

De farverige falske advarsler på pc'en kan faktisk som regel undgås. Find ud af, hvordan du nemt slipper af med dem.



5 EFFEKTIVE LØSNINGER:

Slip for aggressive fup-alarmer på din pc

Højtråbende advarsler på computeren kan ramme os alle. Reagerer du på den rigtige måde, kan du blive fri for falske advarsler fremover.



Journalist
Steffen Nielsen

Du, jeg og alle andre pc-brugere har oplevet problemet. Tilbagevendende pop op-annoncer på skærmen. De aggressive beskeder dukker op i browseren, på Skrivebordet eller nede i højre hjørne af skærmen. Det konkrete budskab er forskelligt fra gang til gang, men essensen er den samme: Noget er galt på din computer, og for at løse problemet skal du reagere så hurtigt som muligt. Denne artikel handler om disse advarsler, og hvad du kan gøre for at slippe for dem.

Det første og vigtigste skridt er at vide, at den slags beskeder er snyd og bedrag. Med det udgangspunkt undgår du at falde i de fælder, som svindlerne har lagt. Det er vores indtryk, at mange pc-brugere har styr på

den del af problemet og ikke så nemt lader sig narre. Vi får i hvert fald ganske mange henvendelser fra læsere, som spørger, om de ikke har ret i, at en given annonce på deres pc er falsk, og gerne vil vide, hvordan de helt kan undgå dem.

Er browseren eller pc'en ramt?

Vores mission er derfor at sikre, at de falske advarsler ikke bliver ved med at dukke hos dig. Det er straks vanskeligere, da årsagen til annoncerne varierer. Nogle gange skyldes det, at din pc er inficeret med malware. I andre tilfælde er annoncerne en konsekvens af problemer i din browser. Det kan fx være, at du har installeret en dårlig tilføjelse eller givet dårlige hjemmesider tilladelser, de ikke skulle have haft. I artiklen her giver vi dig fem løsninger, så din pc ikke længere oversvømmes af falske advarsler.

4 tegn på at en advarsel er fup og svindel

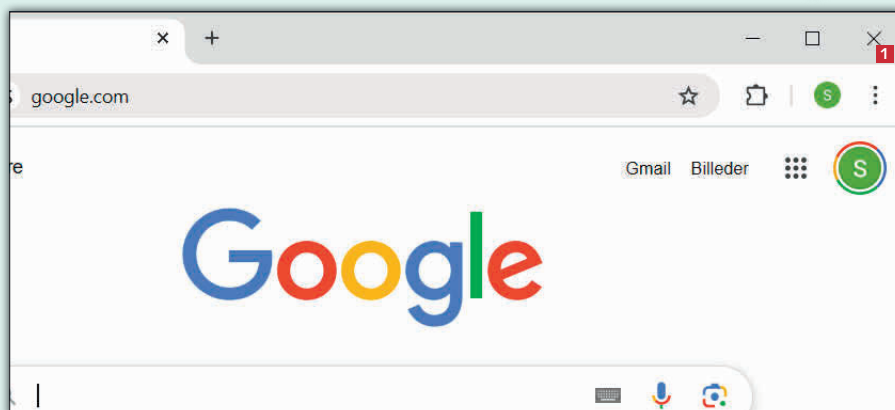
- **Har kraftige farver**
Fupreklamer er tit røde og gule for at få din opmærksomhed.
- **Har ukendt afsender**
Nævner advarslen et program, du slet ikke har på din pc? Så er den helt sikkert falsk.
- **Nævner virus og pc-problemer**
Falske annoncer handler ofte om sikkerhedsproblemer på din pc.
- **Beder om en hurtig reaktion**
Falske annoncer beder dig typisk reagere på problemerne på din pc med det samme.



LØSNING 1

Luk din browser

En hurtig løsning på aggressive advarsler er at lukke browseren. Så forsvinder advarslerne typisk fra skærmen. For at undgå, at de vender tilbage, skal du herefter gennemføre en eller flere andre løsninger.



