Hvad du bør vide om computervirus

er en pjece for dig, der vil vide,
hvordan du undgår virus.
Du finder også information om, hvad du skal gøre,
når skaden er sket.

Du skal sikre dig mod virus, fordi:

- du risikerer at miste dine data
- du risikerer at dine private data misbruges på internettet
- du risikerer at smitte andres pc'er

Derfor er det vigtigt, at du har
et antivirusprogram på din computer
og husker at opdatere det.

IT- og Telestyrelsen
www.itst.dk

Rådet for it-sikkerhed
www.raadetforitsikkerhed.dk

Hvad du bør vide om computervirus

IT- og Telestyrelsen
Ministeriet for Videnskab
Teknologi og Udvikling

RÅDET FOR IT-SIKKERHED

IT- og Telestyrelsen
Holsteinsgade 63
2100 Kbh. Ø

Telefon 3545 0000
Telefax 3545 0010
E-post: itst@itst.dk
www.itst.dk

Rådet for it-sikkerhed
www.raadetforitsikkerhed.dk

Redaktion:
IT- og Telestyrelsen
Grafisk tilrettelæggelse: Gitte Blå Design
Tryk: Schultz Grafisk

Hvad du bør vide om computervirus

Mere end hver fjerde dansker har haft problemer med computervirus.

Hvad er computervirus?

Ordet virus er en generel samlebetegnelse for en række programmer, der kan skade din computer. Her kan du læse om de vigtigste former, som ordet virus dækker over.

Bagest i pjecen finder du en ordliste med forklaringer på de mest almindelige ord, der knytter sig til computervirus.

Virus

En computervirus er et program, der er i stand til at kopiere sig selv og sprede kopierne til andre computere. En computervirus er afhængig af noget, der bærer den videre til en anden computer. Det kan være et program eller en fil, som den skjuler sig i. Virus kan desuden bære et skadeligt indhold, der betyder, at den for eksempel kan slette filer eller give fremmede adgang til den ramte computer.

Orme

En orm er mere selvstændig end den traditionelle virus, fordi den ikke er knyttet til et program eller en fil. Ormen spreder sig selv over det netværk, som computeren er tilkoblet. Det kan både være det lokale netværk eller internettet. Da ormen er afhængig af en forbindelse over et netværk, er servere de mest udsatte, fordi de som regel har fast forbindelse til nettet.

I dag har flere og flere hjemmecomputere bredbåndsforbindelse til internettet i form af ADSL eller et kabelmodem. Det betyder, at hjemmecomputere ligesom servere kan være på internettet hele tiden, og at de er mere udsatte for ormeangreb.

E-post-baserede orme

De mest udbredte orme er en mellemting mellem traditionelle orme og virus. Disse orme er kendetegnet ved, at de spredes via e-post. De ankommer i form af en e-post, der indeholder en vedhæftet fil. Hvis modtageren dobbeltklikker på filen, aktiveres ormen, og den sender sig selv videre til alle de adresser, den finder på computeren.

Makrovirus

Nogle programmer anvender makroer, der er små programstykker til at udføre en række handlinger i programmet. Det er ofte tekstbehandlings- eller regnearksprogrammer, som fx MS Word og MS Excel, der anvender makroer.

En makrovirus er en virus, der bæres af en makro. Når først et dokument er ramt af makrovirus, vil virus blive spredt til alle de dokumenter, du herefter åbner på computeren med tekstbehandlings- eller regnearksprogrammet. Bliver dokumentet åbnet på en anden computer, bliver den også ramt. På den måde spreder makrovirus sig.

Trojansk hest

En trojansk hest er et program, der ikke er, hvad det giver sig ud for at være. Det vil sige, at den forklæder sig som et andet program.

