

Netsikker nu! 2009 - 10 gode råd

Privatlivets fred

1. Læg kun oplysninger om dig selv på internettet, som alle og enhver må bruge.

De oplysninger, du deler med andre på nettet, er lige så tilgængelige, som hvis de stod på et stykke papir, du havde tabt på vejen. De oplysninger du uploader på for eksempel Facebook eller andre sociale netværkstjenester, vil kunne tilgås af alle. Det er ikke kun venner og familie eller kolleger og naboer, men også indbrudstyre, hackere og producenter af spam.

Det er ikke altid sikkert, at du lige tænker over hvilke af dine data, der bør holdes fortrolige. Telefonnummer og adresse kombineret med fødselsdato gør det meget let for andre at udgive sig for at være dig. Et par af fejlene, der ofte begås, er, at CPR-nummer ikke fjernes fra et CV, der lægges op på nettet eller at du fortæller hele verden, hvornår du er på ferie og din lejlighed står til rådighed for indbrudstyre.

Det er ligeledes et problem, at langt flere har adgang til din personlige profil på for eksempel Facebook, end du lige havde regnet med. Det har du dog selv meget indflydelse over ved at rette i dine privatlivsindstillinger, se mere i råd 5.

2. Spørg, inden du lægger billeder og oplysninger ud om andre. Det gælder også børn.

Det er ikke alle, der har ens grænser i forhold til, hvad man lægger ud på sociale netværkstjenester, og dermed deler med en meget stor gruppe mennesker. Billeder, der ses i nye sammenhænge, kan falde i de forkerte hænder. Det kan være den nye arbejdsgiver, ekskæresten, forældre og så videre. Det er også vigtigt, at du er opmærksom på at billeder, der er offentliggjorte på onlinetjenester kan kopieres, manipuleres og bruges i andre sammenhæng.

Skriv derfor ikke noget om andre, og hvad de foretager sig, uden at de har givet tilladelse til. Det samme gælder for billeder. Ikke alle bryder sig om at have billeder liggende forskellige steder på nettet, og bør derfor spørges først. Alle har ret til privatliv, også børn, der ikke selv kan sige fra. Så tænk over det før du lægger en masse billeder og oplysninger op af dig selv, dine børn eller andre.

3. Vær kritisk, når du modtager forespørgsler og invitationer på nettet.

Det gælder selvfølgelig traditionelle spam-mails, hvor du bliver lovet gevinster, russiske brude eller Viagra. Men også sociale netværkstjenester udgør en sikkerhedsrisiko. Hackere bruger de nye tjenester til at sprede virus. På Facebook kan du eksempelvis blive lokket med at få afsløret navnet på en hemmelig beundrer, hvis du downloader et bestemt program til din pc, men i stedet får downloadet en virus. Vær derfor kritisk med hvad du deltager i og reagerer på.

4. Læs aftalevilkår for tjenester, så du ved, hvad du går ind til.

Når du tilmelder dig forskellige tjenester på nettet står der altid noget med småt. Selvom det er fristende blot at sætte i et hak i feltet: "jeg har læst betingelserne", så er det vigtigt at du er

opmærksom på, hvad det er du går ind til. Du giver for eksempel brugsretten over dine billeder til Facebook, når du opretter en profil, idet du accepterer brugerbetingelserne.

Facebook kan også videregive oplysninger om, hvad du som Facebook-bruger foretager dig rundt om på nettet. Denne viden kan bruges til at fortælle dine venner om, hvad du laver, men også til at reklamere for konkrete produkter på dine venners sider. Husk, at der altid står noget med småt.

5. Beskyt dine private oplysninger på tjenester via privatlivsindstillinger/ privacy settings.

Måske har du oplevet, at dine venner og bekendte via en social netværkstjeneste er lidt for orienterede om, hvad du foretager dig, eller at en ven lægger et billede op, som dine kollegaer ikke skulle have set. Ved du, at du har mulighed for at bestemme, hvem der må se hvad?

Ved at gå ind i privatlivsindstillinger, eller privacy settings kan du bestemme, hvem der må se hvad. Du kan dele dine venner op i forskellige grupper og give grupperne forskellige rettigheder. Vær især opmærksom på, at alle i dit netværk på Facebook kan se hele din profil, med mindre du har blokeret for det. Det kan være hele din gamle skole, din gamle arbejdsplads eller netværket ”Danmark”.

DK Cert har udarbejdet en guide til, hvordan du retter i indstillingerne, og hvad du skal være opmærksom på. [Find guiden her](#), eller find evt. andre forklaringer på internettet.

Opdatering af pc'en

1. Hold programmerne på din pc opdateret og brug automatisk opdatering.

Du skal sørge for at holde alle programmer på din pc opdateret - ikke kun antivirus og firewall. Programmer der ikke er opdateret kan have sikkerhedshuller, der fungerer som en ulåst bagdør til din pc, hvor kriminelle får uhindret adgang. Hvis programmerne på din pc har sikkerhedshuller, kan du risikere, at de kriminelle udnytter disse, når du besøger en hjemmeside, du normalt har tillid til.

De kriminelle kan på hjemmesiden have lagt skadelige elementer, der er skjult for dig som besøgende, og som ejeren af siden ikke kender til. Dette kaldes drive-by angreb. Det skadelige element kan være en såkaldt trojansk hest, som de kriminelle bruger til at få fuld kontrol med din pc. Hvis de kriminelle opnår adgang til din pc, har de adgang til dine fortrolige oplysninger. De kan også misbruge computeren til at gemme ulovlige programmer eller bruge din pc til at udsende spam. Sikkerhedshullerne i ikke opdaterede programmer kan også udnyttes af vira eller orme.

