BESKYT COMPUTEREN MOD SAMMENBRUD, VIRUS OG UBUDNE GÆSTER:

I RØG OG DAMP FOR COMPUTERENS DYD

Der raser en voldsom krig omkring computeren. System-bombemænd, virus-befængte drager og destruktive indbrudstyve kan på et øjeblik ødelægge alt for dig. Men du har faktisk en chance for at vinde krigen, hvis du skaffer dig de rigtige våben i tide.

Hvis du aldrig har tænkt over computerens sikkerhed, skal du nok få det lært. Måske den dag du må sige farvel til det 200 siders dokument, som du har arbejdet på i et halvt år. Eller den dag, din lokale computerforretning sender dig en regning på 2000 kroner for at rense din disk for virus. Katastroferne lurer overalt og kan kun undgås, hvis du har de helt rigtige våben. Det tager kun et par timer at få et system på plads, der beskytter dig mod de mest oplagte farer. Og tiden er givet godt ud.

Det basale værktøj, når det handler om sikkerhed, er en god førstehjælpskasse med sikkerhedskopier. De fleste undgår ganske vist det store sammenbrud, der som en bombe smadrer alt på computeren. Men det er ikke usædvanligt, at folk gør noget klodset som fx at overskrive en rapport med indbydelsen til en fødselsdag. Den daglige og løbende sikkerhedskopi er derfor vigtig, fordi den redder det arbejde, du har knoklet med i flere uger. Det vil naturligvis være endnu bedre, hvis du af og til tager en total sikkerhedskopi af alle programmer og dokumenter. En sådan kopi kan bringe alt tilbage til det gamle. Selv hvis en indbrudstyv er løbet med alt udstyret, kan du med den i hånden hurtigt genetablere dine data på en ny maskine. Men desværre kræver det som regel specialudstyr at sikre alle data helt. Harddisken i de nyere computere er nemlig så stor, at en total sikkerhedskopi fylder mellem 400 og 500 disketter. Der er derfor god grund til at overveje, om tusind kroner for et båndrev til sikkerhedskopiering er givet godt ud.

