SLIP FOR VIRUSALARM OG SPAM:

25 tips til total sikkerhed

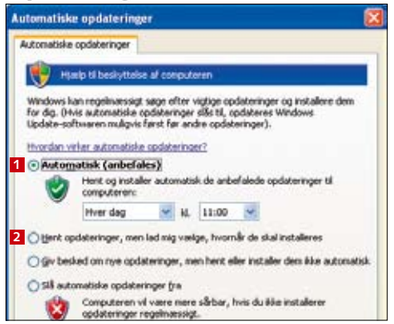
Sikkerhed på nettet er en forudsætning for, at du får glæde af din pc. Hvis du følger vores 25 sikkerhedstips, kan du roligt åbne dine mails og surfe rundt på nettet.

Aktiver Windows' firewall

Den indbyggede firewall i Windows beskytter pc'en mod angreb. Tjek, at den er slået til, ved at gå ind i **Kontrolpanel** og vælge **Windows Firewall**. Sæt kryds ud for **Slået til (anbefales)** 1.

Aktiver Automatiske opdateringer

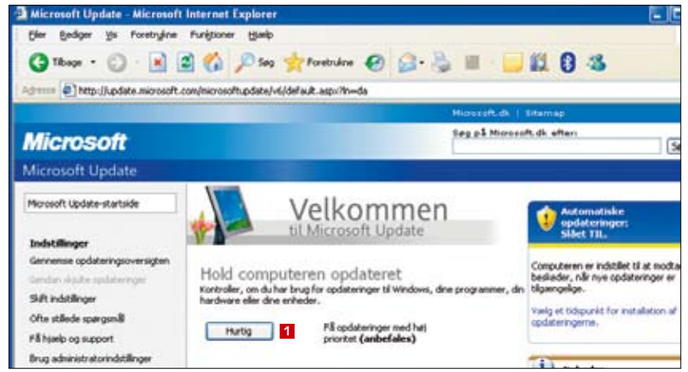
Automatiske opdateringer sørger for at installere sikkerhedsrettelser til Windows og andre programmer fra Microsoft. Dermed bliver sikkerhedshullerne lukket, så snart det er muligt. Åbn **Automatiske opdateringer** via **Kontrolpanel**, og vælg enten **Automatisk (anbefales)** 1 eller **Hent opdateringer, men lad mig vælge, hvornår de skal installeres** 2.



Besøg Microsoft Update

Hvis du ikke har haft automatiske opdateringer slået til, kan du på webstedet Microsoft Update hente de sikkerhedsopdateringer, din pc mangler. Besøg update.microsoft.com. Klik på knappen **Hurtig** 1 for at se en liste over de opdateringer, du mangler.

Under alle omstændigheder er det en rigtig god idé, at du derefter slår automatiske opdateringer til (se boksen herover). På den måde er du sikret de nyeste opdateringer og slipper for selv at skulle huske på at hente rettelser på nettet.



Så vigtige er de forskellige sikkerhedstips

Ved hvert tip angiver antallet af tændte advarselsblink, hvor vigtigt det er at følge, når du mailer eller surfer. Vil du være på den helt sikre side, anbefaler vi dig dog at holde dig til alle rådene.

Fornuftigt at følge

Bestemt en god idé

Bør altid følges

Dette råd handler om internettet

Dette råd handler om e-mails

Tænk dig om

Firewall. Antivirus. Spamfilter. Masser af tekniske hjælpemidler kan gøre din pc mere sikker. Men al den fine teknik er uden betydning, hvis du ikke selv gør en aktiv indsats.

Hvis du henter et program på nettet og installerer det på din pc, kan selv det bedste sikkerhedssystem ikke altid beskytte dig mod konsekvenserne. Måske er programmet helt uskadeligt. Men det kan også indeholde et aflytningsprogram, der registrerer, hver gang du indtaster et kodeord. Med jævne mellemrum sender det så en liste med dine brugernavne og adgangskoder til en skummel bagmand.

Skulle antivirus ikke forhindre det? Jo, men de fleste antivirusprogrammer kan kun standse trusler, som de kender i forvejen. Så hvis du bliver offer for et hidtil ukendt aflytningsprogram, er antivirusprogrammet hjælpeløst.

Derfor skal du optræne din kritiske sans. Når en webside eller en mail har et tilbud, der lyder for godt til at være sandt, skal du tænke: Kan det nu også passe?

