# GJENNOM ILD OG VANN FOR DATAMASKINENS VEL

**Der raser en voldsom krig omkring datamaskinen. Systembombemenn, virusbefengte drager og destruktive innbruddstyver kan på et øyeblikk ødelegge alt for deg. Men du har faktisk en sjanse til å vinne krigen hvis du skaffer deg de riktige våpnene i tide.**

Hvis du aldri har tenkt noe særlig over datasikkerhet, vil du nok lære det. Kanskje den dagen du må si farvel til det 200-siders dokumentet du har jobbet med i et halvt år. Eller den dagen dataforretningen sender deg en regning på 2000 kroner for å rense disken din for virus. Katastrofene lurer over alt, og kan bare unngås hvis du har de riktige våpnene. Det tar bare et par timer å få et system på plass som beskytter deg mot de mest innlysende farene. Og det er vel anvendt tid.

Det basale verktøyet når det er snakk om sikkerhet, er et godt førstehjelpsskrin med sikkerhetskopier. Riktignok unngår de fleste et totalt systemsammenbrudd, som lik en bombe ødelegger alt på datamaskinen. Men det er ikke uvanlig at folk gjør en feil som f.eks. å overskrive en rapport med en fødselsdagsinvitasjon. Den daglige og løpende sikkerhetskopien er derfor viktig, fordi den redder det arbeidet du har strevd med i flere uker. Det ville naturligvis være enda bedre hvis du av og til tar en fullstendig sikkerhetskopi av alle programmene og dokumentene. En slik kopi vil kunne få alt tilbake til det gamle. Selv om en innbruddstyv har stukket av med alt utstyret, kan du med sikkerhetskopien i hånden gjenopprette dataene dine på en ny maskin. Men dessverre krever det som regel spesialutstyr å sikre dataene helt. Harddisken på nyere datamaskiner er nemlig så stor, at en fullstendig sikkerhetskopi vil kreve mellom 400 og 500 disketter. Kanskje en bør overveie om det kunne lønne seg å investere en tusenlapp eller to i en båndstasjon.

## Lett å sikre seg mot dødelige virus

Men uansett hvor godt du er forberedt, er det ikke morsomt å skulle rive en halv lørdag ut av kalenderen for å bygge opp en ødelagt datamaskin. Derfor er det gode grunner til å minimere risikoen for det endelige sammenbruddet.

Den trusselen du lettest kan beskytte deg mot, er de datavirusene som kan ødelegge datamaskinen. Maskinen risikerer å bli smittet når du mottar disketter, bånd, CD-er og filer fra Internett. Men installerer du et antivirusprogram som inneholder "vaksinen" mot de mest kjente sykdommene, er du ganske godt sikret mot den faren.

Man skal heller ikke glemme at de som sitter ved tastaturet – bevisst eller ubevisst – ofte gjør noe dumt når de sitter og tukler med maskinen. Det kan lett skje uopprettelig skade når de endrer innstillinger, installerer programmer eller flytter rundt på datamaskinens "styrende organer". Man bør derfor lage en effektiv adgangskontroll – også fordi du vil hindre andre i å se hva du foretar deg på datamaskinen.

Beskytt deg mot katastrofen før det går galt. Det kan lønne seg, og det er lettere enn du tror. □

**En nyinnkjøpt datamaskin er totalt forsvarsløs uten hjelp fra eieren. Den risikerer total utslettelse på grunn av systemkræsj, virus eller klossete mennesker.**

Illustrasjon: Tegnestiftelsen

# VAKSINER MOT LIVSFARLIGE VIRUS

**Datavirus fungerer som de virusene som gjør mennesker syke. De spres ikke gjennom luften, men fra maskin til maskin når du flytter på dokumenter og programmer.**

Et virusangrep behøver ikke alltid å være alvorlig. Riktignok finnes det virus som sletter alt på datamaskinen, men de fleste ødelegger bare litt om gangen, eller kanskje de forvirrer deg ved å vise artige bilder eller får maskinen til å lage merkelige lyder. Likevel er de en pest og en plage når de først angriper, sprer seg og ødelegger disken litt etter litt. Det finnes i dag minst 10 000 forskjellige virus, og det kommer hele tiden nye.