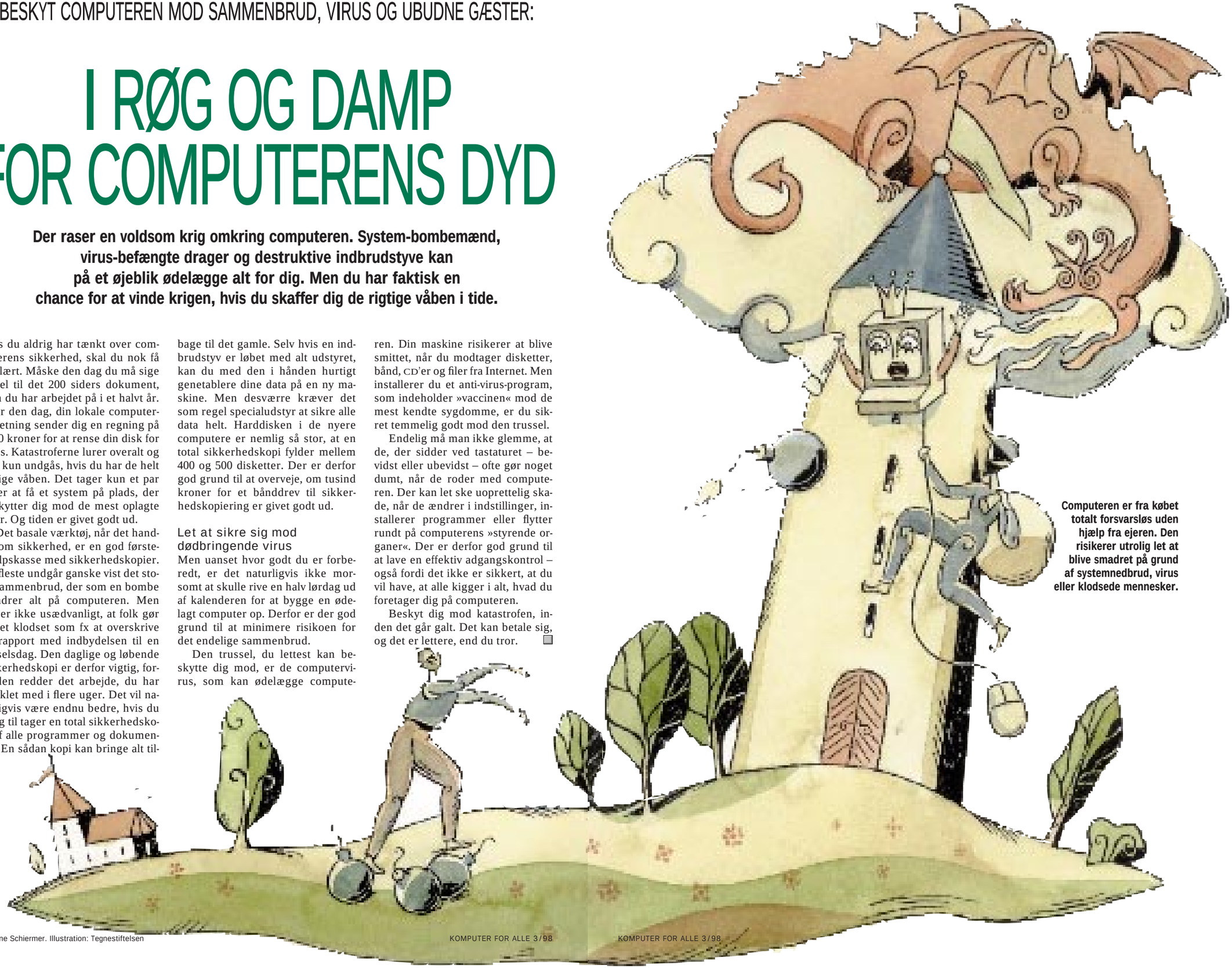
Let at sikre sig mod dødbringende virus

Men uanset hvor godt du er forberedt, er det naturligvis ikke morsomt at skulle rive en halv lørdag ud af kalenderen for at bygge en ødelagt computer op. Derfor er der god grund til at minimere risikoen for det endelige sammenbrud.

Den trussel, du lettest kan beskytte dig mod, er de computervirus, som kan ødelægge computeren. Din maskine risikerer at blive smittet, når du modtager disketter, bånd, CD'er og filer fra Internet. Men installerer du et anti-virus-program, som indeholder »vaccinen« mod de mest kendte sygdomme, er du sikret temmelig godt mod den trussel.

Endelig må man ikke glemme, at de, der sidder ved tastaturet – bevidst eller ubevidst – ofte gør noget dumt, når de roder med computeren. Der kan let ske uoprettelig skade, når de ændrer i indstillinger, installerer programmer eller flytter rundt på computerens »styrende organer«. Der er derfor god grund til at lave en effektiv adgangskontrol – også fordi det ikke er sikkert, at du vil have, at alle kigger i alt, hvad du foretager dig på computeren.

Beskyt dig mod katastrofen, inden det går galt. Det kan betale sig, og det er lettere, end du tror. □

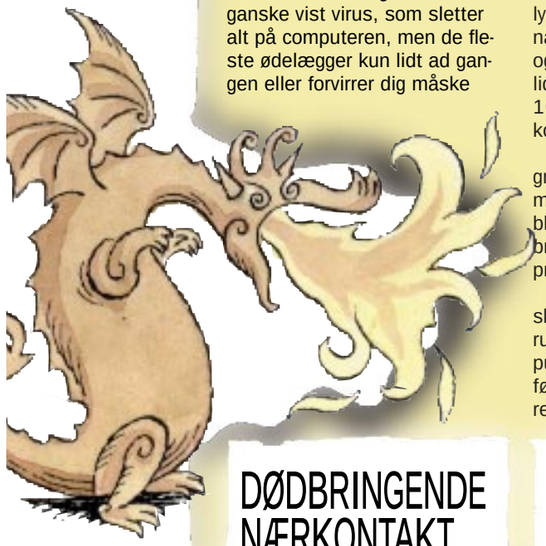


Computeren er fra købet totalt forsvarsløs uden hjælp fra ejeren. Den risikerer utrolig let at blive smadret på grund af systemnedbrud, virus eller klodsede mennesker.

Af Rune Schiermer. Illustration: Tegnestiftelsen

VACCINÉR MOD DE ØDELÆGGENDE VIRUS

Computervirus fungerer som de virus, der gør mennesker syge. De spredes dog ikke gennem luften, men fra maskine til maskine, når du flytter på dokumenter og programmer.



