## C:\Users\B008156\Desktop\DIGST_JPGs\02_Phishing.jpg4. Reagér kun på sikre beskeder Hackerne er blevet dygtige digitale tricktyve. Det er ikke længere nok at tjekke sproget og se om afsenderen ser troværdig ud.

* Klik først, når du har holdt musen over linket, og tjekket om webadressen passer med afsenderen.
* Slet snarest muligt mails med følsomt indhold fx straks efter journalisering.
* Svar ikke på henvendelser, der beder om kredit-, bank-, kodeord eller lignende oplysninger.
* Hvis du får en henvendelse om noget usædvanligt fx fra en kollega, og det ”haster”, så få bekræftet, at henvendelsen er fra den rigtige afsender.
* Brug en sikker, krypteret kanal som fx Digital Post, hvis du skal sende fortrolige eller følsomme personoplysninger (fx CPR.nr. eller helbredsoplysninger). Brug aldrig almindelig e-mail eller sms.

### 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/medarbejdere.  
Her kan du 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 eller 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 personoplysninger 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 medarbejderne åbnede en zip-fil.

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

1. Beskyt borgernes personoplysninger
2. Lav stærke kodeord
3. Brug sikrede netværk og log på via VPN
4. Reagér kun på sikre beskeder

****

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

Det gælder både personoplysninger, og oplysninger som skal behandles fortroligt.

* Hent straks dokumenter med personoplysninger fra printeren.
* Lad ikke borgeres personoplysninger ligge fremme på dit bord.
* Lås altid skærmen på computeren, når du går fra den.

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

Personoplysninger skal beskyttes i overensstemmelse med databeskyttelsesloven.

* Du må kun behandle personoplysninger, som er relevante for din sagsbehandling.
* Brug altid en sikker, krypteret kanal som Digital Post, når du sender personoplysninger fx til en borger.
* Følg den lokale politik om behandling af personoplysninger i din organisation.
* Hvis en borger skal sende en mail med fx et cpr.nr., så bed dem sende oplysningerne via et sikkert system som Digital Post.

Hvad er følsomme personoplysninger?

Følsomme personoplysninger kan være religion, seksualitet eller sundhedsoplysninger.  
2. Lav stærke kodeord

Log sikkert på it-systemer, så de ikke nemt kan hackes. Følg arbejdspladsens regler for kodeord.

Hvis der ikke er en specifik forskrift, bør dit kodeord være:

* **Langt** – mindst 12 tegn.
* **Unikt** – brug ikke det samme kodeord flere steder.
* **Dit og kun dit** – del ikke dit kodeord med dine kollegaer.

Der kan være systemmæssige begrænsninger på antallet af tegn, hvor der til gengæld er andre sikringsforanstaltninger.

Kodeordet må gerne være nemt at huske  
Du kan fx bygge det op efter en simpel sætning eller et almindeligt fornavn:

* I2018spistejegmangeis!

## 3. Brug kendte netværk og log på via VPN

  
Information kan opsnappes, hvis hackere får adgang til netværket.

* Forbind kun til sikrede netværk, hvor du fx skal logge på med en kode.
* Tilslut altid VPN, som er en sikret krypteret forbindelse til din organisations netværk, helst inden du logger på dine systemer.