Søg på web efter flere oplysninger. Langt de fleste svindelforsøg er velkendte.

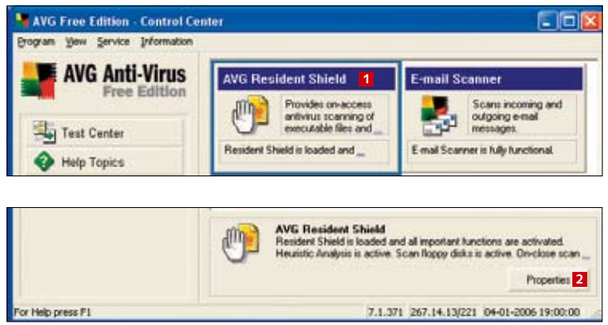
Af Torben B. Sørensen. Foto: Søren Kristensen

Opdater andre programmer

Microsoft Update dækker kun programmer fra Microsoft. Men andre programmer kan også indeholde sårbarheder, som angribere kan udnytte. Besøg derfor jævnligt producentens websted. Nogle programmer indeholder en funktion i stil med **Automatiske opdateringer** i Windows, det gælder blandt andet *Adobe Reader*. Gå ind i **Indstillinger** og derefter **Rediger**, og vælg **Opdateringer**. Vælg **Hent vigtige opdateringer, og giv mig besked, inden de installeres** 1.

Installer AVG Anti-Virus

Et antivirusprogram beskytter mod virus og mail-orme. *AVG Anti-Virus* er et godt og gratis antivirusprogram, som du finder på *K-CD'*en. Når programmet er installeret, styres det fra det indbyggede kontrolcenter. Klik på et modul, fx **AVG Resident Shield** 1. Så kan du indstille modulet med et klik på knappen **Properties** nederst 2.



Installer et spamfilter

Spam er uønskede reklamer, der ankommer som e-mail. De udgør ikke et egentligt sikkerhedsproblem, men kan være irriterende. Installer fx det gratis *Spam-Fighter* fra *K-CD'*en. Programmet lægger sig som et filter mellem dit mailprogram og din mailboks hos internetselskabet.

Begrænset brugerkonto

Hvis du deler din pc med dine børn eller andre, er det en god idé at give dem deres egen brugerkonto. Den skal have færre rettigheder end den administratorkonto, du selv anvender. Det betyder, at når man er logget ind som almindelig bruger, kan man ikke installere programmer eller få adgang til systemfiler. Åbn **Kontrolpanel** og derefter **Brugerkonti**. Vælg **Opret en ny konto**. Giv den et navn, og vælg, at det skal være en begrænset konto 1. Klik på **Opret konto** 2.

Installer et antispywareprogram

Spyware er en samlebetegnelse for en række programmer, der ændrer på din pc's opsætning, uden at du har bedt om det. Fx indstiller de startsiden i *Internet Explorer*. Formålet er at lede dig til bestemte websteder eller at følge din færden rundt på nettet. Har du først fået spyware på pc'en, er det svært at fjerne igen, men programmer som *Ad-Aware* eller *SpyBot Search & Destroy* (billedet) kan hjælpe. *Ad-Aware* ligger på *K-CD'*en, *SpyBot* (billedet) kan du hente på **www.safer-networking.org/dk/download.**

Tag sikkerhedskopi af dine data

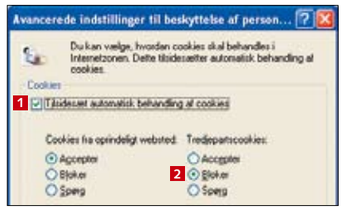
En virus fra nettet kan gøre stor skade, og du kan miste dokumenter. Hvis du vil undgå det, skal du sikkerhedskopiere. Du finder XP's sikkerhedskopiering under **Startmenuen**, **Alle programmer**, **Tilbehør**, **Systemværktøjer** og **Sikkerhedskopiering**. Vælg at kopiere enten **Mine dokumenter og indstillinger** 1 eller **Alles dokumenter og indstillinger** 2. Gem kopien på en ekstern harddisk, eller brænd den på dvd. Har du XP Home skal du først installere sikkerhedskopieringsværktøjet fra mappen \valueadd\msft\ntbackup\ på Windows XP's installations-cd.

