

Jordnær virusvejledning

- om computervirus og andre skadelige programmer

Internettet er en fantastisk opfindelse, men træerne gror ikke ind i himlen, og desværre findes der efterhånden mange trusler for PC-brugerne. De mest kendte og farligste trusler er virus og orme. Det er små programmer som spreder sig som en forkølelse i din computer. Men lige som man kan beskytte sig mod forkølelse og mod at smitte andre med forkølelse, kan man også beskytte sig mod virus og orme.

Det særlige problem ved mange af disse skadelige programmer, er at de spreder sig fra din computer til andre computere, uden at du ved det. For at undgå at gøre skade på andre, bør du derfor ubetinget have et ajourført antivirusprogram. Alt andet vil være ansvarsløst.

Det er lige som at køre bil: man skal have kørekort, og man skal bruge sikkerhedsseler.

I de senere år er der dukket andre trusler op: spam, spyware, hackere phishing mv.

Denne vejledning fortæller grundigt om virus og informerer om de andre PC-trusler. Vejledningen henvender sig til begyndere på området, og der er henvisninger til gode steder på Internettet, hvis man godt vil vide lidt mere.

Fælles for de fleste skadelige programmer er, at de laves af computernørder, enten for sjov ("drengestreger"), for at vinde anerkendelse blandt venner eller fordi man har trang til at være til skade for andre. En særlig computertrussel udgøres af "hackere", dvs. computer nørder, som bryder ind på din computer mens du er på nettet og ødelægger programmer, data eller læser f.eks. pasord til din bank. Men med spyware og phishing er der tale om egentlige forbrydelse, hvor personer forsøger at stjæle dine penge eller at lokke dem fra dig.

Virus kommer som regel med en mail eller hvis du besøger useriøse hjemmesider.

Indhold

[Hvad er virus?](#)

[Hvordan undgår man virus?](#)

[Hvad skal man gøre hvis man alligevel har fået virus](#)

[Hvor køber man antivirusprogrammer?](#)

[Microsoft Outlook og Outlook Express](#)

[Firewall](#)

[Andre trusler](#)

Hvis du vil vide mere:

TDC: <http://sikkerhed.tdconline.dk/>

Symantec: <http://www.symantec.com/avcenter/index.html>

It-leksikon: <http://www.it-leksikon.dk/>

Virus112: <http://www.virus112.com>. Her kan du også tegne abonnement på nyhedsbreve om virus.

Hvad er virus?

Her omtales de mest almindelige virusvarianter: "rigtig" virus, trojanske heste, orme og hoaxer.

Fælles for alle virusser er, at de smitter ved at du afvikler et program eller åbner et dokument på din computer. Angreb kan altså ske på lige så mange måder, som du kan få et program eller et dokument ind på din maskine.

Den mest almindelige angrebsform er nok kopiering af programmer via disketter eller cd-rommer, samt e-mails eller download fra internettet. Men nogle få typer virus kan faktisk trænge ind på din computer, hvis du blot besøger en hjemmeside på internettet, som indeholder ondsindet kode.

Virus

Virus er et lille program, som kopierer sig selv til din computer, så den er aktiv, hver gang computeren er tændt, eller kopierer sig selv til nogle programmer, hvor den venter på at blive aktiveret. Nogle virustyper spreder sig til almindelige dokumenter - for eksempel Word-dokumenter og regneark - og gør dermed din computer meget smittefarlig. Virus kan være en harmløs "øv-bøv"-besked på din skærm, men det kan også være programmer, som ødelægger filer på harddisken. Den såkaldte Tjernobyli-virus ligger f.eks. tålmodigt på din computer og venter på, at datoen skal skifte til 26. april. På den dato i 1986 nedsmeltede en ukrainsk atomreaktor, og på den dato udløses Tjernobyli-computervirusen med det resultat, at harddisken bliver slettet uden varsel - altså en digital "nedsmeltning".

Trojanske heste

En trojansk hest er, som navnet antyder, et program, der ikke er, hvad det udgiver sig for at være. Ofte vil det være en lille sjov animation (f.eks. et julekort eller et lille spil), som du modtager som vedhæftet fil i en e-mail. Én af de mest kendte trojanske heste er Back Orifice. Når du aktiverer programmet, har du hentet den trojanske hest inden for murene. "Hesten" venter nu på at blive kontaktet udefra. Måske sker der slet ingenting, men du risikerer nu, at en hacker opdager, at din trojanske hest står og venter på forbindelse. Sker det, vil hackeren kunne forbinde sig til din computer og overtage kontrollen, fuldstændig som hvis han selv sad ved tastaturet.