Et virusangreb behøver ikke altid at være alvorligt. Der findes ganske vist virus, som sletter alt på computeren, men de fleste ødelægger kun lidt ad gangen eller forvirrer dig måske ved at vise sjove billeder eller ved at få computeren til at lave en sær lyd. Alligevel bliver de en pestilens, når de først angriber, spreder sig og ødelægger din disk lidt efter lidt. Der findes i dag mindst 10.000 forskellige virus, og der kommer hele tiden nye til.

Virus er i virkeligheden små programmer, som lægger sig sammen med almindelige filer. Disse filer bliver så smittebærere, og fra dem bryder sygdommen ud, når virusprogrammet beslutter det.

Heldigvis kan du let blive beskyttet mod angreb med et anti-virus-program, der virker som computerens immunforsvar. Når det først er installeret, vil alle eksisterende filer blive tjekket, og alt, hvad der foregår, vil løbende og automatisk blive undersøgt til bunds, så langt de fleste virus ikke når at ødelægge noget. Hver måned følger sammen med *Komputer for alle* virusprogrammet »McAfee VirusScan«. Det er bygget til at holde øje med alle tænkelige former for virus. Men programmet kan ikke gardere dig mod nye typer af virus, der er blevet opfundet, efter programmet blev lavet. Men de fleste typer af virus er kendte af McAfee og bliver derfor forhindret i at angribe pc'en.

Der findes også andre gode virusprogrammer på markedet, men uanset hvor mange af dem du køber, kan du ikke vide dig sikker. Overalt i verden sidder der vandaler, der konstant udtænker nye måder at ødelægge din pc på. De har altid et forspring i forhold til de firmaer, der tilbyder vaccinen. Det mest sikre er derfor løbende at skaffe nye versioner af anti-virus-programmerne, så computeren i det mindste er beskyttet mod alle de kendte former for virus.

DØDBRINGENDE NÆRKONTAKT

Hver gang din computer kommer i kontakt med andre pc'er, bør du overveje risikoen for virus.

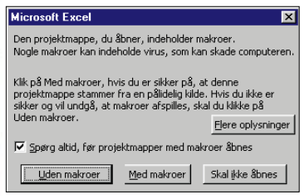
DU RISIKERER AT FÅ VIRUS, NÅR DU …

- Kigger i dokumenter, regneark med videre, der kommer fra andre computere.
- Bruger programmer fra andre computere, fx piratprogrammer og shareware.
- Tilslutter din pc et lokalt netværk. Især, hvis nettet ikke har virussikring.
- Henter programmer og andre filer fra Internettet til din computer.

DU RISIKERER IKKE AT FÅ VIRUS, NÅR DU …

- Surfer på Internet og læser eller sender elektronisk post over Internet.
- Bruger originale programmer fra en forhandler.

Der findes mange programmer til viruskontrol. Sørg for, at kun et af dem er installeret på din computer ad gangen. Ellers skaber de let konflikter og rod i din opsætning.



LYT TIL ADVARSLERNE
Mange programmer meddeler det, når du risikerer at få virus ved at gøre en bestemt handling. Hvis du er nødt til at gennemføre handlingen alligevel, så tjek først dokumentet i virusprogrammet.

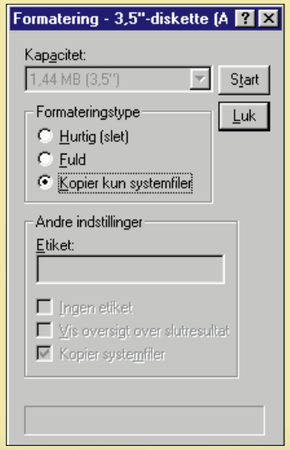
DISKETTER OG MAKROER ER DE FARLIGSTE

DISKETTER
Langt de fleste virus spredes, ved at folk udveksler de inficerede disketter med hinanden. Mange af de virus, der er designet til disketter, angriber kun, hvis du har disketten siddende i, når du tænder din pc. Det første, computeren gør, er nemlig at udføre de ordrer, der måtte ligge på diskettedrevet – også hvis ordren er at slette hele din harddisk. Derfor skal du kun lade disketter sidde i pc'en, når du bruger dem.