En trojansk hest vil udføre uønskede handlinger, som oftest er af skadelig karakter. Programmet kan fx være et spil eller et gratis program, du har downloadet fra internettet. Nogle trojanske heste efterlader en "bagdør" på computeren, som kan give en hacker adgang til computeren. Hermed har hackeren mulighed for at overtage kontrollen med computeren, kopiere og slette dokumenter eller ændre den på anden vis.

Hackere og virus er to begreber, der ofte følges ad. Hackeren kan anvende en virus til at overføre en trojansk hest til en anden computer, så hackeren kan få adgang til den.

Hoax

Hoax betyder spøg eller svindelnummer. En hoax er altså ikke en egentlig virus eller et program, men en falsk advarsel i en e-post om en virus, der ikke findes. E-posten kan indeholde en beskrivelse af virus og en vejledning til, hvordan du fjerner den. Hvis du følger vejledningen, bliver du måske bedt om at fjerne en vigtig fil eller programdel på din computer. Hvis du gør det, virker computerens styresystem måske ikke længere.

E-posten er sandsynligvis sendt af nogen, du kender. En hoax spredes ved, at folk i god tro sender advarslen videre. En hoax kan fx have en tekst, hvor der står noget i retning af: "Send straks denne advarsel videre til alle dine venner".

I august 2003 oplevede verden det værste virusangreb indtil nu. I Danmark blev mange virksomheder og institutioner ramt og bombarderet med beskeder med virus. Det resulterede i ekstrem langsom elektronisk postgang og deciderede nedbrud. Også private brugeres pc'er blev påvirket. Den 20. august filtrerede TDC 350.000 inficerede elektroniske beskeder fra i timen.

Hvorfor får du virus?

Mange virus eller orme udnytter sårbarheder og sikkerhedshuller i den almindelige software, vi anvender. De fleste programmer fungerer udmærket, selvom der er sikkerhedshuller i dem.

Dem, der skriver virus, er interesserede i at få spredt virus til flest mulige computere. Derfor leder de bevidst efter sikkerhedshuller i de mest brugte programmer, som fx Windows, Internet Explorer og Outlook. I dag findes der programmer, der skanner internettet for computere med de sårbarheder, en hacker ønsker at udnytte.

Hvis du har fået virus eller en orm, der giver adgang til din computer, kan konsekvenserne være meget forstyrrende eller endda katastrofale. Du kan risikere at miste vigtige data, som enten virus eller hackeren sletter. Du kan også risikere, at virus via e-post sender tilfældige dokumenter fra din computer til personer i din elektroniske adressebog. I værste fald kan din computer blive udnyttet til kriminelle aktiviteter, fx som lager for ulovlige billeder eller musikfiler.

I øjeblikket er tendensen, at lige så hurtigt softwareproducenterne får lukket sikkerhedshullerne i softwaren, lige så hurtigt finder hackerne eller "virus-bagmændene" et nyt hul. Derfor er det vigtigt, at du opdaterer dine programmer lige så snart, der kommer en ny opdatering. Se afsnittet om opdatering.

Hvordan får du virus?

Alt, hvad der kommer ude fra og ind i din computer, kan være kilde til virus. Det kan være e-post, besøg på hjemmesider, cd'er og disketter.
I dag er det e-post, der er skyld i langt hovedparten af virusangreb. Hvis du får tilsendt en e-post med virus, kan den sprede sig lynhurtigt til alle i din adressebog på computeren. Der er eksempler på virus, der har spredt sig jorden rundt på få minutter.

De fleste virus spreder sig via e-post

I nogle af de e-post skal du først klikke på en vedhæftet fil for at aktivere virus. I andre tilfælde er det nok, at e-postens indhold vises automatisk, uden at man har åbnet den.
Hvis du får en virus, der sender sig selv til personer i din adressebog på computeren, vil dine venner og bekendte få en virusramt e-post med dig som afsender. Der er måske større chance for, at de vil aktivere virus i en e-post fra nogen, de kender. Ofte er virus' afsenderadresse eller tekst i emnelinjen medvirkende til, at den bliver åbnet og aktiveret.
For eksempel vil en e-post fra en kollega med titlen "I LOVE YOU" nok vække interesse hos de fleste.