Orme

En orm (engelsk: worm) er i grunden ikke en virus, men det er et skadeligt program, som automatisk videregiver sig selv til andre computere via dit e-mailsystem. Den mest kendte er vel "**I love you**", som ramte brugere af Microsoft-programmet Outlook ved at videresende sig selv til alle, der stod i modtagerens adressebog. Og for nylig har Badtrans og BugBear vist været overalt. De nye orme er meget elegante: de sætter en forkert afsenderadresse på. Så du kan roligt gå ud fra, at den person som står som afsender på mailen med ormen til dig, ikke selv har sendt mailen.

Foruden at videresende sig selv kan orme have samme skadelige egenskaber som en almindelig virus.

Hoax

Der fjerde slags computervirus er i virkeligheden slet ikke en virus men en fup-virus. De kaldes for hoax'er (engelsk for spøg, svindelnummer, fup).

En typisk hoax kommer fra en ven eller en forretningsforbindelse som har modtaget den fra en anden ven eller forretningsforbindelse. Den advarer f.eks. mod en virus, som slet ikke eksisterer og opfordrer til at sende advarslen videre til alle i dit adressekartoteket. Og af lutter hjælpsomhed sender vi så dette ligegyldige mail til alle vi kender. Spredningen er værre end et kædebrev.

Særligt udspekulerede personer bruger hoaxes til at indsamle en masse e-mail-adresser, fordi beskederne jo bliver videresendt. Adresserne bliver senere brugt til at tæppebombe ("spamme") folk med uopfordrede reklamer. Men oftest opnår man ikke andet end at sprede unødige skræk, spilde en masse menneskers tid og belaste computernetværkene.

For nylig har hoaxen sulfnbk.exe hærgnet. Den indeholder en komplet vejledning på hvordan du kan slette en angiveligt farlig fil. I virkeligheden sletter du en vigtig fil som dit system skal bruge.

En særlig sød hoax-variant er Den Norske Virus. Mailen lyder sådan:

"You have just received a Norwegian virus. Since we are not so smart in Norway, this is a MANUAL virus. Please delete all the files on your hard disk yourself and send this mail to everyone you know. Thank you very much for helping me. Ole Hacker"

Hvordan undgår man virus?

Der findes ingen metode, som med ét skud kan tage livet af alle typer computervirus, så det kan godt betale sig at være lidt paranoid.

Forebyg computervirus:

1. **Vær kritisk over for e-mails.** Luk kun e-mail op, hvis de kommer fra personer du kender eller har tillid til. Du skal aldrig åbne vedhæftede filer med disse extension (de sidste 3 bogstaver efter punktum): ".BAT", ".COM", ".EXE", ".LNK", ".PIF", ".VBS" eller 2 extensions "filnavn.xxx.xxx". f.eks. "Hej Tonny.doc.com" eller "Hej Tonny.doc.pdf" osv. Slet disse mails med det samme.
2. **Installér et antivirusprogram.** Der findes utallige programmer. Nogle er gratis, andre koster penge. Nogle er en kombination, hvor du downloader programmet gratis fra nettet, mens det koster penge i form af et abonnement at holde det opdateret. Se afsnittet Hvor køber man antivirusprogrammer? Det er bedre at have et gratis antivirusprogram end slet ikke noget antivirusprogram.
3. **Hold dit antivirusprogram opdateret, ellers opnår du en falsk tryghed.** Der laves hele tiden nye computervirusser, så det er et evigt kapløb mellem "de gode" og "de onde". De gode programmer holder sig automatisk opdateret via internettet. Hvis du opdaterer manuelt, skal du gøre det mindst én gang om ugen.
4. **Hold dine programmer opdaterede med seneste rettelser fra producenten.** Microsoft har eksempelvis udsendt mange af opdateringer, som forbedrer sikkerheden i Windows, Internet Explorer, Office-pakken og Outlook
5. **Indsæt kun disketter og cd-rommer i din computer, hvis du har tillid til indholdet.** Risikoen for at få virus fra en original programdisk er nærmest ikke-eksisterende sammenlignet med risikoen for at få virus fra en cd-rom med et piratkopieret spil eller en diskette, som har gået på omgang blandt vennerne.
6. **Tænk dig om, før du downloader et program fra nettet.** Har du tillid til den hjemmeside, som du henter programmet fra?
7. **Hvis du er sikker på, at dine disketter er fri for virus, så skrivbeskyt dem ved at åbne den lille skydeknop foran hullet i disketten ene hjørne.**
8. **Tag backup!** Det er så uendeligt trist at miste alle sine breve fra moster Gerda, eksamensopgaverne og alle billederne fra turen til Rhodos...
9. **Vær sikker på, at du har en opstartsdiskette** - på engelsk "boot disk", som ikke indeholder virus (opstartsdisketterne følger for det meste med, når du køber en computer). Skrivbeskyt disketten/disketterne. Du kan få brug for dem, hvis computeren bliver inficeret.
10. **Undgå at surfe på hjemmesider der virker useriøse i sit indhold**
11. **Lad være med at svare på spam og junkmail,** heller ikke hvis afsenderen beder dig afmelde mailen. Så ved afsenderen nemlig at han har ramt en aktiv adresse, og du hænger først for alvor i fedtefadet.
12. **Vær kritisk over for sikkerhedsadvarsler.** De er som regel falske eller en virus i sig selv og de kommer som hovedregel fra dine velmenende venner, som skynder sig at videresende advarslen, inden de selv har sat sig ind i, om den er seriøs.
13. **Hæv evt. sikkerhedsindstillingen på din browser.** Dette kan desværre medføre at du ikke længere kan se visse hjemmesider. Da samtidig denne risiko efter min mening er ret lille, har jeg personligt valgt at stille mit sikkerhedsniveau til "mellem". Til gengæld er jeg hysterisk omhyggelig med at ajourføre mit antivirusprogram.
14. **Undgå masseudsendelse af mails med vedhæftede dokumenter.** Også excell- og word-dokumenter kan indeholde virus. Mange foreninger har for eksempel deres egen kommunikationshjemmeside, som bruges til blandt andet referater, så man ikke behøver at sende vedhæftede mails til medlemmerne. Hvis I ikke har jeres egen portal, så brug f.eks. den gratis www.groupcare.dk.
15. **Fjern adresser fra gamle mails, eller slet mailene.** En del virusser gennemløber simpelthen hele din computer for adresser, som virus'en automatisk kan sprede sig til, når du er på internettet.