Virus er i virkeligheten små programmer som legger seg sammen med vanlige filer. Disse filene blir så smittebærere, og det er fra disse sykdommen bryter ut når virusprogrammet bestemmer det.

Heldigvis kan du beskytte deg mot angrep med et antivirusprogram, som fungerer som datamaskinens immunforsvar. Når det først er installert, vil alle eksisterende filer bli kontrollert, og alt som skjer vil automatisk og kontinuerlig bli undersøkt til bunns slik at de fleste virus ikke rekker å gjøre noen skade. Hver måned følger virusprogrammet "McAfee VirusScan" med *Komputer for alle*. Det er lagd for å holde øye med alle tenkelige former for virus. Men programmet kan ikke gardere deg mot nye typer av virus som er blitt oppfunnet etter at programmet ble lagd. Men de fleste virustypene er kjent for McAfee og blir derfor hindret i å angripe PC-en.

Det finnes også andre gode virusprogrammer på markedet, men uansett hvor mange av dem du kjøper, kan du ikke være helt sikker. Overalt i verden sitter det vandaler som kontinuerlig tenker ut nye måter å ødelegge PC-en din på. De har alltid et forsprang i forhold til firmaene som tilbyr vaksinen. Det sikreste er derfor hele tiden å skaffe nye versjoner av antivirusprogrammene så maskinen i det minste er beskyttet mot de kjente virusene.

## DØDBRINGENDE NÆRKONTAKT

Hver gang maskinen din kommer i kontakt med andre PC-er, bør du vurdere risikoen for virus.

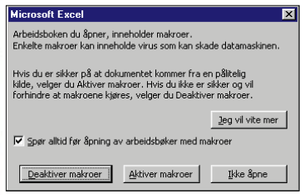
**DU RISIKERER Å FÅ VIRUS NÅR DU …**

- Ser på dokumenter, regneark osv. som kommer fra andre datamaskiner.
- Bruker programmer fra andre maskiner, bl.a. piratprogrammer og shareware.
- Kobler PC-en til et lokalt nettverk. Særlig hvis nettet ikke har virussikring.
- Henter programmer og andre filer fra Internett og ned på maskinen din.

**DU RISIKERER IKKE Å FÅ VIRUS NÅR DU …**

- Surfer på Internett og leser eller sender elektronisk post over Internett.
- Bruker originale programmer fra en forhandler.

Det finnes mange programmer til viruskontroll. Sørg for at du bare har ett av dem installert på PC-en om gangen. Ellers skaper de lett konflikter og rot i konfigurasjonen.




**LYTT TIL ADVARSLENE**

Mange programmer gir beskjed om det når du risikerer å få virus ved å gjøre en bestemt handling. Hvis du er nødt til å utføre handlingen likevel, så sjekk først dokumentet i virusprogrammet.

## DISKETTER OG MAKROER ER DE FARLIGSTE

**DISKETTER**

De aller fleste virus spres ved at folk utveksler de infiserte disketter med hverandre. Mange av de virusene som er utviklet til disketter, angriper bare hvis du har disketten stående i maskinen når du slår den på. Det første maskinen gjør, er nemlig å utføre de kommandoene som måtte ligge i diskettstasjonen – også hvis ordren er å slette hele harddisken. Derfor skal du bare ha disketter i PC-en når du bruker dem.

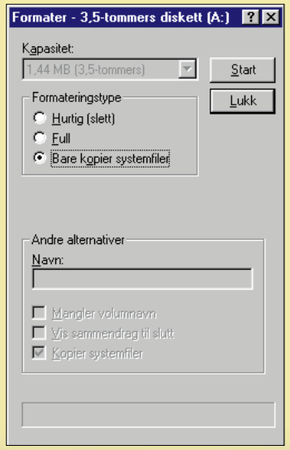
**MAKROVIRUS**

De vanlige virusene har fått en særdeles destruktiv lillebror som er i sterk vekst, en såkalt makrovirus. En makro er en liten instruksjon som utløses når man trykker på en bestemt tast. Det kan f.eks. være en ordre om å kontrollere et dokument for typiske stavefeil. Et makrovirus fungerer som vanlige makroer, men det ber kanskje datamaskinen om å slette alt på harddisken. Det beste rådet er å lytte til advarsler, og virussjekke alt før du bruker dokumentet.