Spam

En særlig type e-post, der også kan medføre virus, kaldes spam. Spam er e-post, du ikke har bedt om at få, og som reklamerer for alverdens ting lige fra pornohjemmesider til "billige" lån. Spam sendes ud i uhyre store mængder til vilkårlige modtagere. Den, der

udsender spam, har programmer, der skanner internettet for e-postadresser, så de kan opsamle millionvis af e-postadresser. Det nyeste påfund er at udsende spam med virus, der kan få andre folks computere til selv at udsende spam.

Det er ulovligt at udsende spam i Danmark. Du kan klage over spam til forbrugerombudsmanden på www.fs.dk.

Filer fra internettet

Har du adgang til internettet, har du også mulighed for at downloade filer. Hvis du er uheldig, kan disse filer indeholde virus. Det kan være noget så uskyldigt som et tekstbehandlings-dokument, som indeholder en makrovirus.
Du kan også downloade programmer, der i virkeligheden indeholder en trojansk hest, uden at det kan ses.
Der findes også hjemmesider, hvor du får virus bare ved at besøge dem. På nogle hjemmesider kan du få en besked, der ligner en advarsel fra Windows-systemet, og ligegyldigt om du trykker OK, JA eller NEJ starter et program, som er en virus.

Brug din sunde fornuft

Der er desværre ikke nogen metoder eller produkter, der kan sikre dig 100 procent mod virusangreb. Selvom det er vigtigt at beskytte sig med antivirusprogrammer og firewalls, afhænger sikkerheden også meget af din adfærd.

Opmærksomhed..

Det første, du skal gøre for at beskytte dig selv mod virus og hackere, er at være opmærksom på problemet. Opmærksomhed og gode vaner er vigtigt, når du bruger internettet og computeren. Du kan sammenligne det med at færdes i trafikken. Her er lovlydige trafikanter, men også farlige, og det er livsvigtigt at være opmærksom både for din egen og for andres skyld.
Plejer du ikke at få e-post fra nogen, der skriver på engelsk, bør du være på vagt, hvis du får en e-post, hvor emnet står på engelsk. Også selvom den er fra én, du kender.

Forhold dig kritisk til det du modtager!

Der er ofte nyheder i pressen om virus og hackere, og det kan give dig nyttige forholdsregler om din gøren og laden på internettet. Det er også let at finde nyheder og advarsler på nyhedstjenester på internettet. Virus og hackere ændrer nemlig strategi og metode hele tiden. Derfor er det vigtigt at følge med i, hvordan den aktuelle "virussituation" ser ud. Se afsnittet "Mere information".

**Det er ikke kun dig, det går ud over, hvis du bliver ramt af virus – virus kan sprede sig fra din computer til mange andre.
Så beskyt dig selv og alle andre!**

Forebyggelse - antivirus

Det er en god idé at have et antivirusprogram kørende på computeren. Et antivirusprogram er en fornuftig investering i forhold til, hvad en computer koster, og hvad informationer og data er værd. Også af hensyn til de personer, som du har kontakt med over internettet. Der findes mange forskellige antivirusprodukter på markedet. Når en ny virus opdages, laver antivirusproducenten en opdatering, der indeholder et filter, som beskytter også mod den virus. Som regel kan antivirusprogrammet på computeren selv hente en opdatering over internettet. Du er først beskyttet, når du har installeret opdateringen på din computer. Du bør derfor opdatere dit antivirusprogram ofte.

Forebyggelse - personlig firewall

Det er en god idé at supplere antivirus med en personlig firewall. Det er et program, der lukker for uønsket trafik ind og ud af computeren. Det kan hjælpe til at holde hackere ude af din computer. Nogle antivirusprodukter indeholder også en personlig firewall. Følger der ikke en firewall med i det antivirusprodukt, du har valgt, kan du finde ganske gode og gratis produkter på internettet. Det er dog vigtigt, at du anvender pålidelige kilder.

