer på din computer automatisk kan starte op sammen med computeren. Funktionen aktiveres ved at sætte fluebenet ved **Autorun entries** og er ikke en del af de anbefalede indstillinger.

## Ingen rod med sikkerhedsindstillinger

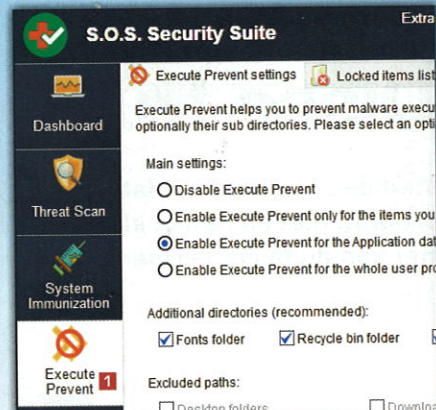
Hvis du ikke vil have, at uvedkommende kan ændre i sikkerhedsindstillingerne i din browser, hvad enten du bruger Chrome, Edge eller Firefox, kan du i S.O.S Security Suite vælge, at indstillingerne ikke må kunne ændres. Det kræver blot, at du sætter fluebenet ved feltet **Secure preferences**, som er en del af de anbefalede indstillinger.



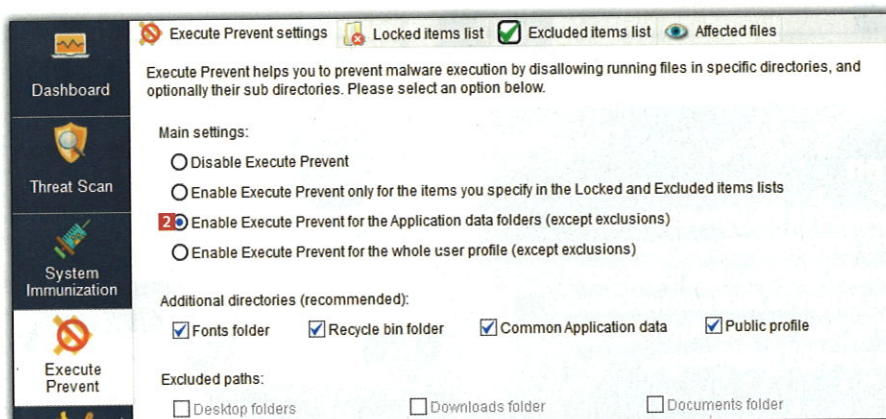


# Sæt en stopper for farlige programmer

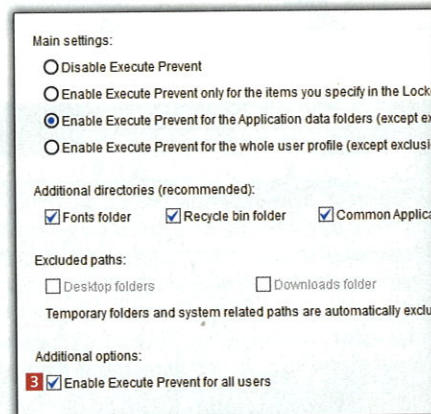
Execute Prevent-funktionen giver dig ekstra beskyttelse mod virus. Den tilføjer særlige begrænsninger direkte i Windows' registreringsdatabase og forhindrer på den måde filer i at køre i bestemte mapper og undermapper.



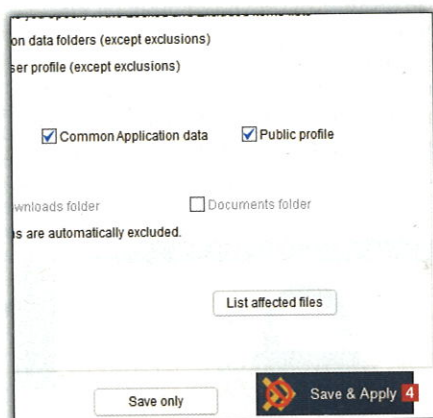
**1** Klik på feltet **Execute Prevent** i hovedvinduet.



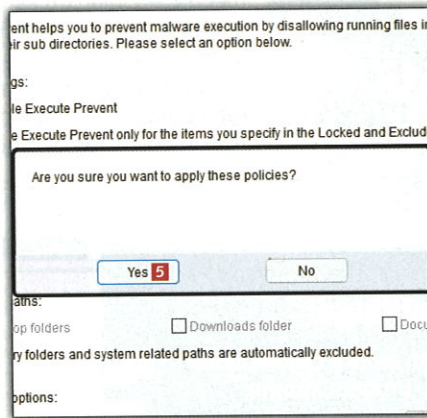
**2** Vi anbefaler, at du vælger indstillingen **Enable Execute Prevent for the Application data folders (except exclusions)** **2**. På den måde sikrer du, at der sættes begrænsninger for programmer i Windows' registreringsdatabase, men at du også kan vælge, at de programmer, du stoler på, ikke rammes af begrænsningerne.



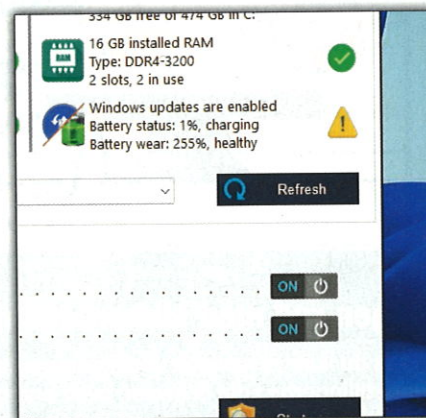
**3** Sørg også for, at der er sat flueben ved **Enable Execute Prevent for all users** **3**. Så gælder indstillingen for alle brugere.