# INSTALLER MCAFEE PÅ DATAMASKINEN PÅ EN HALV TIME

**Antivirusprogrammet McAfee er et solid forsvar mot virus. Det ligger på K-CD-en og er lett å installere. Les hvordan det gjøres.**




**1 FORBERED NØDDISKETT**

Du bør fra starten ha en nøddiskett klar som programmet får bruk for senere. Sett en tom diskett i stasjonen, dobbeltklikk på "Min datamaskin" og klikk én gang på diskettikonet. Velg "Fil" og "Formater". Velg "Bare kopier systemfiler", og klikk deretter på "Start".


**2 START INSTALLERINGEN**

Nå starter du K-CD-en og trykker på "Skattkisten". Velg "McAfee" og deretter "Installer". Nå følger du bare installasjonsveiledningen og foretar en vanlig installasjon slik programmet foreslår, til programmet spør om det skal startes på nytt.

**3 START PC-EN PÅ NYTT**

Før programmet startes på nytt, må du først "skrivebeskytte" nøddisketten. Da vil den aldri bli infisert av virus. Flytt den lille plasttappen opp så det blir et "hull" i disketten. Oppbevar disketten på et trygt sted. Ved et ev. virusangrep kan du få bruk for den fordi den inneholder de nødvendige filene som skal til for å starte opp datamaskinen.

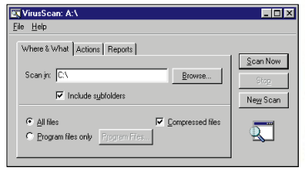
Når du bruker et virusprogram for første gang, finner det kanskje et virus på datamaskinen. Det har nok ligget der en stund uten at du har merket noe til det. Derfor kan det være vanskelige å si hvor viruset kommer fra.

## JUSTER MCAFEE TIL DINE BEHOV

McAfee er i utgangspunktet utstyrt med et "skjold" som kontinuerlig holder øye med om det kommer virus utenfra. Hvis du ikke endrer på det, kan du ta det helt med ro etter installasjonen. McAfee starter automatisk med Windows og forteller deg når noe går galt. Men prisen er at datamaskinen jobber litt langsommere fordi det tar på kreftene å overvåke alt.

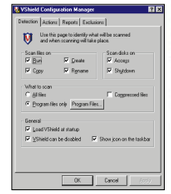
Hvis du heller vil bruke kreftene på noe annet, kan du slå av automatikken. Til gjengjeld må du selv vurdere når du gjør noe risikabelt, og kontrollere det selv. Det vil primært si at du må tenke deg om hver gang datamaskinen kommer i kontakt med data utenfra.

Du kan endre innstillingene i McAfee ved å trykke på "Start"-knappen og finne McAfee i "Programmer".




**MANUELL KONTROLL AV DISK OG DISKETTER**

Har du mottatt en CD eller diskett fra en annen maskin, eller oppfører maskinen seg merkelig, er det en god idé å ta en helsjekk av de mistenkelige stasjonene. Gå inn i "VirusScan". Velg stasjon samt "All files". Klikk deretter på "Scan now" for å kontrollere alt på stasjonen.

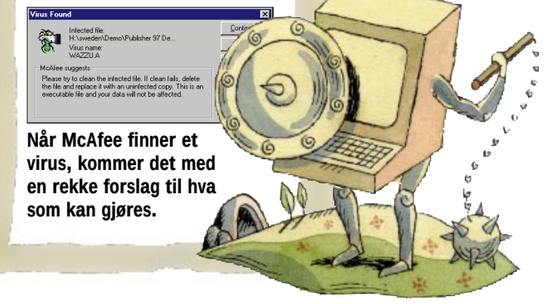



**STOPP OG START AUTOMATISK**

Du stanser eller starter den automatiske kontrollen ved å gå inn i "VirusScan Console". Dobbeltklikk på det blå symbolet med skjoldet på venstre side. I neste bilde kan du velge "enable" (aktiver) eller "disable" (fjern), og OK.