Hvad gør jeg hvis jeg har fået virus?

Man må ubetinget følge disse 3 regler:

1. undlade at koble sig på internettet overhovedet indtil problemet er løst
2. anskaffe sig et antivirusprogram.
3. lave en antivirus scanning ved hjælp af sit nye program.

Dette vil sandsynligvis løse 98% af problemerne. Men nogle virusser er meget ondsindede, og det kan være nødvendigt at tage sin PC ned i den lokale computershop for at få hjælp til at klare situationen. I værste fald er der kun ét at gøre: slet og reformater hele harddisken og indlæg programmer og data igen. Man kan godt tage sikkerhedskopi af virusbefængte data, idet det ikke volder de store problemer at scanne for virus i data. Der er derfor absolut ingen grund til f.eks. at slette alle mails, som en af mine gode bekendte var blevet rådet til af en "klog" men velmenende mand.

Problemet opstår hvis der også kommer virus i programmerne og især hvis der kommer virus i Windows systemfilerne.

En god nødløsning er at bruge en af de mange gratis on-linescannere som efterhånden findes på nettet, f.eks. Stinger fra <http://mcafee.dk/>

Der findes et hav af antivirusprogrammer, men Norton fra firmaet Symantec og McAfee er de mest udbredte. Jeg bruger selv Norton, som jeg varmt kan anbefale

Desværre bruger antivirusfirmaerne ikke altid samme benævnelse på den samme virus.

Hvor køber man antivirusprogrammer?

Du må som nævnt ubetinget skaffe et antivirusprogram. Jeg bruger selv Norton fra Symantec.

Man køber programmer i computerbutikker, i radioforretninger (Merlin, Fona etc.) eller i specialiserede post-ordrefirmaer. Bemærk: vejledningen i radioforretninger kan være af meget blandet kvalitet. Vælg et sted hvor du kan få vejledning (spørg dig for hos venner eller kolleger).

Personligt handler jeg hos KP Data i Aabenraa, MJ Software tlf. 86 26 16 88 eller hos www.it-butikken.dk.

Sammen med programmerne får du en installationsvejledning. Følg den.

Men en ting er at installere et antivirusprogram. Noget andet er den løbende ajourføring. Én gang om ugen skal du kontrollere om der er kommet nye antivirusser, som du skal downloade. De gode nyere antivirusprogrammer, gør dette helt automatisk (du skal dog selv indstille hvor tit du vil ajourføre).

Microsoft Outlook og Outlook Express

Outlook og Outlook Express er verdens mest udbredte mail-systemer. Derfor er de også viruskonstruktørers foretrukne "legeplads".