- 1** Luk browseren ved at klikke på krydset i øverste højre hjørne **1**. Hvis annoncen stadig vises på din skærm, er det næppe browseren, der står bag. Du er sandsynligvis ramt af malware, og skal benytte løsning 2. Hvis annoncen lukkes ved, at du lukker browseren, skal du arbejde videre med løsningerne 3, 4 og 5.



**Malwarebytes
Antimalware**

Programmet hjælper dig med at finde ud af, om din pc er inficeret af malware og fjerner de skadelige filer fra din pc.

Sprog
Engelsk

Virker med
Windows 10 og 11

Hent programmet på vores hjemmeside:
komputer.dk/2512



LØSNING 2

Fjern malware fra din computer

Hvis de falske annoncer ikke stammer fra din browser, kan afsenderen være et skadeligt program på din pc. Disse små programmer kan være godt skjult og kan ofte kun graves frem af specialiserede værktøjer som Malwarebytes Antimalware. Se her, hvordan du fjerner malware.



Malwarebytes Setup Wizard

Install now to clean and protect your computer for good

Install **1**

[Advanced options](#)

1 Hent programmet fra vores side, og start installationen. Vælg **Install** **1**. I næste vindue vælger du punktet **Personal**.

Next, secure your online activity with Browser Guard

- Protect your finances from online threats
- Block online phishing and scams
- Keep your personal data private
- Stop annoying ads and trackers

Secure my browser

[Skip this step \(not recommended\)](#) **2**

2 I dette vindue klikker du på **Skip this step (not recommended)** **2**. Vælg så **Open Malwarebytes**.

Welcome to Malwarebytes!

malware, check your defenses, and search for exposures

Scan now **3**

[Skip](#)

3 Klik nu på knappen **Scan now** **3**.

☒	Name	Type	Object type	Location
☒	PUP.Optional.Adva...	Potentially Unwan...	Registry Value	HKU\S-1-5-21-21431085...
☒	PUP.Optional.Adva...	Potentially Unwan...	File	C:\USERS\STJEF\CONT...
☒	PUP.Optional.Bundl...	Potentially Unwan...	File	C:\USERS\STJEF\CONT...
☒	PUP.Optional.Adva...	Potentially Unwan...	File	C:\USERS\STJEF\ONED...

[Skip](#) **Quarantine 9 items** **4**

4 Efter et stykke tid vises en liste med resultater. I vores tilfælde var der ni farlige filer, og vi vælger **Quarantine 9 items** **4** for at uskadeliggøre de farlige elementer. Du skal gøre det samme på din computer (Antallet af farlige filer vil variere).