Nogle programmer har automatisk opdatering, som du med fordel kan slå til. Andre programmer kræver, at du selv gør noget for at opdatere dem. Hvis du ikke har overblikket over dette, kan du gratis scanne din pc på opdaterdinpc.dk, hvor du også kan læse mere om opdatering.

2. Hold dit antivirusprogram ved lige og brug firewall.

Det er vigtigt, at du holder dit antivirusprogram og din firewall opdateret. Dit antivirusprogram holder øje med, om din pc bliver angrebet af virus fra mails, filer og hjemmesider. Programmet kan også hjælpe med at scanne din pc, for at se om der allerede er virus. Hvis det ikke er opdateret, vil der være en lang række vira, som programmet ikke kender til, og dermed ikke kan være opmærksom på. Foruden at holde programmet opdateret er det også vigtigt, at du jævnligt udfører en virusscanning af din harddisk.

Din firewall beskytter dig mod kriminelle, der forsøger at bryde ind i din pc. Find en indstilling der spærrer for uønsket trafik, men ikke spærrer for alt du foretager dig på internettet. I langt de fleste tilfælde vil det være dig, der opretter en forbindelse fra din pc til en anden maskine på internettet. Derfor kan du som hovedregel sætte din firewall til at afvise alle opkald udefra. Det kan være komplekst at konfigurere en firewall, så hvis du har svært ved det, er det bedre at du søger hjælp, f.eks. blandt venner eller i familien, end at du giver op.

3. Husk at sikre dit trådløse netværk.

For at undgå at andre får adgang til din pc eller din internetforbindelse via dit trådløse netværk, er det vigtigt, at du benytter kryptering. Hvis du krypterer, sikrer du, at andre ikke kan læse din kommunikation eller bruge din internetforbindelse til kriminelle handlinger. Hvis din forbindelse bliver brugt, er det dig, der bliver mistænkt – ikke de kriminelle. Det er også vigtigt, at du laver et ordentligt password på minimum 8 tegn, og gerne med små og store bogstaver, tal og specialtegn.

Der findes forskellige former for kryptering: WPA, WPA2 og WEP. WPA2 og WPA er de mest sikre. WEP er ikke længere en sikker kryptering, så hvis du kun kan bruge WEP, bør du skifte password ofte, og så hurtigt som muligt enten opgradere dit udstyr eller udskifte det, så du kan anvende en sikker kryptering på dit trådløse netværk.

Hvis det er muligt, er det også en god ide at slå broadcastmeddelelser fra på dit trådløse netværk. På den måde bliver det sværere for de kriminelle at finde frem til dit netværk og tilslutte sig. Hvis du ikke kan slå broadcastmeddelelser fra bør du ændre det standard navn (betegnet SSID), dit netværk hele tiden udsender. Derved gør du det sværere for de kriminelle at identificere producenten af dit trådløse udstyr. Hvis de kriminelle kender udstyrsmærket, har de nemlig lettere ved at udnytte dit udstyrs svagheder.

Den sidste ting du bør overveje for at sikre dit trådløse netværk, er at anvende MAC-adresse filtrering. En MAC-adresse er en entydig identifikation af udstyr, der er tilkoblet et netværk, også et trådløst netværk. Netop fordi en MAC-adresse er unik, kan du i din basis station (router) oprette en liste med alle de pc'er (identificeret ved deres MAC-adresse), du vil tillade, får adgang til dit trådløse netværk.

Du kan læse mere om, hvad og hvordan du skal gøre på it-borger.dk.

4. Pas på med at klikke på links i mails fra ukendte afsendere.

Du skal ikke klikke på links, som du ikke har tillid til, hverken hvis mailen kommer fra nogen du kender eller hvis afsenderen er ukendt. Hvis du klikker på linket, kan det medføre, at din pc bliver inficeret med virus, eller at du i fremtiden vil modtage mere spam. Det kan selvfølgelig være svært at afgøre, om du skal have tillid til et link, især når du kender afsenderen. Hvis du er i tvivl, så lad være med at klikke på linket. Du bør først få bekræftet tilliden ved at spørge afsenderen om vedkommende HAR sendt mailen.

Et andet problem er phishing, der er en form for identitetstyveri. Disse skal du være særlig opmærksom på, hvis du modtager mails fra troværdige afsendere, som f.eks. din bank eller dit forsikringssselskab, hvor du bliver bedt om at opgive personlige oplysninger. Det kan være numre på kreditkort, kontonumre, cpr-nummer eller pinkoder. Banker og betalingstjenester vil ALDRIG bede dig om personlige oplysninger i mails.

Det kan også ske via en falsk hjemmeside, der f.eks. ligner din banks hjemmeside, hvor du bliver bedt om at indtaste personlige kontooplysninger mv. Det vigtigste er, at du er kritisk og tænker dig om en ekstra gang, før du åbner eller downloader materiale, som du ikke stoler på. Ligeledes bør du ALDRIG videregive personlige oplysninger til tvivlsomme afsendere.

5. Installér kun programmer, du har behov for.

Hent kun programmer fra netsteder du har tillid til - og hent kun programmer du har brug for. Det bliver på den måde lettere for dig at sikre, at dine programmer er opdateret.

Hvis du installerer et program, som du efterfølgende finder ud af, du ikke har brug for, så afinstaller programmet så du ikke behøver at holde det opdateret.

Du skal være opmærksom på om installeringen kræver at du opgiver personlige oplysninger eller siger ja til at modtage reklamer. Særligt gratis programmer og fildelingsprogrammer kan udgøre en sikkerhedsrisiko.