Men der er blandt fagfolk også en vis opfattelse af at Microsoft sjusker med sikkerheden og derfor hele tiden har behov for at udsende opdateringer ("patches") til sine programmer. Opdateringerne er gratis og det er vigtigt at følge med i disse hele tiden på <http://windowsupdate.microsoft.com/>,

Mange mener at disse Microsoft problemer er så store, at det er bedst at undgå Outlook og Outlook Express. Men der er blandt fagfolk måske en lille religionskrig her: for eller imod Microsoft.

Der findes gode, gratis e-mailprogrammer, som ikke er nær så udsat som Microsofts, for eksempel Netscape, som kan downloades fra <http://home.netscape.com/download/index.html?cp=errdwn>, men det nemmeste er at købe et computerblad, f.eks. Datatid, hvor der er indlagt en CD-rom med mange nyttige programmer.

Firewall

I forbindelse med fast opkobling til internettet via bredbånd (ADSL) er det også vigtigt at beskytte sig mod hacker-angreb. Hackere er – lige som grafittimalere og virus-konstruktører – også sabotører og balademagere, som ønsker at gøre skade – eller måske blot at have det sjovt eller at prale blandt kammerater.

Hackere skaffer sig adgang til din computer mens du er koblet på nettet, og de kan læse data på din computer, f.eks. adgangskoder.

Man beskytter sig mod hackere ved hjælp af en såkaldt "firewall".

Ligesom for antivirus-programmer findes der et hav af firewall-programmer. Blandt de mere kendte programmer er Tiny Personal Firewall (gratis) og BlackICE Defender.

Mange routere har indbygget firewall, hvilket overflødiggør et firewall-program.

Efter min egen mening er Firewall kun nødvendigt hvis du har en fast opkobling, - men entusiaster vil sikkert hævde at det også er nødvendigt hvis du er meget på nettet via ISDN eller almindeligt modem.

Øvrige trusler

Spam

Spam er masseudsendelse af enslydende data til modtagere, der ikke på forhånd har sagt 'Ja, tak' til at modtage. Det kan være om alt, lige fra overflødige kopier af referater på din arbejdsplads, til masseudsendelse af reklamer for pornografiske hjemmesider og medicin.

Udsendelse af spam-mails er forbudt i hele EU, men er fx tilladt i USA.

"Spam" er det Engelsk ord for dåseskinke - udødeliggjort af Monthly Python i sketchen, hvor der indgår dåseskinke i alle retter.

Spam kaldes ofte også for junkmail, som betegner e-mail som modtageren ikke har bedt om, men som afsenderen blot sender til alle tilgængelige E-post-adresser.

Adware

Programmer, som i det skjulte indsamler personlige oplysninger om din internettrafik – typisk besøgsstatistikker - og videresender disse til andre med henblik på markedsføring af bestemte ydelser. De downloades typisk med shareware-programmer, free-ware programmer eller instant messengers men kan også lægge sig på din PC fra både tilsyneladende seriøse og iøjnefaldende useriøse hjemmesider.

Se mere på <http://www.spywarefri.dk/>

Beskyt dig ved hjælp af f.eks. Ad-aware fra <http://www.javasoft.de>

Spyware

Spyware er i familie med spyware, men af grovere karakter. Spyware indsamler dine tasteoperationer, og personlige oplysninger om din internettrafik, f.eks. adgangskoder eller anden fortrolig information. De downloades typisk med shareware-programmer, free-ware programmer eller instant messengers. og kan misbruges til alt muligt

Beskyt dig ved hjælp af f.eks. Ad-aware fra <http://www.javasoft.de>

Læs mere på <http://www.spywarefri.dk/>

Malware

Malware er også i familie med adware, men er kendetegnet ved at det lægger skadelige programmer på din PC, for eksempel pornosider, som det er stort set umuligt at fjerne.

Læs mere på <http://www.spywarefri.dk/>

Dialer

Et program, som uden din tilladelse kalder op til bestemte telefonnumre, typisk til afsindigt høje priser.

Beskyt dig ved hjælp af f.eks. Ad-aware fra <http://www.javasoft.de>

Phishing

Phishing er sammensat af de engelske ord "fishing" og "phony" Fishing betyder fiskeri eller "lade sig lokke" Phony betyder falsk. Phishing er på godt dansk: Bondefangeri på nettet.

Et eksempel: Man modtager en mail, fra det man tror, er sin bank. I mailen står der, at man skal opdatere eller bekræfte kontoinformationer ved at følge et medleveret link. Klikkes på linket kommer man om til bankens

hjemmeside. Det tror man i hvert fald, men den er forfalsket, hvilket er meget svært at se. Indtaster man kodeord og brugernavn, sker ulykken. Nu står kontoen åben for personer med onde hensigter.

Læs mere på <http://www.spywarefri.dk/>