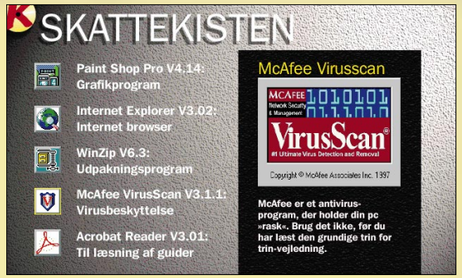
MAKROVIRUS
De almindelige virus har fået en særdeles destruktiv lillebror, som er i stærk vækst, den såkaldte makrovirus. En makro er en lille instruktion, som udløses, hvis man trykker på en bestemt tast. Det kan fx være en ordre om at kontrollere et dokument for typiske stavefejl. En makrovirus fungerer som almindelige makroer, men den beder måske computeren om at slette alt på harddisken. Bedste råd er at lytte til advarsler og virustjekke alt inden brug af dokumentet.

INSTALLER MCAFEE I DIN COMPUTER PÅ EN HALV TIME

Anti-virus-programmet McAfee er et solidt forsvar mod virus. Det ligger på K-CD'en og er let at installere. Se her, hvordan du gør.



1 FORBERED NØDDISKETTE
Du skal fra starten have en nøddiskette klar, som programmet får brug for senere. Sæt en ledig diskette i dit drev, dobbeltklik på »Denne computer«, og klik én gang på diskette-ikonet. Vælg »filer« og »formater«. Nu markerer du »kopier kun systemfiler« og trykker »start«.



2 START INSTALLATION
Nu starter du din K-CD og trykker på »Skattekisten«. Vælg »McAfee«, dernæst »Installer«. Herefter følger du blot installationsvejledningen og laver en typisk installation, som programmet foreslår, indtil programmet spørger, om det skal genstartes.

3 GENSTART COMPUTEREN
Inden programmet genstartes, skal du først »skrivebeskytte« nøddisketten. Så kan den aldrig inficeres af en virus. Flyt den lille plastictap op, så der kommer et hul igennem disketten. Gem disketten et godt sted. Ved virusangreb kan du få brug for den, fordi den rummer de nødvendige filer, der skal til for at få computeren til at starte op.

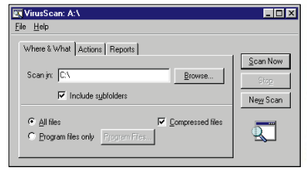
Når du bruger et virusprogram for første gang, finder det måske en virus på computeren. Den har nok ligget i lang tid på din pc, uden at du har bemærket det. Derfor kan det være meget svært at sige, hvor virusen kommer fra.

JUSTER MCAFEE TIL DINE BEHOV

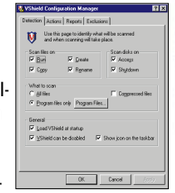
McAfee er fra starten sat op med et »skjold«, der automatisk og hele tiden holder øje med, om der kommer virus udefra. Hvis du ikke ændrer på det, kan du efter installationen slappe af. McAfee starter automatisk med Windows og fortæller dig, når noget går galt. Prisen er dog, at computeren vil køre lidt langsommere, fordi det koster kræfter at overvåge alt.

Vil du hellere bruge kræfterne på noget andet, kan du slå automatikken fra. Til gengæld skal du så selv vurdere, hvornår du laver noget farligt, og selv tjekke det. Det vil primært sige, at du selv skal tænke dig om, hver gang din computer kommer i kontakt med data udefra.

Du kan komme ind i styringen af McAfee ved at trykke på »Start«-knappen og finde McAfee i »Programmer«.



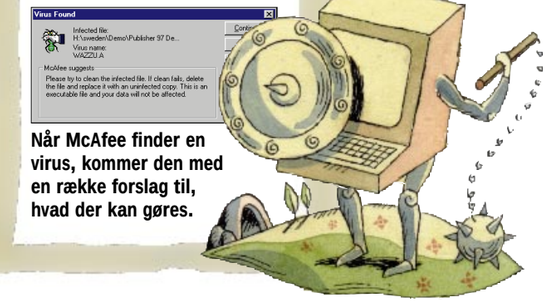
MANUELT TJEK AF DISK OG DISKETTER
Har du modtaget en CD eller diskette fra en anden computer, eller opfører din computer sig mærkeligt, er det en god idé at tage et totalt tjek på de mistænkelige drev. Gå ind i »VirusScan«. Vælg drev samt »All files«. Tryk dernæst »Scan now« for at kontrollere alt på drevet.



