TI GOD RÅD OM IT-SIKKERHED

Til den private pc-bruger, der har en pc med internetadgang.

1. Installer et antivirusprogram og hold det opdateret.
2. Installer en firewall.
3. Opdater pc'ens styresystem og hold det opdateret.
4. Installer et antispywareprogram.
5. Installer et spamfilter.
6. Dobbeltklik aldrig på vedhæftede filer i mails.
7. Følg ikke tilsendte links til banker og betalingstjenester.
8. Brug browserens sikkerhedsindstillinger.
9. Pas på programmer, du henter via internettet.
10. Brug hovedet.

1. Installer et antivirusprogram og hold det opdateret
Et antivirusprogram beskytter pc'en mod to typer trusler: Virus og mail-orme. En virus er et skadeligt program, der inficerer et uskadeligt program. Når brugeren kører programmet, aktiveres virussen, der så prøver at smitte andre programmer på pc'en. Nogle virus sletter data, mens andre nøjes med at sprede sig.

Mail-orme er skadelige programmer, der spreder sig via e-mail (se også godt råd nummer 6). En mail-orm ankommer som en mail med en vedhæftet fil. Den vedhæftede fil indeholder selve ormeprogrammet. Hvis man aktiverer det (typisk ved at dobbeltklikke på den vedhæftede fil), inficeres pc'en. Mail-ormen spreder sig herefter ved at sende sig selv videre til adresser, den finder på pc'en.

Antivirusprogrammer kan opdage og standse virus og mail-orme. Men de virker kun mod trusler, som programmet kender. Derfor skal du løbende opdatere antivirusprogrammet med information om de nyeste virus. Det kan gøres via nettet, og det er en god ide at sætte programmet til at opdatere automatisk en gang om dagen.

2. Installer en firewall
En firewall er et program eller en boks, der regulerer trafikken mellem en computer og internettet. Som regel tillader en firewall al trafik, der starter fra din pc og sendes ud på nettet. Omvendt forbyder den al trafik, der stammer fra internettet og forsøger at komme ind på din computer. På den måde beskytter den mod angreb fra hackere og netværksorme.

Hvis du kun skal beskytte en enkelt pc, kan du anvende en personlig firewall. Det er et program, der kører på pc'en. Har du brug for at beskytte et netværk med flere pc'er, kan du anvende en hardwarebaseret firewall. Det er en boks, som placeres mellem internetforbindelsen og netværket.

Når en firewall først er installeret, kræver den som regel ikke yderligere opdateringer.

3. Opdater pc'ens styresystem og hold det opdateret

De fleste angreb mod computere er rettet mod sårbarheder. Det er fejl i computernes programmer, der fungerer som sikkerhedshuller. Ved at udnytte en sårbarhed kan en hacker eller et angrebsprogram få kontrol over din pc. Derfor skal du undgå, at din pc har sårbarheder, der kan udnyttes via internettet. Det kan du gøre ved at holde styresystemet opdateret.

Microsoft udsender hver måned rettelser, der lukker sikkerhedshuller i firmaets programmer. Hvis du slår funktionen "Automatiske opdateringer" til i Windows, sørger den automatisk for at installere nye rettelser fra Microsoft, når de bliver udsendt. Du kan også besøge webstedet Microsoft Update og kontrollere, at du har fået alle nødvendige opdateringer.

4. Installer et antispywareprogram

Spyware er software, der udspionerer en pc-bruger og hans færden på nettet. Men betegnelsen bruges mere generelt om programmer, der ændrer på pc'ens opsætning og er til gene for brugeren.

Man risikerer at få spyware, hvis man installerer software, man har hentet over nettet. Noget spyware installerer sig selv, når man besøger bestemte websider.

Der findes en række programmer, som kan opdage og fjerne spyware på en computer. Flere af dem er gratis at bruge for private. Men ligesom antivirusprogrammer kan de kun fjerne spyware, som de kan genkende. Derfor skal antispywareprogrammer opdateres løbende.

5. Installer et spamfilter

Spam er uopfordrede reklamer, man får tilsendt via e-mail. Spam udgør ikke i sig selv noget sikkerhedsproblem, men det kan være meget irriterende.

Man kan nedbringe risikoen for at få spam ved kun at oplyse sin e-mail-adresse til folk, man kender. Hvis adressen optræder på websider eller i diskussionsfora, kan den let blive opsnappet af dem, der udsender spam.
Får man meget spam, kan man installere et program, der sorterer spam fra. Der findes flere programmer, som kan løse opgaven.