Tjek at sikkerhedskopien virker

En sikkerhedskopi gavner kun, hvis den kan indlæses. Prøv derfor at gendanne et par af filerne fra din sikkerhedskopi, før du gemmer den væk et sikkert sted. Åbn **Startmenuen**, og vælg **Alle programmer**, **Tilbehør**, **Systemværktøjer** og **Sikkerhedskopiering**. Vælg at gendanne filer. Marker så de filer, du vil gendanne 1.

Begræns cookies

Websteder bruger cookies til at se, om du har besøgt dem før – og de kan anvendes til at overvåge din færden på nettet. Du kan begrænse risikoen for, at andre får adgang til den information, ved at forbyde såkaldte tredjepartscookies. Start *Internet Explorer*, og gå ind i menuen **Funktioner**. Vælg **Internetindstillinger**. Klik på fanebladet **Beskyttelse af personlige oplysninger**. Klik på knappen **Avanceret…** Sæt et flueben ud for **Tilsidesæt automatisk behandling af cookies** 1, og vælg **Bloker** under **Tredjepartscookies** 2. Klik på **OK**.



Stop pop-up-vinduer

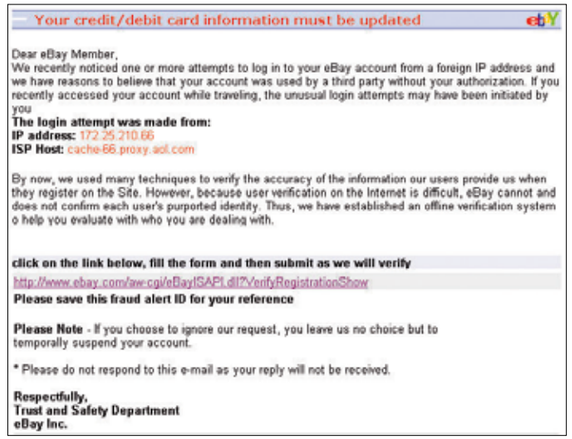
Pop-up-vinduer på websider er ikke et egentligt sikkerhedsproblem, men meget irriterende. Du kan indstille *Internet Explorers* håndtering af pop-up-vinduer ved at gå ind i menuen **Funktioner**. Vælg **Blokering af pop-up-vinduer** og så **Indstillinger for blokering af pop-up-vinduer**. Du kan indtaste adresser på websteder, der skal have lov til at åbne pop-up-vinduer 1, vælge, hvordan du bliver advaret om pop-up-vinduer 2, og indstille det generelle niveau for blokering 3.

Pas på phishing og anden svindel

"Kære kunde! Der er sket et sikkerhedsbrud på din konto hos os. Hvis du fortsat vil have adgang til den, skal du gå ind på denne webside og bekræfte dit brugernavn og din adgangskode."

Har du modtaget en mail i denne stil? Så er du udsat for phishing – et forsøg på at narre fortrolige oplysninger fra dig. Linket henviser til en falsk webside, og hvis du indtaster oplysninger her, går de direkte videre til svindlerne. Billedet viser et phishingforsøg rettet mod brugere af auktionsstedet eBay.

Du kan beskytte dig mod at blive offer ved aldrig at følge links, der optræder i mails. Opret i stedet bogmærker i din browser, som du bruger, hver gang du fx skal ind på din netbank.


Your credit/debit card information must be updated

Dear eBay Member,
We recently noticed one or more attempts to log in to your eBay account from a foreign IP address and we have reasons to believe that your account was used by a third party without your authorization. If you recently accessed your account while traveling, the unusual login attempts may have been initiated by you
The login attempt was made from:
IP address: 172.25.210.66
ISP Host: cache-66.proxy.aol.com

By now, we used many techniques to verify the accuracy of the information our users provide us when they register on the Site. However, because user verification on the Internet is difficult, eBay cannot and does not confirm each user's purported identity. Thus, we have established an offline verification system to help you evaluate with who you are dealing with.

click on the link below, fill the form and then submit as we will verify
http://www.ebay.com/aw-cgi/eBayISAPI.dll?VerifyRegistrationShow
Please save this fraud alert ID for your reference

Please Note - If you choose to ignore our request, you leave us no choice but to temporally suspend your account.

* Please do not respond to this e-mail as your reply will not be received.