STANDS OG START AUTOMATIK
Du standser eller starter den automatiske kontrol ved at gå ind i »VirusScan Console«. Dobbeltklik på den blå bjælke med skjoldet i venstre side. I næste billede kan du vælge »enable« – etabler eller »disable« – fjern. Tryk »OK«.

SÅDAN KLARER DU ET ANGREB

Hvis McAfee finder en virus, så gå ikke i panik. Som regel er skaden ikke sket endnu, og du får faren væk ved at følge de råd, du får på skærmen. Hvis en alvorlig virus slipper uden om dit virusprogram, er det bedste råd at skaffe en ny version af virusprogrammet og se, om den kan fjerne den. Hjælper det ikke, kan du forsøge at fjerne de beskadigede dele. I værste fald bliver du nødt til at formatere harddisken og bygge den op fra bunden igen.



Når McAfee finder en virus, kommer den med en række forslag til, hvad der kan gøres.

LAV EN GOD NØDHJÆLPSKASSE INDEN BOMBEN RAMMER DIN PC

Sikkerhedskopiering er i bund og grund et temperamentsspørgsmål, der handler om, hvor meget du tør risikere at miste. De fleste nøjes med kopier af det vigtigste, men vil du hurtigt kunne redde en smadret pc, er det nødvendigt at have det rette udstyr.

I Windows 95 skal du ofte selv installere systemet til at tage backup i »tilføj/fjern programmer« i »Kontrolpanel« under »Indstillinger«.

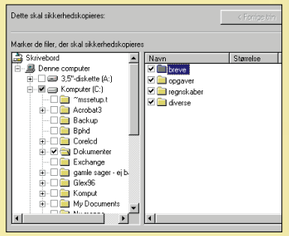
Hvis du bruger din computer meget og ofte installerer nye programmer, er der god grund til at overveje at købe udstyr til at tage en total sikkerhedskopi. Hvis du fx køber et båndrdrev, kan alt i computeren gemmes på et bånd, som hurtigt kan indlæses igen, hvis computeren bryder helt sammen. Det er bedst at lave en total, »ren« kopi straks, når den nye computer er installeret med programmer. Det skyldes, at en nyinstalleret harddisk ikke er »forurenet« med de ubrugelige ting, der ofte bliver glemt på disken af forskellige programmer. Hvis der ofte bliver installeret mange nye programmer på computeren, bør der tages en total kopi, når ændringerne er så store, at det vil være for stort et arbejde at bygge computeren fra den »rene« kopi, du tog efter købet af computeren.

En total kopi kan godt undværes, hvis du har alle dine programmer på CD-rom. Så kan computeren bygges op fra dem. Men det er ikke enkelt, og det tager lang tid at jonglere med de mange CD-rom'er og sætte programmerne op, som de var før.

Desværre er det de færreste, der har udstyret til en total kopi, og de fleste nøjes derfor med at tage en større sikkerhedskopi på disketter af de vigtigste dokumenter. Det kan for eksempel være breve, opgaver, adresser eller hjemmebyggede baner til et spil. Hvis computeren bryder totalt sammen, er alle dokumenterne parat, når den er blevet genopbygget fra totalkopien eller fra CD-rom'er med computerens programmer.

De vigtigste dokumenter gemmes i samme katalog

Den nemmeste måde at holde styr på, hvad der skal gemmes i den store kopi, er altid at have sine vigtigste dokumenter i samme katalog. I Microsoft Office ligger kataloget »Dokumenter« eller »My Documents«. Gør det til en vane altid at lægge vigtige ting der. Det er også



Det er en god idé at lægge alle de vigtigste sager i ét katalog, som der så kan tages en backup af.

en god idé på forhånd at skrive ind i kalenderen, hvornår sikkerhedskopien skal tages.

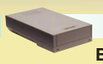
Mellem de store kopier kan alt dog stadig forsvinde. Derfor skal der tages en kopi, når et større arbejde er afsluttet. Det er ikke nødvendigt at gå vejen over backup-programmet. Med et ekstra tryk på »Gem«-tasten kan dokumentet lægges på en diskette. Disketten skal så gemmes, indtil næste gang en større kopiering får »opsnappet« de vigtige sager.