## SLIK TAKLER DU ET ANGREP

Hvis McAfee finner et virus, så ikke få panikk. Som regel er ikke skaden skjedd ennå, og du unngår faren ved å følge rådene du får på skjermen. Hvis et alvorlig virus slipper gjennom viruskontrollen, er det beste rådet å skaffe en ny versjon av virusprogrammet, og se om den kan fjerne det. Hjelper ikke det, kan du forsøke å fjerne de ødelagte områdene. I verste fall blir du nødt til å formatere harddisken og bygge den opp fra bunnen av.




**Når McAfee finner et virus, kommer det med en rekke forslag til hva som kan gjøres.**

# LAG ET GODT FØRSTEHJELPSSKRIN FØR BOMBEN TREFFER PC-EN DIN

**Sikkerhetskopiering er i bunn og grunn et spørsmål om temperament. Det handler om hvor mye du våger å risikere å miste. De fleste nøyer seg med kopier av det viktigste, men vil du raskt kunne redde en ødelagt PC, er det nødvendig å ha det riktige utstyret.**

I Windows 95 må du ofte selv installere systemet til å ta sikkerhetskopi med. Fra Start-menyen velger du "Innstillinger", "Kontrollpanel" og "Legg til/fjern programmer".

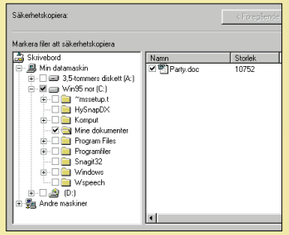
Hvis du bruker datamaskinen mye og installerer nye programmer ofte, bør du vurdere å kjøpe alt utstyret som kreves for å ta en fullstendig sikkerhetskopi. Hvis du f.eks. kjøper en båndstasjon, kan du lagre alt du har på maskinen på et bånd, som fort lar seg lese inn igjen hvis datamaskinen bryter helt sammen. Det beste er å lage en "ren" kopi straks den nye datamaskinen er installert med programmer. Det er fordi en nyinstallert harddisk ikke er "forurenset" med all slags ubrukelige ting som ofte blir lagret på disken av forskjellige programmer. Hvis det ofte blir installert nye programmer på maskinen, bør det tas en fullstendig sikkerhetskopi når endringene er så omfattende at jobben med å bygge opp maskinen fra den "rene" kopien du tok da maskinen var ny, blir for stor.

En fullstendig sikkerhetskopi kan unnværes hvis du har alle programmene på CD-rom. Da kan datamaskinen bygges opp fra dem. Men det er ikke enkelt, og det tar lang tid å sjonglere med alle CD-rom-ene og sette opp programmene slik de var før.

Dessverre er det de færreste som har utstyr til en fullstendig kopi, og de fleste nøyer seg derfor med å ta en større sikkerhetskopi av de viktigste dokumentene på disketter. Det kan for eksempel være brev, oppgaver, adresser eller hjemmebygde baner til et spill. Hvis datamaskinen bryter helt sammen, vil alle dokumentene være intakt når den blir gjenoppbygd fra sikkerhetskopien eller fra CD-rom-ene med programvaren.

## De viktigste dokumentene lagres i samme katalog

Den enkleste måten å holde styr på hva som skal lagres i den store kopien, er å ha de viktigste dokumenten i samme katalog. I Microsoft Office ligger katalogen "Dokumenter" eller "My Documents". Gjør det til en vane å alltid




**Det er en god idé å legge de viktigste sakene i samme katalog, som det så tas en backup av.**

legge viktige ting der. Det er også en god idé å skrive inn i kalenderen på forhånd når sikkerhetskopien skal tas.

Ting kan imidlertid forsvinne mellom sikkerhetskopieringene. Ta derfor en kopi når du avslutter en jobb. Det er ikke nødvendig å gå veien om backupprogrammet. Med et ekstra klikk på "Lagre"-tasten kan dokumentet legges på en diskett. Disketten settes bort til neste gang en større kopiering får "snappet opp" det viktigste.

## UTSTYR TIL EN RASK BACKUP

**Det finnes muligheter på alle prisnivåer når du skal finne det riktig tilbehøret**

Mulighetene er mange når du skal finne det rette utstyret til sikkerhetskopieringen. Det billigste er å kjøpe en båndstasjon, men når du allikevel har lommeboken framme, er det kanskje en idé å kjøpe utstyr som også kan brukes til andre formål.