6. Dobbeltklik aldrig på vedhæftede filer i mails

Foruden selve brevteksten kan en e-mail også indeholde en eller flere vedhæftede filer. Det kan for eksempel være billeder, dokumenter eller programmer. Hvis du uopfordret modtager en mail med en vedhæftet fil, kan det være en såkaldt mail-orm. Det er et program, der spreder sig via e-mail. Hvis du undlader at dobbeltklikke på den vedhæftede fil, sker der ikke noget. Men dobbeltklikker du, bliver din pc inficeret, og den sender ormen videre til adresser, den finder på pc'en.

Selvom afsenderen er en, du kender, skal du alligevel være forsigtig. Orme forfalsker ofte deres afsenderadresse. Ring eller skriv til vedkommende og spørg, hvad filen indeholder, før du åbner den.

Filtypen angives som regel med en forkortelse efter det sidste punktum i filnavnet, for eksempel .doc for Word-dokumenter og .exe for programmer. Nogle mail-orme forsøger at skjule deres filtype ved at have dobbelte endelser, så filen for eksempel kan hedde "information.doc.exe". Her er der tale om et program, der forklæder sig som et Word-dokument.

7. Følg ikke tilsendte links til banker og betalingstjenester
Måske modtager du mails, der angiver at komme fra din bank eller en auktionstjeneste, du bruger. I mailen kan der være links til web-sider, som du bedes besøge for at bekræfte dine kundeoplysninger.

Den slags mails er ofte forsøg på "phishing". Det er en form for svindel, hvor svindleren narrer kreditkortnumre, fødselsdato og andre personlige oplysninger fra sit offer. Som regel sker det ved at narre offeret til at udfylde en formular, der øjensynlig ligger på et websted, man har tillid til. Men i virkeligheden er der tale om et falsk websted, som er under svindlerens kontrol.

I stedet for at følge links, der sendes i mails, skal man derfor gå ind via sine normale bogmærker eller webstedets hovedside. Er man i tvivl, kan man ringe eller maile til banken og spørge, om den virkelig har sendt den mail, man er i tvivl om.

8. Brug browserens sikkerhedsindstillinger
Mange angreb på pc'er udnytter i dag svagheder i browserprogrammer, især Internet Explorer. Man kan beskytte sig ved at benytte en anden browser. Men man kan også beholde Internet Explorer og udnytte dens sikkerhedsfaciliteter.

Det vigtigste er muligheden for at slå avancerede funktioner fra. For eksempel kan man vedtage, at websteder som udgangspunkt ikke må kunne køre programmer på pc'en, de må kun vise tekst og billeder i browseren. Har nogle websteder brug for mere, kan man gøre undtagelser for dem, der har behov for det.

Indstillingerne findes i Internet Explorer i menuen "Funktioner" under punktet "Internetindstillinger". Vælg fanebladet "Sikkerhed". Klik på zonen "Internet" og træk skyderen under "Sikkerhedsniveau for denne zone" til "Høj". De websteder, der ikke fungerer med denne indstilling, kan derefter tilføjes til zonen "Websteder, du har tillid til". Klik på zonens ikon og klik på knappen "Websteder…"

9. Pas på programmer, du henter via internettet
Hvis du henter et spændende program fra en webside, risikerer du at få mere med, end du har bedt om. Måske er programmet inficeret med en virus (se godt råd nummer 1). Eller måske indeholder det spyware, der overvåger din færden på nettet (se godt råd nummer 4).

For at undgå problemer skal du så vidt muligt kun hente programmer fra websteder, du har tillid til. Du kan også læse licensbetingelserne for at se, om du forpligter dig til noget uønsket ved at hente og installere programmet.

Når du henter et program, skal du ikke køre det med det samme, men placere det i en mappe. Herefter kan du scanne det med et antivirusprogram. Efter du har installeret det, kan du køre et antispywareprogram for at sikre, at det ikke har installeret spyware på din pc.

10. Brug hovedet
Lyder det for godt til at være sandt? Så er det sikkert løgn.

Med den indstilling kan du undgå mange it-sikkerhedsproblemer. Hvis en mail lover dig guld og grønne skove, vil den sikkert prøve at lokke noget fra dig – for eksempel dit kreditkortnummer.

Det gælder også, hvis du modtager en underlig mail fra en god ven. Før du dobbeltklikker på den vedhæftede fil, skal du overveje, om den nu også kommer fra din ven. Ring eller mail og spørg ham.

Vær forsigtig med websider, som du finder gennem søgninger eller henvisninger i mails. Brug så vidt muligt dine egne bogmærker til at gå ind på de sider, du jævnligt besøger.

Helt generelt: Hvis du bruger din kritiske sans, kan du undgå mange problemer – også når det gælder it-sikkerhed.