4. 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 information 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, sikre postkasser eller elektronisk patientjournal, hvis du skal sende personoplysninger. Brug aldrig almindelig e-mail, sms eller opkald.

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/sundhed
Her kan du se film, gennemgå e-læring og få flere gode råd.

Denne pjece er udviklet af:

SUNDHEDSDATA-STYRELSEN KL DIGITALISERINGSSTYRELSEN DANSKE REGIONER

Sikker adfærd er vigtig

Som sundhedspersonale arbejder vi ofte med patientoplysninger, som skal behandles fortroligt eks. personfølsomme oplysninger.

Tilgængelighed, fortrolighed og integritet af data og systemer er en forudsætning for vores daglige arbejde. Det er derfor vigtigt, at du ved, hvordan du 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 følge disse råd:

1. Beskyt patienters personoplysninger
2. Lav stærke kodeord
3. Brug sikrede netværk
4. Reagér kun på sikre beskeder

sikker digital DK

1. Beskyt patienters personoplysninger

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

- Lad ikke patienters personoplysninger ligge fremme.
- Gem ikke personoplysninger på USB eller harddisk. Brug i stedet det system, som din arbejdsplads stiller til rådighed til at gemme sikkert.
- Lås altid skærmen på computeren eller din tablet/telefon, når du går fra den. Og husk at logge af din bruger.

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

> Personoplysninger skal beskyttes i overensstemmelse med databeskyttelsesloven.

- Du må kun videregive personoplysninger til dem, de er relevante for.
- Brug altid en sikker, krypteret kanal som fx Digital Post eller sikre postkasser, når du sender personoplysninger fx til en borger.
- Hvis du skal sende personoplysninger fx et CPR-nummer til en kollega, så send dem via et sikkert system fx sikre postkasser eller elektronisk patientjournal. Hvis det er en kollega internt i regionen, kan du bruge jeres interne mailsystem, som er krypteret.
- Følg den lokale politik om behandling af personoplysninger på din arbejdsplads.

Hvad er følsomme personoplysninger?

Følsomme herunder fortrolige personoplysninger kan fx være religion, seksualitet eller helbredsoplysninger.

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 er andre systemmæssige 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 sikrede netværk

Information kan opsnappes, hvis hackere får adgang til netværket.

- Forbind kun til sikrede netværk, hvor du fx skal logge på med en kode.