Respectfully,
Trust and Safety Department
eBay Inc.

Pas på vedhæftede filer

Der er som regel ingen risiko ved at læse en e-mail. Men når den indeholder en vedhæftet fil, skal du passe på. Den vedhæftede fil kan være et skadeligt program. Derfor skal du aldrig ukritisk dobbeltklikke på en vedhæftet programfil, som du får tilsendt uopfordret. Du får som regel en advarsel, hvis du forsøger at åbne en programfil fra en e-mail.

Nogle programfiler forklæder sig som uskyldige tekstfiler. De bruger navne som Readme.txt (en masse mellemrum) .exe. Filnavne, der ender på com, pif, scr, cmd, bat eller exe, er alle programmer.

Styrk sikkerheden i Internet-zonen

Internet Explorer opdeler websteder i zoner. Hvis et websted ikke er tildelt en bestemt zone, hører det automatisk til i zonen **Internet**. Derfor er det en god idé at begrænse, hvad websteder i denne zone har lov til. Viser et websted sig at være pålideligt, kan du altid flytte det til zonen for websteder, du har tillid til. Sådan øger du sikkerhedsniveauet for zonen **Internet**: Gå ind i **Funktioner**. Vælg **Internetindstillinger…** og fanebladet **Sikkerhed** 1. Klik på zonen **Internet** 2. Træk skyderen til **Høj** 3. Klik på **OK** 4.

Brug en alternativ browser

Der er en række kendte sikkerhedsproblemer i *Internet Explorer*. Du kan undgå dem ved at anvende en anden browser. Det kan fx være *Opera* (**www.opera.com**) eller *Firefox* (**www.mozilla.com/firefox**). De kan også få sikkerhedsproblemer, men der er færre, og de rettes som regel hurtigt.

Åbn for pålidelige websteder

Hvis sikkerheden for zonen **Internet** er sat til **Høj** i *Internet Explorer*, holder nogle websteder op med at virke. De skal flyttes over i zonen **Websteder, du har tillid til**. Sæt først sikkerhedsniveauet for denne zone til **Lav**: Gå ind i **Funktioner**, og vælg **Internetindstillinger…** Vælg fanebladet **Sikkerhed** 1. Klik på zonen **Websteder, du har tillid til** 2. Træk skyderen til **Lav** 3. Klik derefter på knappen **Websteder…** 4, og indtast adresserne på websteder, som du ved er i orden.

Pas på programmer fra nettet

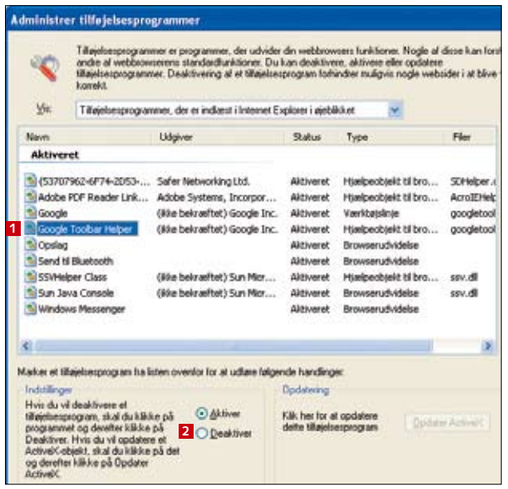
Det er let at hente og installere programmer fra nettet. Men du risikerer at få mere, end du regner med. Programmer kan indeholde virus eller spyware. Derfor er det en god idé aldrig at vælge **Kør** 1, når du henter en fil. Vælg i stedet **Gem** 2. Kør så et virustjek på filen, før du åbner den.

Gør Outlook Express sikker

Mailprogrammet *Outlook Express* kan indstilles, så det er mere sikkert at bruge. Gå ind i **Funktioner**. Vælg **Indstillinger**, og vælg fanebladet **Sikkerhed** 1. Vælg **Klassificeret zone (mere sikker)** 2. Sæt kryds ud for **Advar mig, hvis andre programmer forsøger at sende e-mail på mine vegne** 3. Vælg også **Bloker billeder og andet eksternt indhold i html-e-mail** 4. Klik på **OK**.

