

# Virus, spyware, spam og så videre....

## Hvad er det ?

### **Virus:**

Selve ordet "virus" stammer fra den medicinske verden, hvor en virus er mikroorganismer, der ikke er i stand til at formere sig alene, men er nødt til at invadere en værtscelle og overtage dens maskineri for at kunne lave flere viruspartikler.

En computervirus er grundlæggende det samme, nemlig et program, der gør noget ved din computer, som du helst er fri for, og som du ikke har bedt den om.

Ofte er virussen gemt i et program eller en mail. Virus kan være en harmløs besked på din skærm, men det er desværre ofte programmer, som ødelægger filer på din PC.

En virus kan kopiere sig selv til dine systemfiler, så den er aktiv, hver gang computeren er tændt. Den kan også kopiere sig selv til andre programfiler. Nogle typer spreder sig endda til almindelige dokumenter som for eksempel Word dokumenter og regneark.

Virusen kan ødelægge dine filer, men selve hardwaren tager ikke skade. Værste fald er at alt software skal installeres forfra. Undtagelsen er en virus, der kan ødelægge din BIOS chip, hvilket kan medføre at chippen skal udskiftes.

### **Spyware:**

Spyware er software, der sender informationer om dine internetvaner videre til tredjeperson uden brugerens (din) viden. Tredjepersonen (ofte underlødige reklame- og marketings-firmaer) kan herefter foretage en målrettet reklameindsats mod brugeren, ofte i form af irriterende pop-up reklamer.

Afsender kan også have mere ondsigtede hensigter, som at aflure dine passwords osv. Vi er så ovre i det vi kalder "malware".

### **Browser Hijacker:**

Programmer som kan ændre din startside eller fodre dig med pop-up reklamer. Udefra kommende kræfter overtager mere eller mindre kommandoen over din pc.

### **Dialere:**

Programmer som ringer op til tjenester uden at du er klar over det. Er kun et problem hvis man bruger modem. Altså intet problem på ADSL.

### **Spam:**

Spam er uopfordret reklame e-mail. Afsenderen har på en eller anden måde opfanget ens e-mail adresse f. eks. gennem søgt websider, nyhedsgrupper eller registreret et besøg.

"Spammeren" sender ofte hundrede eller tusinder spammails af sted af gangen. Normalt er afsenderen af en spam mail ikke en gyldig e-mail-adresse, derfor kan og bør man ikke skrive tilbage og klage over spam. Det kan i de værre tilfælde gå ud over en række uskyldige personer, som svaret er sat til at gå til.

### **Phishing:**

En afart af spam hvor man forsøger at udgive sig for et legitimt foretagende - typisk en bank

eller Microsoft - for at lokke modtagerne til at indtaste personlige oplysninger, f. eks. ens bankkonto.  
Her er der alene tale om svindel.

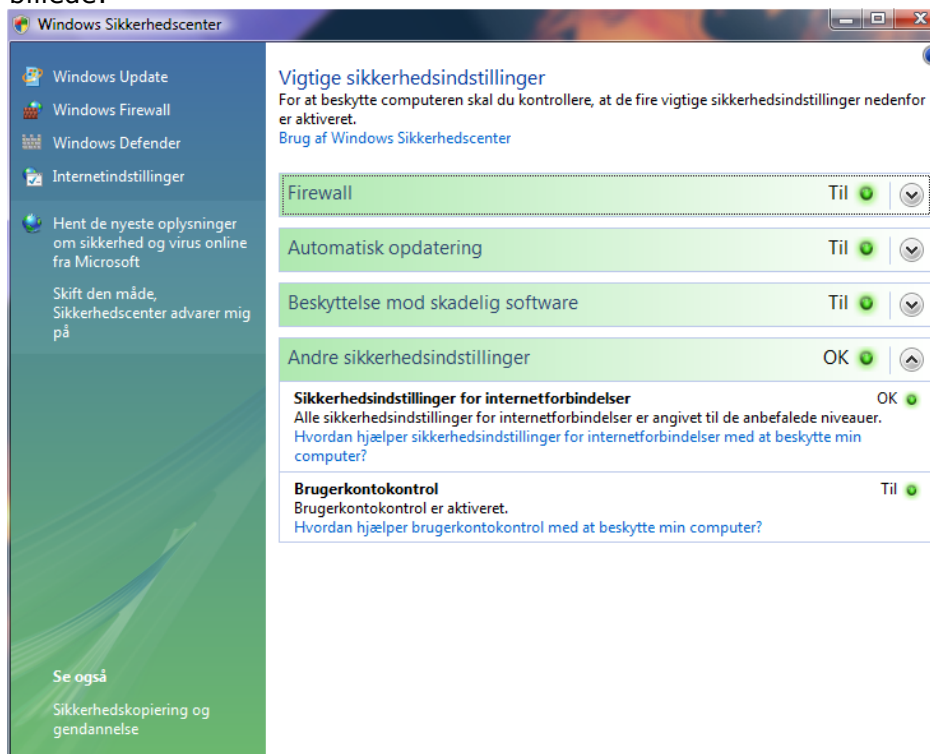
## Og hvordan bekæmper man det så?

