## C:\Users\B008156\Desktop\DIGST_JPGs\02_Phishing.jpg4. Reagér kun på sikre beskederCyberkriminelle 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 underret din leder og din koordinator for informationssikkerhed.

### 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.

Denne pjece er udviklet af:



**Sikker adfærd er vigtig**

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

Tilgængelighed, fortrolighed og integritet af data og systemer er en forudsætning for vores daglige arbejde. Det er derfor vigtigt, at vi alle ved, hvordan vi skal behandle informationer sikkert.

**Større hackerangreb kan lægge en hel sektor ned**

I foråret 2017 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. Beskyt borgernes personoplysninger
2. Lav stærke kodeord
3. Log på via VPN, og brug kun sikre netværk
4. Reagér kun på sikre beskeder

Vær opmærksom på, at din arbejdsplads kan have lokale politikker for fx kodeord eller sikker behandling af informationer.

****

## C:\Users\B008156\Desktop\DIGST_JPGs\01_Personf├©lsom_Data.jpg1. Beskyt borgeres personoplysninger

* Lad ikke borgeres eller medarbejderes personoplysninger ligge fremme, fx på dit bord eller ved en printer.
* Lås altid skærmen på computeren, når du går fra den.

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

Personoplysninger skal beskyttes i overensstemmelse med databeskyttelsesforordningen og databeskyttelsesloven.

* Du må kun behandle personoplysninger, som er relevante for din sagsbehandling.
* Brug altid en sikker, krypteret kanal som Digital Post, når du sender personfølsomme eller fortrolige oplysninger.
* Hvis du skal modtage fortrolige eller følsomme personoplysninger, fx et cpr.nr. fra en borger, så bed dem sende oplysningerne via et sikkert system som Digital Post.

Hvad er følsomme personoplysninger?

Følsomme personoplysninger er bl.a. oplysninger om en persons religion, etniske oprindelse, seksualitet, politiske overbevisning og helbred. Læs mere i databeskyttelsesforordningens artikel 9.

Hvad er fortrolige oplysninger?

Visse informationer må af sikkerhedsmæssige hensyn ikke offentliggøres. I Sikkerhedscirkulæret kan du læse om fire niveauer af klassificerede informationer: *til tjenestebrug*, *fortroligt*, *hemmeligt* og *yderst hemmeligt*.

2. Lav stærke kodeord

Lav stærke kodeord, så dine systemer ikke nemt kan hackes.

Dit kodeord bør være:

* **Langt** – mindst 15 tegn.
* **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.

Kodeordet bør være nemt at huske for dig og svært for svindlerne at gætte

Du kan fx bygge det op efter en simpel sætning:

* I2018spistejegmangeis%

## 3. 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.