Opdatering

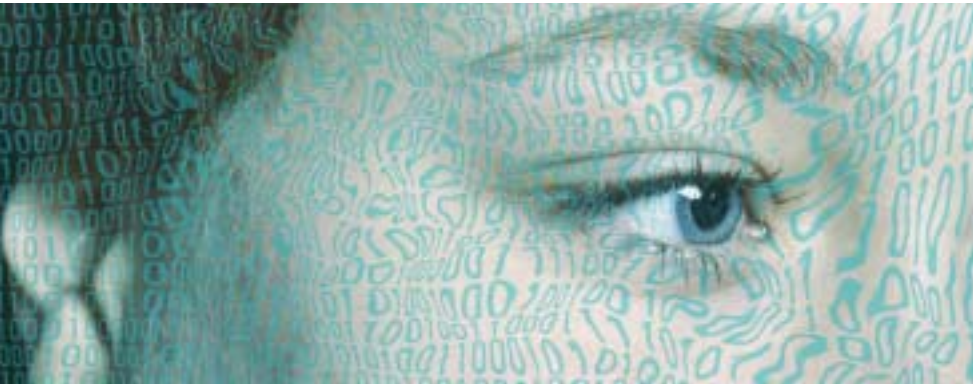
Som tidligere nævnt udnytter virus og hackere sikkerhedshuller i programmerne. Og det er ofte de mest udbredte programmer, hvor hackerne prøver at finde sikkerhedshuller. Derfor er det vigtigt, at du får "lappet" de huller, der er. De fleste softwareproducenter yder den service, at du kan downloade opdateringer via internettet fra producentens hjemmeside. Det er en meget vigtig forebyggelse mod angreb.

Tag en kopi af dine data

Det er en god idé at gemme vigtige data, som fx billeder og dokumenter, på en cd eller på disketter, så du stadig har dem, hvis noget på computeren slettes. Det er bare vigtigt, at der ikke også er virus på cd'en eller disketterne. Det skal gerne være en indarbejdet rutine, at du tager backup (kopi af data), før du får virus. Tag derfor backup regelmæssigt og gem den, så du har en backup, der er virusfri.

Du kan aldrig være 100 procent sikker på at undgå virusangreb. Efterhånden sker ormeangrebene så hurtigt, at antivirusprogrammer ikke når at blive opdateret. De er dog stadig vigtige at have, så gamle virus og orme på internettet bliver opdaget.

Når skaden er sket



Hvis uheldet er ude, og du får virus, kommer skadens omfang meget an på, hvilken type virus du har fået, hvilket styresystem du har, og hvilket antivirusprodukt du har.

De værktøjer, der skal til for at reparere eller geninstallere computeren, skal være klar inden virusudbruddet, hvis det skal gå hurtigt med at få computeren op at køre igen.

Det første, du kan gøre, er at prøve, om virus kan fjernes igen. De fleste antivirusproducenter sørger for, at deres antivirusprogram også kan fjerne virus fra ramte computere. Det er vigtigt at følge antivirusproducentens anvisninger, hvis du prøver det.

Nogle virus er ikke så skadelige og er lette at fjerne igen. Andre er næsten umulige at rydde op efter, og det kan betyde, at du bør geninstallere alt på computeren.

Hvad enten du vil forsøge at fjerne virus på computeren, eller om du vil geninstallere computeren, skal computeren have været slukket først, da en virus kan "overleve" i computerens hukommelse. For at være sikker på, at den er fjernet, er det nødvendigt at slukke computeren, inden du påbegynder en reparation eller geninstallation. Kontroller efter installationen for virus igen, så du er sikker på, at den er helt renset.