**DISKETTER** er billige, men dessverre ikke særlig velegnet til backup. De tar bare 1,4 megabyte, hvilket tilsvarer 1/1000 av en nyere harddisk. De kan derfor bare anbefales til mindre sikkerhetskopier av utvalgte data.

**BÅND** Det er en nærliggende løsning å kopiere dataene over på bånd, ikke minst fordi en båndstasjon bare koster cirka 1500 kroner. Båndene kommer i tillegg, og de koster omkring 350 kroner stykket. Til gjengjeld kan du på kort tid kopiere over en full harddisk på to–tre gigabyte.

**BÆRBAR** Det går fort å ta backup på en utskiftbar harddisk som har plass til omtrent to gigabyte. Den er lett å koble til andre datamaskiner uansett hvor du ferdes. Den største ulempen er prisen, omkring 4000 kroner. For mye hvis du ikke har bruk for den ellers.

**CD-ROM** Du kan lett brenne en sikkerhetskopi med en CD-brenner, som også kan brukes som CD-stasjon til vanlig. En slik koster fra kr 3500, men prisen er på vei ned. Når du har kjøpt den, kan du for bare 40 kroner stykket brenne sikkerhetskopier som rommer 650 megabyte stykket.

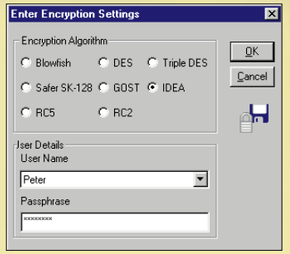
**EGEN HARDDISK** Du kan lage en sikkerhetskopi av en del av harddisken og legge kopien et annet sted på samme disk. Det er gratis. Men til gjengjeld er du ikke beskyttet hvis disken svikter, eller hvis et virus sprer seg til hele disken.

**ZIP-DISKETTER** Kan du leve med at en vanlig harddisk tar ti superdisketter á 100 megabyte, kan du kjøpe en såkalt zip-stasjon. Prisen er fra kr 1500. I tillegg kommer disknettene, som koster ca. 120 kroner stykket. Hvis du har en svært stor harddisk, kan dette bli en dyr løsning.

**EKSTRA HARDDISK** En billig harddisk fås fra kr 2000, og med en ekstra kabel kan den installeres på den vanlige harddisken. Ulempen er at alt som er fast installert i maskinen, i prinsippet kan risikere å få virus, så sikkerhetskopien er ikke helt sikker.

Foto: Ole Raffel






**I månedens K-program, Citadel Safstor, kan brukerne lage passord til sine egne filer.**

# HOLD KLÅFINGRER OG NYSGJERRIGE UNNA DATAENE

**En oversett fiende for PC-en din, er alle menneskene som bruker den.**

Selv om du ikke har noe hemmelig liggende på maskinen, kan det være en idé å sikre den mot at alle og enhver kan rote rundt i filene dine. Hvis noen går inn og flytter på styrefilene, kan systemet lett bryte sammen. Det mest nærliggende våpenet mot klåfingrer er et passord som man må kunne for å få tilgang til datamaskinen. I Windows 95 er det mulig å lage forskjellige oppsett for brukerne. Men dessverre er dette systemet ganske komplisert, og ikke særlig sikkert. Det er derimot det lille programmet Citadel Safstor, som ligger på K-CD-en. Det endrer innholdet etter en avansert matematisk formel. Først når du har skrevet inn kodeordet, får du tilgang til dokumentet.

Til tross for de tekniske mulighetene, bør man ikke glemme at det letteste ofte vil være å gjemme datamaskinen rent fysisk for uvelkomne gjester.

## VÅPEN MOT UVENTEDE GJESTER

**BIOS-PASSORD:** Må skrives inn for at datamaskinen kan starte. Passordet lar seg ikke "knekke" uten bruk av verktøy. Nederst på denne siden kan du lese mer om hva et BIOS-passord er.

**CITADEL SAFSTOR:** På K-CD-en ligger et program som du kan bruke til å sette inn koder i de viktigste dokumentene. Det bruker formler som i praksis er umulige å "knekke". Alle i familien kan opprette sine egne dokumenter med egne, personlige koder.