Trusted Advisor

Success! 9 threats resolved

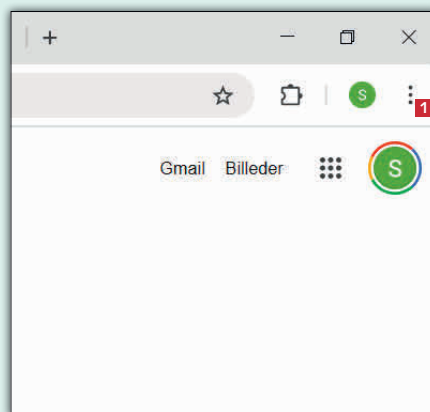


5 De skadelige elementer er fjernet. Nu vil du forhåbentligt slippe for flere falske advarsler.

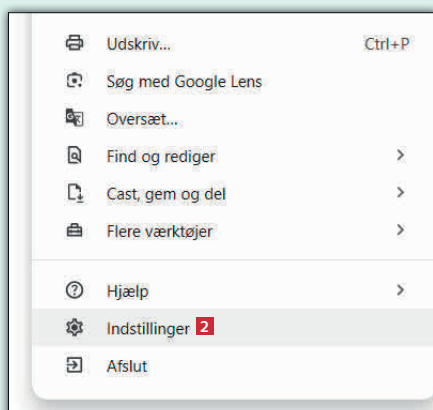


Ryd browserdata

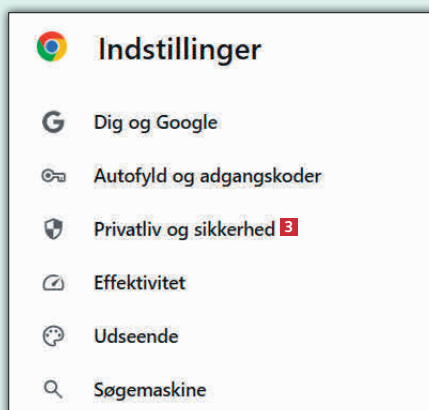
Hvis advarslerne stammer fra browseren, kan det eventuelt hjælpe at rydde cookies og andre data, som kan bruges til at sende dig falske annoncer. Vi viser her, hvordan du fjerner browserdata i Chrome.



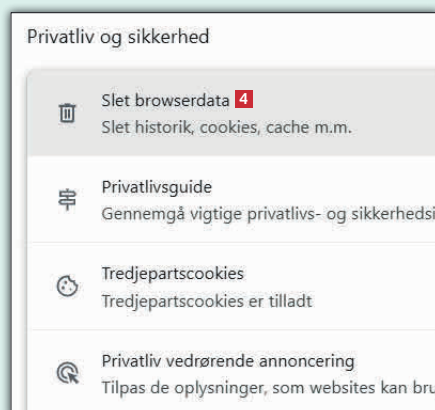
1 I Chrome klikker du på de tre prikker **1** oppe til højre.



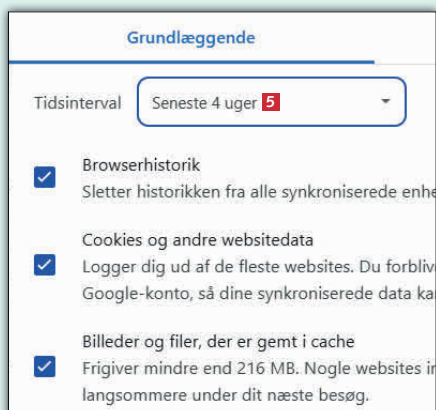
2 Vælg derpå menupunktet **Indstillinger** **2** langt nede i menuen.



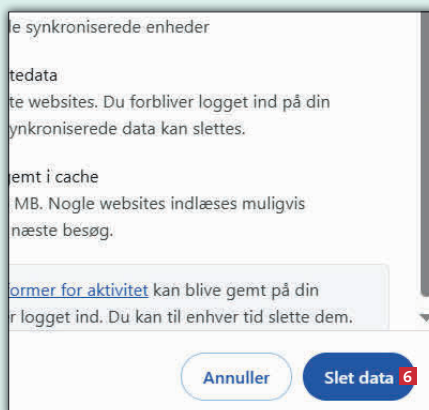
3 I panelet til venstre vælger du nu **Privatliv og sikkerhed** **3**.



4 Klik på punktet **Slet browserdata** **4**.



5 Alt efter hvor længe problemet med advarsler har stået på, vælger du, hvor langt tilbage i tiden du vil slette data. Vi sletter data for de seneste fire uger **5**.



6 Til sidst klikker du på **Slet data** **6** for at slette browserdata.

Sådan gør du i Edge



I Edge kan du også slette data. Besøg **edge://settings/privacy**. Vælg **Ryd browserdata**. Klik på **Vælg, hvad der skal ryddes**. Vælg hvor langt tilbage, der skal slettes data, og klik på **Ryd nu**.