**4** Klik til sidst på knappen **Save & Apply** **4** i bunden af programmet.



**5** I vinduet, der åbner, skal du klikke på **Yes** **5**.

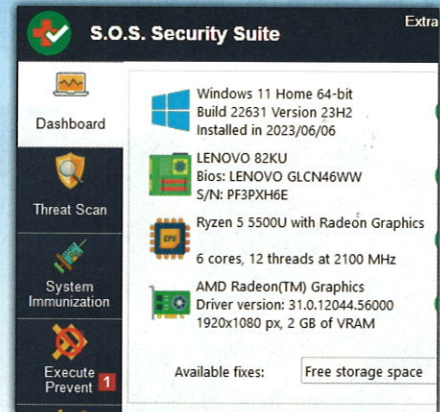


**6** Nu er indstillingen slået til og din computer er nu beskyttet af programmet S.O.S Security Suite.

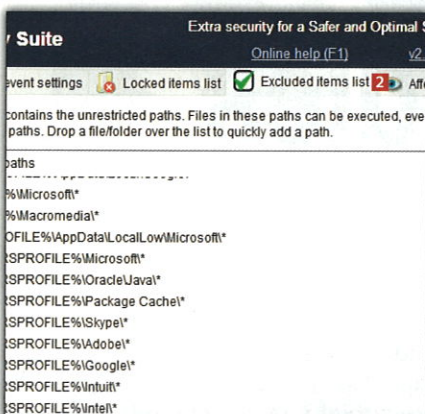


# Lav undtagelser for programmer, du stoler på

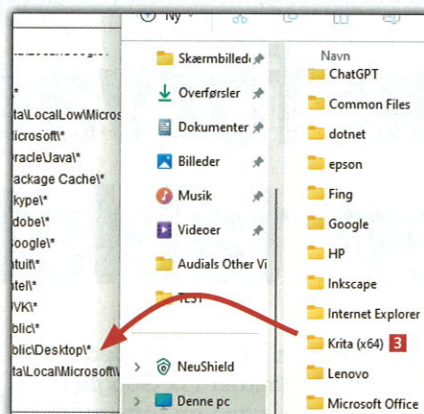
Du har nu begrænset både programmer og processer gevaldigt i at kunne ændre i registreringsdatabasen. Hvis du oplever problemer med programmer, du har tillid til, kan du lade dem slippe for begrænsningerne.



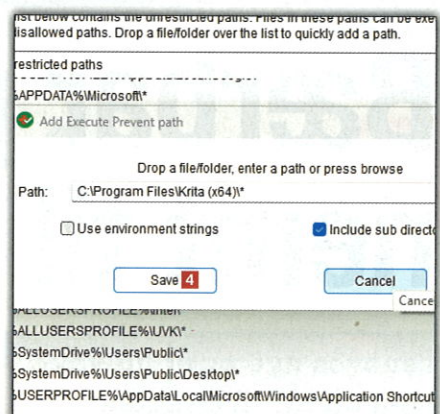
**1** Åbn S.O.S Security Suite og klik på fanen **Execute Prevent** **1**.



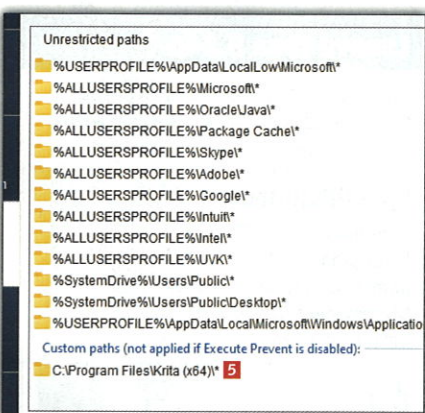
**2** Klik på **Excluded items list** **2**. Herefter åbner et vindue på computeren, hvor du kan vælge det program, der gerne må køre.



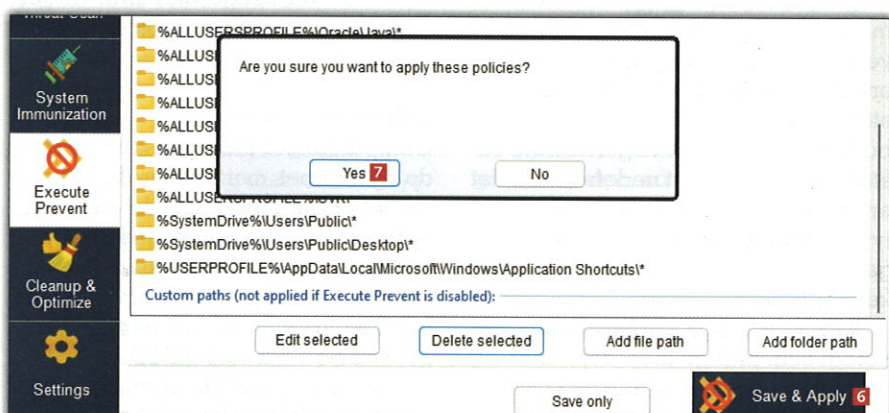
**3** I Stifinder finder du nu frem til det program, du gerne vil tilføje en undtagelse for. Træk programmets mappe, fx **Krita (x64)**, **3** over i S.O.S Security Suites oversigt.



**4** Klik på **Save** **4** i vinduet, der åbner.



**5** Du kan nu se programmet **5** i bunden af listen over programmer, der ikke er begrænset af S.O.S Security Suite.



**6** Klik på **Save & Apply** **6** for at gemme ændringerne og klik på **Yes** **7** i vinduet, der åbner. Så gemmes ændringerne på computeren, og din computer er nu særdeles godt beskyttet.