Den lille folder om fejl på internettet

Fejl 1: Dit kodeord er svagt.
Dit kodeord er din dørlås. Sørg for at den er stærk.
Simple kodeord kan nemt gættes. Brug aldrig ord, der relaterer til dig selv fx dit favorit sportshold, husdyrets navn eller navne og fødselsdage på dig selv eller familie mv. Del aldrig dit kodeord med nogen og anvend et separat kodeord til din email. Brug gerne forskellige kodeord til dine forskellige adgange fx email, bank, sociale medier, streaming tjenester mv. Bruger du det samme kodeord, og det bliver gættet, så giver du en kriminel adgang til hele dit liv.

Svage kodeord:
Brug aldrig svage kodeord, som er nemme at gætte.
~~Sammyhund~~ ~~Brøndbyfc~~ ~~password123~~ ~~qwerty~~ ~~170743~~ ~~kodeord~~ ~~1234~~

Brug i stedet tre tilfældige ord

Fiskbådtulipan √ (Stærkt kodeord)

Meget stærkt kodeord:
For at skabe et rigtig stærkt kodeord, skal du bruge både store og små bogstaver samt tal.
Brug fx tre tilfældige ord og tilføj tal eller symboler – her er et eksempel med kodeordet fra før

19fisKbåD3tuliP95!! √ (Meget stærkt kodeord)

Fejl 2: Ikke at have et antivirus program
Antivirus programmet er din sikkerhedsvagt. Sørg for at have antivirus og hold det altid opdateret.
Virusser og malware (= ondsindet software) kan inficere alle dine enheder (computer, tablet, telefon mv.). Hvis dit udstyr er blevet inficeret, kan du blive låst ude, dine personlige informationer kan stjæles, eller du kan blive overvåget i dit hjem!

De fleste systemer har indbygget antimalware program. Sørg for at anvende det, så der bliver ryddet op på din enhed. Som ekstra sikkerhed bør du installere et antivirus program (det kan sagtens være en gratis version). Begge typer programmer er dine sikkerhedsvagter, som holder øje med alt, der forsøger at få adgang til din enhed, og de advarer dig, hvis nogen forsøger at inficere enheden.
Der kommer hele tiden nye vira og malware, så hold altid dine sikkerhedsprogrammer opdateret, så de kan advare dig i tide.

Fejl 3: At du ikke opdaterer din software
Software er aldrig 100% perfekt. Der er ofte sikkerhedsbrister eller huller, som kriminelle kan bruge til at skaffe sig adgang til dine data. Det er derfor vigtigt, at du altid opdaterer din software, når producenten anbefaler det. Producenten tilbyder oftest enten en fuld opdatering eller et "patch"= en lap, som kan lukke for sikkerhedsrisikoen.
Software er ikke 100% sikkert, så husk altid at opdatere.

Fejl 4: At du ikke tager backup af dine data
Tag altid backup (kopier) af de ting, som er væsentlige for dig. Gem dem på et sikkert sted.
Spørg dig selv hvilke ting, du ikke vil undvære, hvis enheden går i stykker eller bliver stjålet i morgen. Dine filer, billeder, kontakter, minder er nogle af de mest væsentlige ting på din enhed. Så tag en backup og gem den på et sikkert sted. Backup kan foretages på et fysisk medie eller i "skyen". Tag backup ofte og gerne på flere medier.
Tag backup ofte og gem dem på et sikkert sted. Tag backup af det væsentlige.

Fejl 5: At klikke på links og vedhæftede filer

Du ville ikke lukke en fremmed ind i dit hjem, så hvorfor lukke dem ind på din enhed?

Emails er den største risiko, da disse tit indeholder links eller vedhæftede filer, som du kan klikke på eller åbne. Men du skal også være opmærksom på sociale medier, som bugner med links og konkurrencer. Når du klikker eller åbner et usikkert link eller dokument, giver du kriminelle adgang til at installere malware på din enhed, som kan give dem adgang til dine data, overtage din enhed eller overvåge dig.

Tryk derfor aldrig på links eller åben dokumenter, medmindre du er helt sikker på, hvem afsenderen er. Hvis du er i tvivl om indholdet, så kontakt afsenderen og spørg om de har sendt noget.

Fejl 6: At dele alt på de sociale medier

Du ville aldrig sætte en annonce i avisen og fortælle, at du er på ferie og at dit hus står tomt, så hvorfor fortælle hele verden det på de sociale medier?

De sociale medier er gode til at holde kontakt med familie og venner, men medmindre du har helt styr på dine privatlivsindstillinger, så kan du ende med at fortælle mere om dit liv end du ønsker. Du ved aldrig 100% sikkert, hvem der kigger med. Bruger du fx indstillingen venners venner, så overvej hvor mange tusinde det kan være, og hvem de mon er? Hold også øje med hvem du selv har som venner og pas på falske profiler. En god tommelfingerregel er aldrig at dele noget, som du ikke ville fortælle offentligt i en stor forsamling.

Vær forsigtig med hvad du deler på de sociale medier. Tjek dine privatlivsindstillinger.

Fejl 7: Giv aldrig personlige oplysninger online

Du ville aldrig give en tilfældig på gaden dit CPR nummer eller din pinkode, så hvorfor gøre det online?

Falske emails med links, hvor du skal bekræfte det ene eller det andet, florerer jævnligt. Oplys aldrig personlige informationer som CPR nummer, kodeord, pinkoder, betalingsoplysninger mv. Offentlige myndigheder, SKAT mv. vil aldrig kontakte dig i en email og bede om den type informationer. Når du bliver bedt om den slags, så forhold dig kritisk til afsenderen, og tjek evt med afsender om ægtheden.

Oplys aldrig personlige oplysninger online. Tjek afsenderen før du deler informationer.

Fejl 8: Overføre penge uden at tjekke modtageren først

Du ville aldrig give penge til en tilfældig på gaden, uden at tjekke hvem de er, så hvorfor gøre det online?

Kriminelle kan nemt udgive sig for at være hvem som helst online. De kan kopiere hjemmesider, emailadresser og telefonnumre på familie, venner, kolleger, chefen, kunder, banken, forsikringsselskabet mv. De vil gøre hvad som helst for at snyde dig til at overføre penge til dem. Så selvom det hele ser legalt ud, så kan det være snyd! Vær kritisk!

Overfør derfor aldrig penge hvis du ikke ved, hvem modtageren er. Tjek modtageren eller få på anden vis bekræftet budskabets ægthed før du overfører penge. Undlad at sende penge, hvis du er det mindste i tvivl.