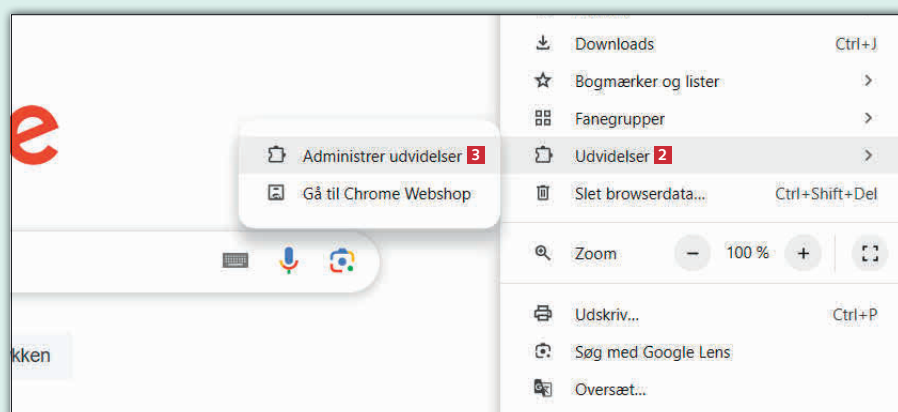


LØSNING 4

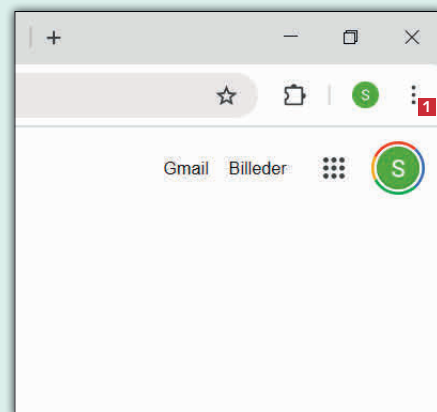


Fjern tilføjelser fra browseren

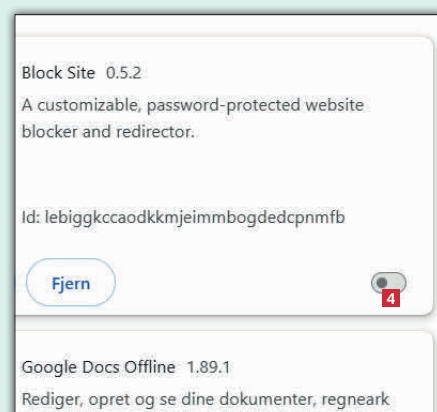
Dårlige browsertilføjelser er en kilde til flere problemer. Et eksempel er de falske annoncer, vi behandler i denne artikel. Det er dog ikke let at vide, hvilke tilføjelser der er årsagen. Derfor skal du fjerne browsersens tilføjelser enkeltvis for at se, om det gør en forskel. Vi viser det her i Chrome.



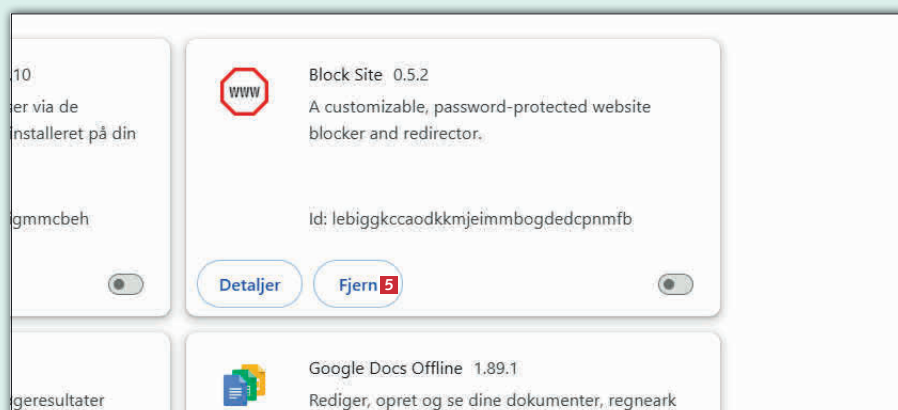
2 Vælg nu **Udvidelser** **2** fulgt af **Administrer udvidelser** **3**.



1 Klik på de tre prikker **1** oppe til højre i Chrome.



3 Vælg en tilføjelse i listen, og slå skyderen fra **4**. Den skal blive grå som vist her.



4 Hvis du ikke bruger tilføjelsen, er det en god ide at fjerne den helt **5**. Vent nu og se, om advarslerne forsvinder efter en genstart af browseren. Dukkér de stadigvæk op, går du videre og deaktiverer eller fjerner den næste tilføjelse på listen.

Sådan gør du i Edge



I Edge fjernes tilføjelser således: Klik på de tre prikker oppe til højre. Vælg **Udvidelser**. Klik derpå på **Administrer udvidelser**. Du kan nu fjerne en udvidelse ved at klikke på **Fjern**. Prøv det samme med andre udvidelser, til du slipper for annoncer.