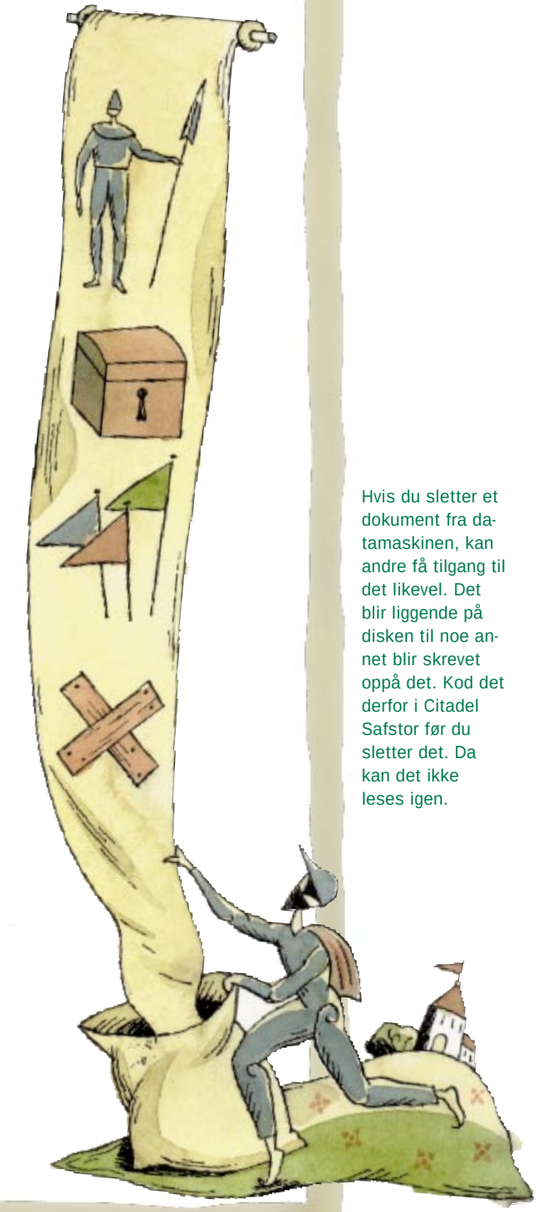
**WINDOWS 95-PASSORD:** I Windows 95 kan du lage forskjellige passord til forskjellige mennesker, slik at ikke alle har tilgang til det samme. Men iherdige snokere kommer likevel inn.

**SKJERMBESKYTTER:** Skjermbeskytteren kan også brukes til å hindre andre i å komme til. Uten et passord blir skjermbeskytteren værende på skjermen. Men med litt tålmodighet kan man klare å bryte seg inn likevel.

**NØKLER:** Mange datamaskiner har en nøkkel som du kan låse med når du går. Dessverre er det ingen sak å kortslutte forbindelsen og bryte seg inn i maskinen.

**FJERN TASTATURET:** Innenfor husets fire vegger er det ofte nok å fjerne en del av maskinen for at barna ikke får tilgang til viktige data. Det enkleste er å fjerne tastaturet.

**GJEM DISKETTER:** Hvis du har noen få, meget private dokumenter, bør du jobbe med dem på disketter. Da kan du alltid låse diskettene ned i en skuff eller ta dem med deg.



Hvis du sletter et dokument fra datamaskinen, kan andre få tilgang til det likevel. Det blir liggende på disken til noe annet blir skrevet oppå det. Kod det derfor i Citadel Safstor før du sletter det. Da kan det ikke leses igen.

## BIOS-PASSORD ER MEST EFFEKTIVT

I de fleste datamaskiner har du muligheten til å lage et passord i den såkalte BIOS-enheten. BIOS inneholder også opplysninger om disker og andre enheter til datamaskinen, og den holder styr på klokken og datoen. Grunnen til at tiden alltid stemmer, er at BIOS bruker et lite batteri. Fjernes det, mister maskinen de nødvendige opplysningene for å kunne starte opp. Vil du ha et BIOS-passord, bør du be en dataforhandler sette det opp, for selv om det bare tar fem minutter å gjøre det, risikerer du å gjøre en alvorlig feil som kan blir dyr å rette.