Har du geninstalleret computeren, skal du vurdere, om der er en risiko for, at virus stadig findes på backup'en, inden du indlæser den. Det er under alle omstændigheder vigtigt at installere og opdatere antivirusprogrammet som noget af det første, inden du flytter dine data tilbage på computeren.

Mere information på danske hjemmesider

DK-CERT: Overvåger it-sikkerheden i Danmark som en del af et internationalt samarbejde. **www.cert.dk**

IT- og Telestyrelsen: Er en del af Ministeriet for Videnskab, Teknologi og Udvikling. **www.itst.dk**

Rådet for it-sikkerhed: Rådet for it-sikkerhed er et uafhængigt råd nedsat med det formål at styrke it-sikkerhed-sniveauet i Danmark. Her kan du finde råd og vejledning. **www.raadetforitsikkerhed.dk**

Datatilsynet: Tager sig af beskyttelse af persondata. **www.datatilsynet.dk**

TDC: Portal om it-sikkerhed. Bliv alarmeret via e-post eller sms, når der er store virusudbrud. **www.sikkerhed.tdconline.dk**

Cybercity: Hjælp til sikkerhed på internettet. **www.cybercity.dk/privat/produkter/sikkerhed**

EMU: Elektronisk mødested for undervisningsverdenen. **www.emu.dk**

Symantec: Antivirusproducent hvor du også kan finde information om virus. **www.symantec.dk**

Windows Update: Henter de sikkerhedsopdateringer din computer mangler, hvis du bruger Windows. **www.windowsupdate.com**

Ordliste

Backup En sikkerhedskopi af data, som er gemt på et andet medie, fx disketter eller cd'er.

Downloade At hente filer eller programmer ned fra internettet.

Fil En samling data lagres i en fil. Et Word-dokument er fx en fil.

Firewall Et program, der lukker for uønsket trafik ind og ud af computeren.

Hacker En person, der "bryder ind" på en computer eller et netværk.

Hoax En e-post, som advarer om en virus, der ikke findes.

Makrovirus En virus, som skader dokumenter, der anvender makroer.

Orm En "virus", der er i stand til at sprede sig selv uden brugerens medvirken, og som udnytter sikkerhedshuller i computerens styresystem.

Server En computer, der servicerer andre computere.

Spam E-post, du ikke har bedt om at få, som reklamerer for alverdens ting.

Styresystem	Det program, som styrer computeren, fx Windows eller Linux.
Trojansk hest	Et program, som udadtil ser harmløst ud, men som i virkeligheden har en skadelig effekt på computeren, eller som kan lukke en hacker ind af en "bagdør". Ordet trojansk hest er lånt fra den græske mytologi, hvor Odysseus smugler dele af sin hær ind i Troja i en kæmpe hest af træ, hvorefter han erobrer Troja.
Virus	Skadeligt program, der kopierer og spreder sig selv.

Gode råd

- [ ] Kør altid et antivirusprogram på din computer
- [ ] Sørg for, at antivirusprogrammet opdateres automatisk
- [ ] Hav en personlig firewall
- [ ] Slet e-post fra ukendte afsendere uden at læse dem
- [ ] Slet e-post uden at læse dem, hvis teksten i emnelinjen ikke giver nogen mening, ser underlig ud eller undtagelsesvis er på engelsk
- [ ] Vær forsigtig med hjemmesider, der vil have dig til at gøre noget
- [ ] Vær forsigtig med hjemmesider, e-post og filer, der ser specielle ud
- [ ] Vær forsigtig med programmer, du får tilsendt, eller du finder på suspekte hjemmesider
- [ ] Indtast aldrig din e-postadresse på hjemmesider, du ikke har tillid til
- [ ] Opdater dine programmer ofte
- [ ] Tag backup af vigtige filer regelmæssigt
- [ ] Hav installationsdisketter eller cd'er klar til enhver tid
- [ ] Følg med i pressen
- [ ] Brug din sunde fornuft