Grundlæggende skal du have fem ting i orden på din computer:

1) Et Antivirus program. Det kan være Bullguard, Panda eller en af de mange varianter der findes. De virker ved at skanne alle programmer der kører, alle filer du skriver eller læser fra, alle mails osv. For altid at være opdateret (så de kender de nyeste virustyper) er det vigtigt at du holder det opdateret. De fleste klarer selv dette når du starter maskinen op. De fleste koster penge (typisk ca. 300 kr. pr. år) mens enkelte er gratis for private. Bemærk dog at du får hvad du betaler for. De gratis giver slet ikke samme beskyttelse som de kommercielle.

Personligt bruger jeg Bullguard, men også andre er gode.

2) En firewall. Den sikre at der kun foregår kommunikation på din internetforbindelse, som du har givet lov til. Check at den er slået til i "Kontrolpanel" - "Sikkerhedscenter", hvorefter du får dette billede:



Her skal der ud for Firewall stå "Slået til".

I mange af sikkerhedspakkerne f.eks. fra Symantec, Norman, Bullguard mv. er der inkluderet en firewall. De er alle langt bedre end Windows version, men de koster jo også penge.

Windows 7 og Vista har begge en OK firewall indbygget, mens Windows XP ikke har (der er godt nok en, men den dækker ikke tilfredsstillende).

Bruger du Mac eller Linux findes der også gode indbyggede firewalls.

3) Et program til at checke for Spyware. Igen er dette incl. i de gode beskyttelsesprogrammer som Bullguard, Panda eller McAfee. Windows har indbygget Windows Defender, som er en minimumsløsning.

4) Du skal sikre at Windows henter opdateringer automatisk. Microsoft finder løbende "huller" i programmerne og retter disse, så det er vigtigt at dit system er up-to-date.

5) Du skal sikre at alle andre programmer er opdateret. F.eks. finder hackerne tit huller i Adobe Reader, Sun Java, eller lignende. Disse skal derfor også være up to date, så flest muligt fejl er rettet.

Et alternativ er at undlade de værste. F.eks. findes gode alternativer til Adobe Reader, f.eks. Foxit Reader, der er langt mindre og langt hurtigere.

Og endelig skal du altid bruge din sunde fornuft!

- Åben aldrig mail fra personer du ikke kender.
- Sker det alligevel, så klik aldrig på links i sådanne mails, uanset hvor fristende det kan være. I så fald ved de nu at du læser deres skidt... og du får endnu mere...
- Sig aldrig ja til at installere noget fra en Internet side, med mindre du er 100 % sikker på hvad det er.
- Din bank (eller Microsoft for den sags skyld) udsender ALDRIG information via mails, så svar aldrig på sådanne mails. Er du det mindste i tvivl, så ring til banken inden du svarer.

Vil du læse mere om emnet, kan jeg anbefale [www.spywarefri.dk](http://www.spywarefri.dk) der er en meget omfattende side om emnet.

Læs mere:

[www.spywarefri.dk](http://www.spywarefri.dk) eller  
[www.firewallguide.com](http://www.firewallguide.com)