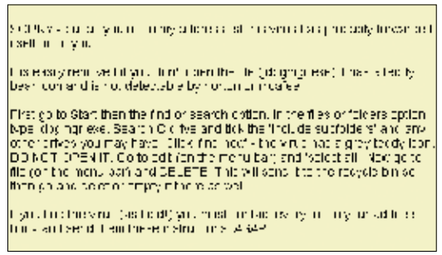
Få styr på tilføjelsesprogrammer

Spyware og andre uønskede programmer installerer ofte sig selv som såkaldte tilføjelsesprogrammer i *Internet Explorer*. Får du problemer med browseren, så vælg **Administrer tilføjelsesprogrammer…** under menuen **Funktioner**. Klik på et program på listen 1, og klik på **Deaktiver** 2, hvis du vil slå det fra. Klik på **OK**.



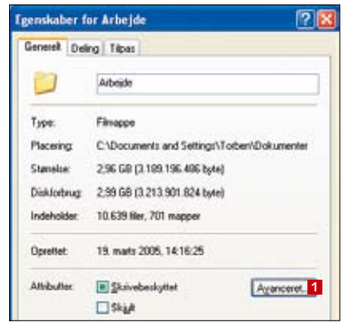
Vær kritisk over for advarsler

Der cirkulerer e-mails, som fortæller om alvorlige virusangreb. De siger, at man skal slette en bestemt fil og i øvrigt sende advarslen videre til alle, man kender. Men det er løgn. Den pågældende fil er uskadelig, og advarslen er et falsum. Andre mails lover en gratis mobiltelefon, hvis man videresender mailen til 20 andre. Før du sender noget videre, som du modtager pr. mail, kan du søge efter information om emnet på nettet. Du vil som regel finde ud af, at det er en såkaldt hoax – et fupnummer.



Krypter dine data

Hvis din bærbare pc bliver stjålet, kan tyven se alle dine filer – også selv om du har beskyttet din brugerkonto med et password. Hvis du har Windows XP Pro kan du forhindre det ved at kryptere filerne. Så kan indholdet kun ses, når du er logget ind på pc'en. Sådan krypterer du mappen: Find mappen i Windows Stifinder. Højreklik på den, og vælg **Egenskaber**. Klik på knappen **Avanceret...** 1. I det nye vindue skal du sætte kryds ud for **Krypter indhold for at sikre data** 2 og klikke på **OK** 3.

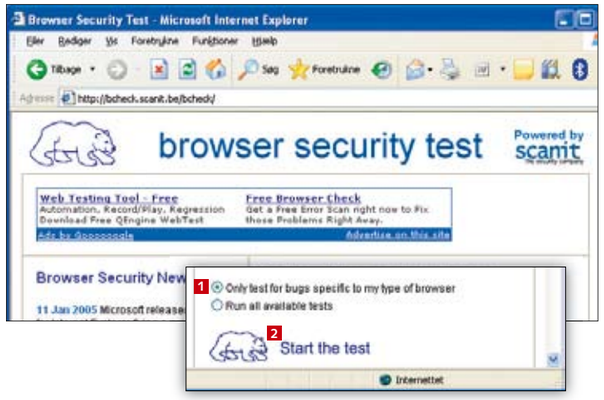


Brug stærke adgangskoder

Passwords er ofte den eneste beskyttelse mod, at dine data kommer i gale hænder. Derfor skal du anvende passwords, der er svære at gætte. Et godt password er på mindst otte tegn, består af store og små bogstaver, tal og specialtegn og er ikke et ord eller et navn. Brug forskellige passwords til forskellige tjenester.

Test browseren for sårbarheder

Uanset om du anvender *Internet Explorer* eller en anden browser, kan den være sårbar. Du kan tjekke det ved at besøge fx http://bcheck.scanit.be. Vælg **Only test for bugs specific to my type of browser** 1, og klik på **Start the test** 2. Testen åbner en del vinduer. Lad den køre færdig, før du lukker dem.



Stol ikke på afsendernavnet

Når en mail kommer fra nogen, man har tillid til, er man mindre mistænksom over for indholdet. Det udnytter de skadelige programmer på nettet. Fx udsender mail-ormen Swen mails, der angiver at komme fra MS Technical Assistance 1, altså Microsofts tekniske supportcenter. Men det er løgn. Det er let at forfalske afsenderadressen på en mail, så den kan ikke bruges til at vise, hvem mailen kommer fra.