Sikkerhed på nettet....

Hvilke farer er der?

I dag er der normalt et formål med de ting en hacker forsøger at gøre mod brugerne af telefoner, tablets og/eller PC'er. Der er efterhånden sjældent at det blot er for at ødelægge.

De oplagte muligheder er:

- Få kendskab til dine kortoplysninger o.lign. så de kan stjæle fra dig.
- Spionere på dig, fordi du har adgang til interessante oplysninger.
- Spionere på dig med henblik på at indsamle og videresælge oplysningerne.
- Inficere din enhed, så den kan anvendes i angreb på andre.
- Presse penge af dig, f.eks. ved at ødelægge dine data.

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.
Virussen kan ødelægge dine filer, men selve hardwaren tager normalt ikke skade.

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.

Spam:
Spam er uopfordret e-mail. Afsenderen har på en eller anden måde opfanget ens e-mail adresse ved f. eks. at gennemsøge websider, nyhedsgrupper eller registrere et besøg. "Spammeren" sender ofte hundrede eller tusinder spammails af sted af gangen.
Man må aldrig svare på spam, da man herved bekræfter at ens mailadresse er aktiv.

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.

Ransomware:
Program der krypterer dine data/hele maskinen, og kræver et beløb for at låse op igen. Betal aldrig – du får alligevel ikke en kode.

Og hvordan bekæmper man det så?

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

For det første - Et antivirus program. Brug et anerkendt program. Hos safetydetectives.com kan du læse om de bedste.

For det andet - En firewall. Den sikre at der kun foregår kommunikation på din internetforbindelse, som du har givet lov til. Er incl. i mange sikkerhedspakker.

Bruger du Windows 10/11 (alle tidligere Windows versioner er i dag usikre, da de ikke længere opdateres) er både antivirus og firewall indbygget, så hvis du opfører dig fornuftigt, så behøver du ikke andet.

For det tredje skal du holde dit styresystem og dine programmer opdateret. For Windows sker dette automatisk i ”Home” versionerne.
Sørg også for at holde programmer/apps opdateret.

Endelig skal du have styr på brugeren af enheden – dig selv. Opfør dig fornuftigt!
Det inkluderer (men er ikke begrænset til):

- Svar aldrig på mails du ikke kender afsender på.
- Installer kun programmer/apps som du ved hvad du skal bruge til, og som du ved hvor kommer fra.

- Du har IKKE vundet en ny iPhone, ligesom du IKKE har arvet en ukendt onkel i Uganda. Slet disse mails, hvis dit spamfilter slipper dem igennem.
- Lad ALDRIG andre installere noget på din enhed.
- Oplys ALDRIG dine passwords, kontonumre, MitID koder eller andet til nogen der ringer eller skriver til dig. Det er ALTID svindel !
- Gå ikke ind på hjemmesider der ser tvivlsomme ud.
- Når du handler på nettet, så betal ALTID med Dankort, og brug kun danske hjemmesider. Check først at de rent faktisk kan skrive på korrekt dansk på siden….
- Hvis et tilbud er for godt til at være sandt – så er der nok en årsag….

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 safetydetectives.com som har gode artikler og værktøjer. Også borger.dk har gode vejledninger om emnet.

Udvidet sikkerhed

Arbejder du med kritiske data eller på din arbejdsPC/telefon udenfor hjemmet, så kan der være behov for yderligere sikkerhed. For sidstnævnte er det vigtigt at følge de sikkerhedsregler der gælder for din arbejdsplads.

Følgende kan være ekstra foranstaltninger, som er værd at overveje:

- Brug VPN på nettet. Dette sikre mod usikre trådløse forbindelser, f.eks. på et hotel, og mod at nogen skulle opsnappe din kommunikation. Det gør dig også anonym overfor den side du besøger.
  Nogle sikkerhedspakker har VPN inkluderet, og ellers kan du købe billige gode VPN løsninger mange steder.
- Slå Bluetooth fra. Bluetooth er en usikker protokol som kan benyttes til at få adgang til din enhed, samt til at spore dig.
- Brug en sikker kode på din enhed. D.v.s mindst 6 cifre og gerne flere.
- Brug to-faktor godkendelse på mailkonti, og andre konti hvor det er muligt.
- Slå alle former for sporing fra både i apps og mellem apps. Sørg for at apps/programmer ikke har adgang til ting (f.eks. kamera) hvis de ikke har brug for det.
- Indstil DuckDuckGo som default søgetjeneste. Den sporer dig ikke i modsætning til alle de kendte som Google og Bing.
- Brug en sikker browser. Jeg anbefaler Firefox – ALDRIG Google Chrome eller Microsoft Edge.
- Tænk meget nøje over hvilke apps du installerer. Undgå nogen der kræver adgang til mikrofon, kamera osv. uden at have brug for det.
- Undgå cloud tjenester. Skriver du f.eks. på en patentansøgning er det lidt ærgerligt at nogen stjæler den fra skyen.
- Brug evt. et privacy filter på enheden, så skærmen kun kan læses forfra (altså af dig).