UDSTYR TIL EN HURTIG BACKUP

Der findes muligheder i alle prislag, når du skal finde det rigtige tilbehør

Mulighederne er mange, når det rette udstyr til sikkerhedskopieringen skal findes. Det billigste er klart at købe en båndstation, men når du alligevel har pengepungen fremme, er det måske en idé at købe udstyr, der også kan bruges til andre formål.

BÅND Det er en oplagt løsning at optage dine data på bånd, ikke mindst fordi et båndrev kun koster cirka 1000 kroner. Dertil kommer så båndene, der koster omkring 300 kroner stykket. Til gengæld sluger hvert bånd på ret kort tid en fuld harddisk på op til to-tre gigabyte.



BÆRBAR Det er hurtigt at tage backup på en udskiftelig harddisk, der rummer omkring to gigabyte. Den kan hurtigt tilsluttes andre computere, overalt hvor du færdes. Den største ulempe er prisen, hele 4000 kroner. For meget, hvis man ellers ikke har brug for den.

CD-ROM Du kan let brænde din backup med en CD-brænder, der også kan bruges som CD-drev i det daglige. Sådan en koster stadig 3000 kroner, men prisen er på vej ned. Når du har købt den, kan du for bare 25 kroner stykket brænde back-up'er, der rummer 650 megabyte stykket.

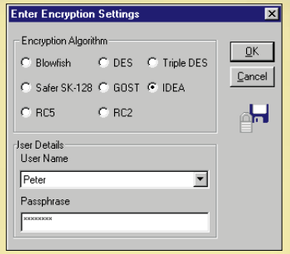
EGEN HARDDISK Du kan lave en backup af én del af harddisken og lægge kopien et andet sted på samme disk. Det er gratis og lige ved hånden. Men til gengæld er du ikke beskyttet, hvis disken svigter, eller hvis en virus spreder sig til hele disken.

DISKETTER er billige, men desværre ikke særligt velegnede til backup. De rummer kun 1,4 megabyte, hvilket svarer til 1/1000 af en nyere harddisk. De kan derfor kun anbefales til mindre backup af udvalgte data.

ZIP-DISKETTER Kan du leve med, at en almindelig harddisk fylder ti superdisketter a 100 megabyte, kan du købe et såkaldt zip-drev. Prisen er omkring 1300 kr. Dertil kommer så disketterne, der koster 100 kroner stykket. Derfor kan det godt blive en dyr løsning, hvis din harddisk er meget stor.

EKSTRA HARDDISK En billig harddisk kan købes for 1300 kr. og kan med et ekstra kabel installeres sammen med din almindelige harddisk. Ulempen er, at alt, der er fast installeret i din computer, i princippet kan risikere at få virus, så din backup er ikke helt sikker.

Foto: Ole Raffel



I månedens K-program Citadel Safstor kan computerens brugere lave kodeord på deres egne filer.

HOLD PILFINGRE OG NYSGERRIGE FRA DINE DATA

En ret overset fjende for din computer er de mange mennesker, der bruger den.

Selv om din computer ikke indeholder noget hemmeligt, er der god grund til at sikre den mod, at alle kommer til at rode med den. Flytter nogen rundt på computerens styrefiler, kan systemet let bryde sammen. Det mest oplagte våben mod pilfingre er et kodeord, som man skal kende for at få adgang til computeren. Skal mange have adgang til den, kan man i Windows 95 lave forskellige opsætninger til brugerne. Men desværre er det system ret kompliceret og ikke særlig sikkert. Det er derimod det lille program Citadel Safstor, der ligger på K-CD'en. Det ændrer indholdet efter en avanceret matematisk formel. Først når et kodeord tastes, kan dokumentet læses igen.

På trods af de tekniske muligheder skal man ikke glemme, at det letteste ofte er fysisk at gemme computeren væk for de uvelkomne gæster.

VÅBEN MOD UVENTEDE GÆSTER

BIOS PASSWORD: Skal tastes for overhovedet at køre med computeren. Det kan ikke »knækkes« uden brug af værktøj. Nederst på denne side kan du læse mere om, hvad et BIOS password er.

