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 mails eller beskeder med følsomt indhold.
- Svar ikke på henvendelser, der beder om kredit-, bank-, kodeord eller lignende oplysninger.
- Brug en sikker, krypteret kanal som fx E-post eller SkoleIntra/Aula, hvis du skal sende personoplysninger (fx cpr-nummer, politisk overbevisning 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/underviser
Her kan du se film, gennemgå e-læring og få flere gode råd.

Denne pjece er udviklet af:

KL · Digitaliseringsstyrelsen · Danske Regioner

Sikker adfærd er vigtig

På skolerne arbejder vi med væsentlige og ofte fortrolige eller følsomme informationer, og dem skal vi passe godt på.

Som lærer får du måske personoplysninger om den enkelte elev, som kan ligge i elektroniske systemer.

Det er derfor vigtigt, at du ved, hvordan du skal undgå, at ondsindede it-kriminelle får adgang til de oplysninger, til at ændre i oplysninger eller afskærer dig og dine kolleger fra systemer.

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 elevernes personoplysninger
2. Lav stærke kodeord
3. Brug kendte netværk og log på via VPN
4. Reagér kun på sikre beskeder

sikkerdigital.dk

1. Beskyt elevernes personoplysninger

Det gælder både personoplysninger og oplysninger, du skal behandle fortroligt.

- Hent hurtigt dokumenter med personoplysninger fra printeren.
- Lad ikke elevers/forældres personoplysninger ligge fremme i forberedelses- eller klasselokaler.
- Lås altid skærmen på computeren, når du går fra den. Og husk at logge af din bruger.

Glemmer du det, risikerer du at gøre elevernes 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 E-post og SkoleIntra (Aula), når du sender personoplysninger fx til en forælder eller kollega.
- Hvis en elev, forælder eller lærer skal sende en mail med fx et cpr-nummer, så bed dem sende oplysningerne via et sikkert system fx E-post eller SkoleIntra (Aula).

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.

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 sikre netværk, hvor du fx skal logge på med en kode: Tjek fx, at det er skolens, caféens, eller konferencestedets eget netværk, du logger på.
- Tilslut så vidt muligt altid VPN, som er en sikret krypteret forbindelse til skolens netværk, helst inden du logger på.