Installerede udvidelser

Fra Store til Microsoft Edge-tilføjelsesprogrammer



Avast SafePrice
Discover the best coupons at your favorite online sh
[Detaljer](#) [Fjern](#)



Stop notifikationer fra hjemmesider

Hvis du ved et uheld har tilladt en hjemmeside at sende dig notifikationer, kan det være årsagen til de falske reklamer. Vi viser, hvordan du blokerer notifikationer og popupbeskeder fra sider i Chrome.

Standardadfærd

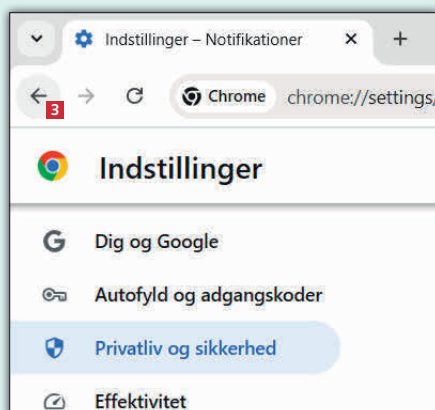
Websites følger automatisk denne indstilling, når du besøger dem, at informere dig om breaking news eller chatbeskeder.

☐ Websites kan spørge dig, om de må sende dig besked.

☒ Tillad ikke, at websites sender notifikationer

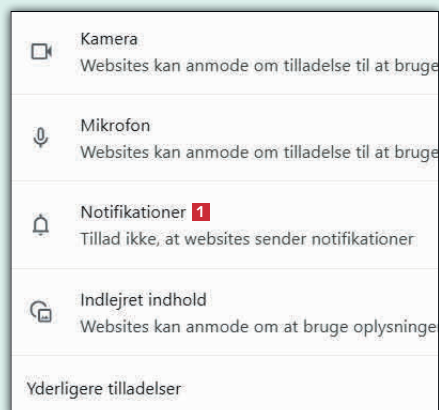
Tilpasset adfærd

De websites, der er angivet nedenfor, anvender en tilpasset adfærd.

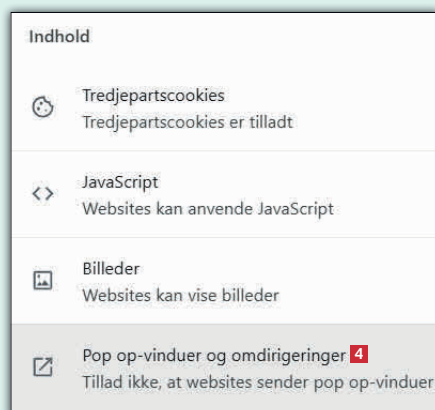


2 Sæt markering ved punktet **Tillad ikke, at websites sender notifikationer** **2**.

3 Klik på tilbageknappen i browseren **3**.



1 Besøg siden **chrome://settings/content**, og vælg **Notifikationer** **1**.



4 Vælg nu **Pop op-vinduer og omdirigeringer** **4**.

Websites kan sende pop op-vinduer for at vise annoncer eller bruge omdirigeringer til at føre dig til websites, du måske ikke ønsker at besøge.

Standardadfærd

Websites følger automatisk denne indstilling, når du besøger dem.

☐ Websites kan sende pop op-vinduer og bruge omdirigeringer

☒ Tillad ikke, at websites sender pop op-vinduer eller anvender omdirigeringer

5 Sæt markering ved **Tillad ikke, at websites sender pop op-vinduer eller anvender omdirigeringer** **5**.

Nu skulle du gerne slippe for de aggressive annoncer.

Sådan gør du i Edge



I Edge sætter du en stopper for pop op-beskeder på følgende vis: Besøg **edge://settings/content/popups**. Vælg derefter **Blokeret (anbefales)**. Besøg så **edge://settings/content/notifications**, og slå skyderen ved **Spørg altid, inden der sendes (anbefales)** fra (den skal være sort-hvid).