CITADEL SAFSTOR: På din K-CD ligger et program, som du kan bruge til at sætte koder på dine vigtigste dokumenter. Det bruger formler, som i praksis er umulige at »knække«. Alle i familien kan oprette deres egne dokumenter med egne, personlige koder.

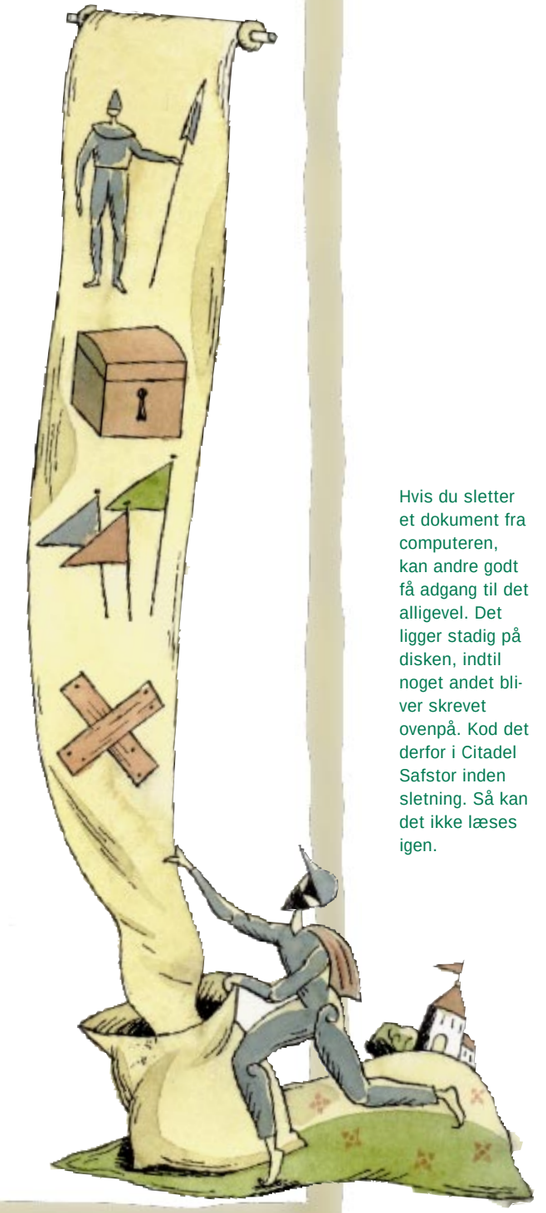
WINDOWS 95 PASSWORD: I Windows 95 kan du lave forskellige password til forskellige mennesker, så alle ikke har ret til det samme. Men ihærdige snagere kan godt komme ind alligevel.

SCREENSAVER: Din screensaver kan også bruges til at forhindre andre i at komme til. Uden et password bliver screensaveren ved med at køre på skærmen. Med lidt tålmodighed kan man dog godt bryde ind alligevel.

NØGLE: Mange computere har en nøgle, som du kan låse med, når du går. Desværre er det ret let at kortslutte forbindelsen og alligevel bryde ind på computeren.

FJERN TASTATURET: Inden for hjemmets fire vægge er det ofte nok at fjerne en enkelt del af computeren, for at børnene ikke piller ved ens vigtige data. Det mest enkle er at fjerne tastaturet.

GEM DISKETTER: Hvis du har nogle få meget private dokumenter, er det oplagt kun at arbejde med dem på disketter. Så kan du altid låse disketterne ned i en skuffe eller tage dem med dig.



Hvis du sletter et dokument fra computeren, kan andre godt få adgang til det alligevel. Det ligger stadig på disken, indtil noget andet bliver skrevet ovenpå. Kod det derfor i Citadel Safstor inden sletning. Så kan det ikke læses igen.

BIOS PASSWORD ER MEST EFFEKTIVT

De fleste computere tilbyder at lave et password i den såkaldte BIOS-enhed. BIOS indeholder også oplysninger om computerens diske og andre enheder, og den holder styr på klokken og datoen. Grunden til, at tiden altid passer, er, at BIOS bruger et lille batteri. Fjernes det, mister computeren de nødvendige oplysninger for at kunne starte op. Vil du have et BIOS password, bør du bede en computerforhandler sætte det op, for selv om det kun tager fem minutter at lave, risikerer du let at lave en alvorlig fejl, der er svær og dyr at rette igen.