Brug kun din computer til arbejdsrelaterede opgaver > **Gå ikke på sociale medier eller tjenester på din arbejdscomputer**

Sociale medier som eksempelvis Facebook, LinkedIn, Twitter og Instagram kan give IT-kriminelle adgang til personfølsomme data, hvis de anvendes uhensigtsmæssigt. Det kan eksempelvis ske gennem videoer eller links til videoer i opdateringer og annoncer på sociale medier. Vises en video inden for Facebooks eget univers, er der som regel ingen risiko, men trykker du på et link, som fører videre til en anden hjemmeside, bør du være på vagt. Linket kan indeholde skadelige selvinstallerende programmer, som giver bagmænd kontrol over computeren og adgang til fortrolige oplysninger.

I den alvorlige ende risikerer du ubevidst at installere software, som overvåger alt, hvad du foretager dig på computeren. På den måde kan IT-kriminelle få kendskab til brugernavne og passwords til Facebook, LinkedIn, mailkonti, PayPal-konto og andre webshopudbydere, der ikke kræver NemID.

IT-kriminalitet kan også ske via mails, der skal forestille at være fra LinkedIn eller Facebook. I mails opfordrer IT-kriminelle dig til at indtaste brugernavn og password via et link. Handler du på deres opfordring, kan de stjæle loginoplysninger og potentielt dele kompromitterende fotos og upassende indlæg i dit navn på sociale medier med krav om, at du betaler en løsesum. De kan også sprede virus og spam fra din personlige profil.

Cloudtjenester som eksempelvis Dropbox, Picasa, iCloud, Gmail, Hotmail, Salesforce , Evernote, Carbonite og LastPass indeholder også risici, hvis de bruges forkert. IT-kriminelle kan via en browser få adgang til konti på cloudtjenester, hvis de har sneget et spionprogram ind på din computer, eller hvis de på anden måde har fået viden om login og passwords. Det kan medføre misbrug af fotos eller dokumenter til skade for den enkelte person, kollegaerne, klinikken, patienterne og samarbejdspartnerne. Ligesom det kan føre til, at ondsindede programmer spredes til arbejdsnetværk, når den samme cloudtjeneste-konto bruges til både arbejdsrelaterede og private formål. Alt hvad det kræver, er et dobbeltklik på den forkerte fil i skyen, som kan være placeret der ved en fejl eller af en IT-kriminel.

Tre gode råd

- Undgå at bruge din arbejdscomputer til sociale medier og cloudtjenester i det omfang, det er muligt. Ved brug af private cloudtjenester og sociale medier øges risikoen for, at IT-kriminelle kan få adgang til personfølsomme data samt sprede ondsindede programmet.

- Klik aldrig på mails fra et socialt medie, hvori du bliver opfordret til at indtaste dine loginoplysninger via et link. Gå i stedet direkte til hjemmesiden for det sociale medie for at foretage eventuelle ændringer.

- Læg aldrig fortrolige eller personfølsomme oplysninger ud på en cloudtjeneste - medmindre der er givet specifik tilladelse til det, og i så fald bør det kun være på godkendte erhvervsløsninger.