# 4 Beskyt fortrolige oplysninger

**Nogle oplysninger og informationer, herunder personoplysninger, skal håndteres særligt.**

Vær opmærksom på følgende:

- Lad ikke fortrolige oplysninger, herunder borgeres eller medarbejderes personoplysninger, ligge fremme.
- Lås altid skærmen på computeren, når du går fra den. Benyt evt. WIN + L som genvej.
- Du må kun behandle fortrolige oplysninger, herunder personoplysninger, som er relevante for din sagsbehandling.
- Brug altid en sikker, krypteret kanal som Digital Post, når du sender fortrolige oplysninger. Skal du modtage fortrolige oplysninger, fx et cpr.nr. fra en borger, så bed ligeledes om, at de sendes via et sikkert system som Digital Post.

Glemmer du det, risikerer du at gøre fortrolige oplysninger, fx borgeres personoplysninger, tilgængelige for uvedkommende.

Fortrolige oplysninger kan fx være følsomme personoplysninger såsom personers helbred, etniske oprindelse eller seksualitet, det kan være detaljer om sikkerhedshændelser eller klassificerede informationer i arbejdssager.

*Denne pjece er udviklet af:*

Digitaliserings-styrelsen KL DANSKE REGIONER

# Sikker adfærd er vigtig

I det offentlige arbejder vi ofte med personoplysninger, som er følsomme, og informationer, der skal behandles fortroligt.

Derfor er det vigtigt, at vi alle ved, hvordan vi skal behandle informationer sikkert.

**Større hackerangreb kan lægge en hel sektor ned**
For nogle år tilbage lammede et hackerangreb den britiske sundhedssektor i flere døgn. 19.500 patientaftaler blev annulleret, og 600 computere hos praktiserende læger blev låst. Det skete, fordi medarbejdere åbnede en zip-fil.

**Derfor skal du som medarbejder følge disse råd:**

1. Lav stærke kodeord
2. Log på via VPN og brug kun sikre netværk
3. Reagér kun på sikre beskeder
4. Beskyt fortrolige oplysninger, herunder personoplysninger

Vær opmærksom på, at din arbejdsplads kan have lokale politikker for fx kodeord eller sikker behandling af informationer, som du skal orientere dig i og følge.

sikker digital DK

# 1 Lav stærke kodeord

**Lav stærke kodeord, så dine systemer er sværere at hacke. Dit kodeord bør være:**

- Langt – mindst 15 tegn, jf. anbefaling fra Center for Cybersikkerhed.
- Unikt – brug ikke det samme kodeord flere steder.
- Dit og kun dit – del ikke dit kodeord med dine kollegaer.

Det er vigtigt, at kodeordet er langt. Hvert ekstra tegn giver flere kombinationsmuligheder og gør det sværere at bryde.

**Du kan fx bygge kodeordet op efter en simpel sætning:**

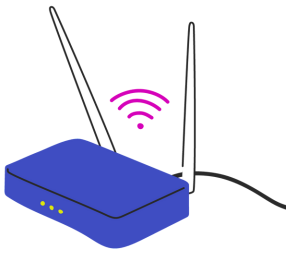
I2023spistejegmangeis%

# 2 Log på via VPN, og brug sikre netværk

**Hvis cyberkriminelle har adgang til det WIFI, du anvender, kan dine informationer opsnappes.**

Tilslut altid VPN, som er en sikret krypteret forbindelse til din organisations netværk, inden du logger på dine systemer.

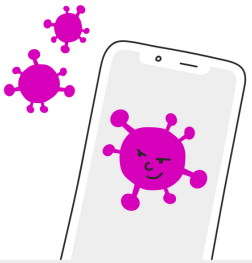
Brug kun sikre WIFI, hvor du skal logge på med en kode. Husk, at offentlige netværk, fx i caféer og i tog, hvor koden er tilgængelig for alle, ikke er sikre. Benyt dig i stedet af internetdeling fra din arbejdstelefon, hvis du kan.



# 3 Reagér kun på sikre beskeder

**Cyberkriminelle er blevet dygtige digitale tricktyve. Det er ikke længere nok at tjekke sproget og se, om afsenderen ser troværdig ud.**

- Er du i tvivl, om en henvendelse er ægte, så kontakt afsenderen på anden vis og få den bekræftet.
- Offentlige myndigheder sender ikke mails eller SMS'er med direkte links. Gå i stedet ind på myndighedens hjemmeside.
- Svar ikke på henvendelser, der beder om kredit- og bankoplysninger, kodeord eller lignende oplysninger.
- Vær påpasselig med at klikke på links. Tjek fx, om webadressen ser mistænkelig ud, ved at holde musen over linket.



**Er du i tvivl …**
om du har fået klikket på noget usikkert eller sendt fortrolig information til en forkert modtager, så følg din lokale politik og procedure for hændelseshåndtering.

**Få mere inspiration …**
til sikker adfærd i det offentlige på sikkerdigital.dk/myndigheder.
Her kan du bl.a. se film, gennemgå e-læring og tage en quiz.