VEJEN TIL EN SIKKER, EKSTERN ARBEJDSORGANISATION

Med en tredjedel af IT-beslutningstagere, der indrømmer, at deres organisationer har været udsat for dataovertrædelser som følge af fjernarbejde[1], hvordan kan I så sikre, at jeres virksomhedsdata forbliver beskyttede i disse usædvanlige tider?

01.

Få jeres politik for fjernarbejde på plads

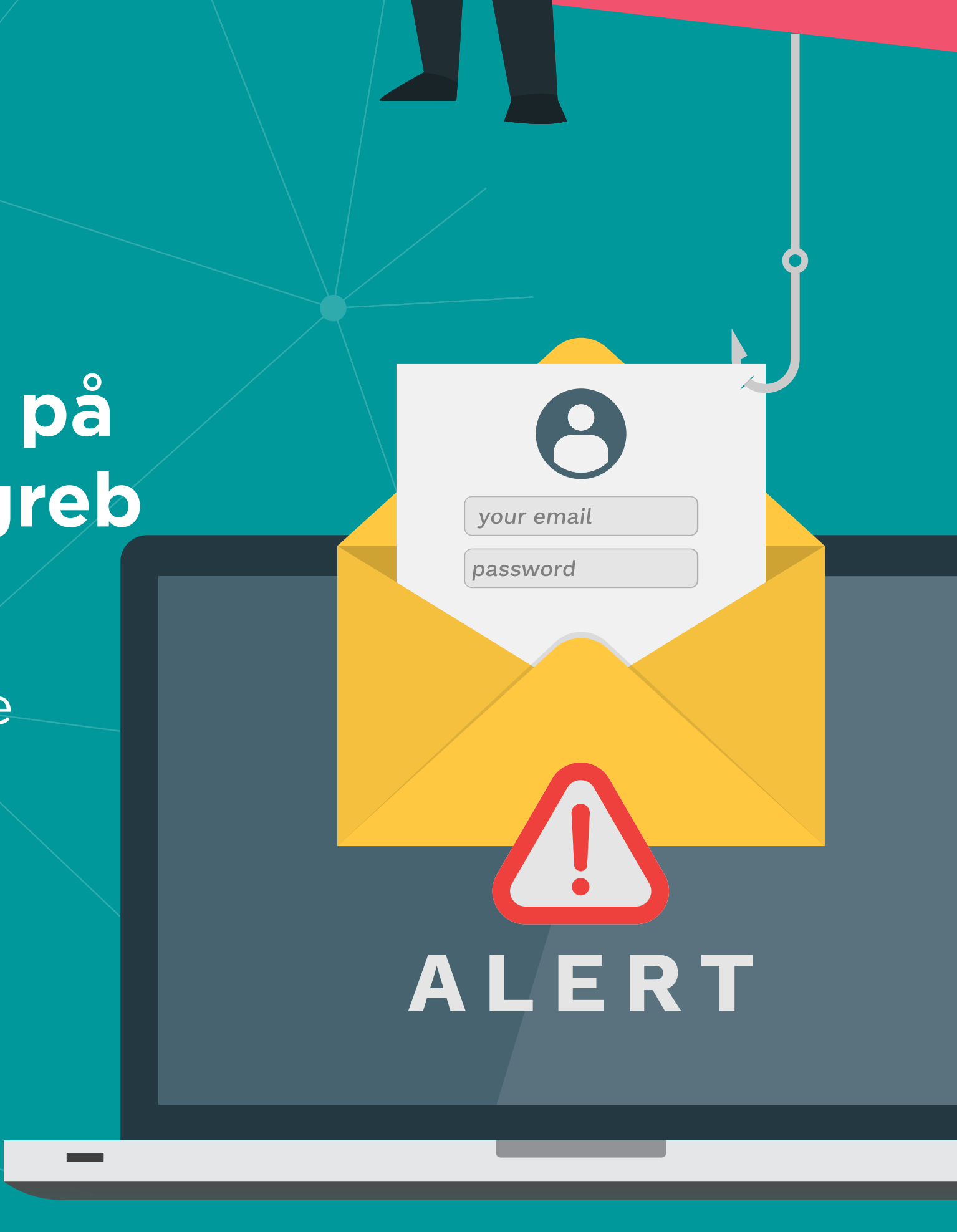
Et hjemmenetværk har **3,5 x større** sandsynlighed for at blive inficeret med malware end et virksomhedsnetværk[2]

Cyber-kriminelle **ved**, om du er hjemmebruger eller virksomhedsbruger, der arbejder hjemme

Beskyt jeres medarbejdere med en **sikker politik for fjernarbejde**, og undgå potentielle tab af data eller at blive holdt som gidsler med jeres egne filer

02.

Vær ekstra opmærksom på phishing-angreb



Covid-19-relaterede phishing-e-mails rstår nu for den største andel af **angreb**[3]

Svindelnumre steg med mere end **400 %** alene i Storbritannien i februar og marts[4], hvor ofre tilsammen mistede over £ 1,6 millioner[5]

Sørg for, at jeres medarbejdere ved, **hvem der har sendt en e-mail**, før de åbner den. De bør også tænke sig ekstra om, før de klikker på ukendte links

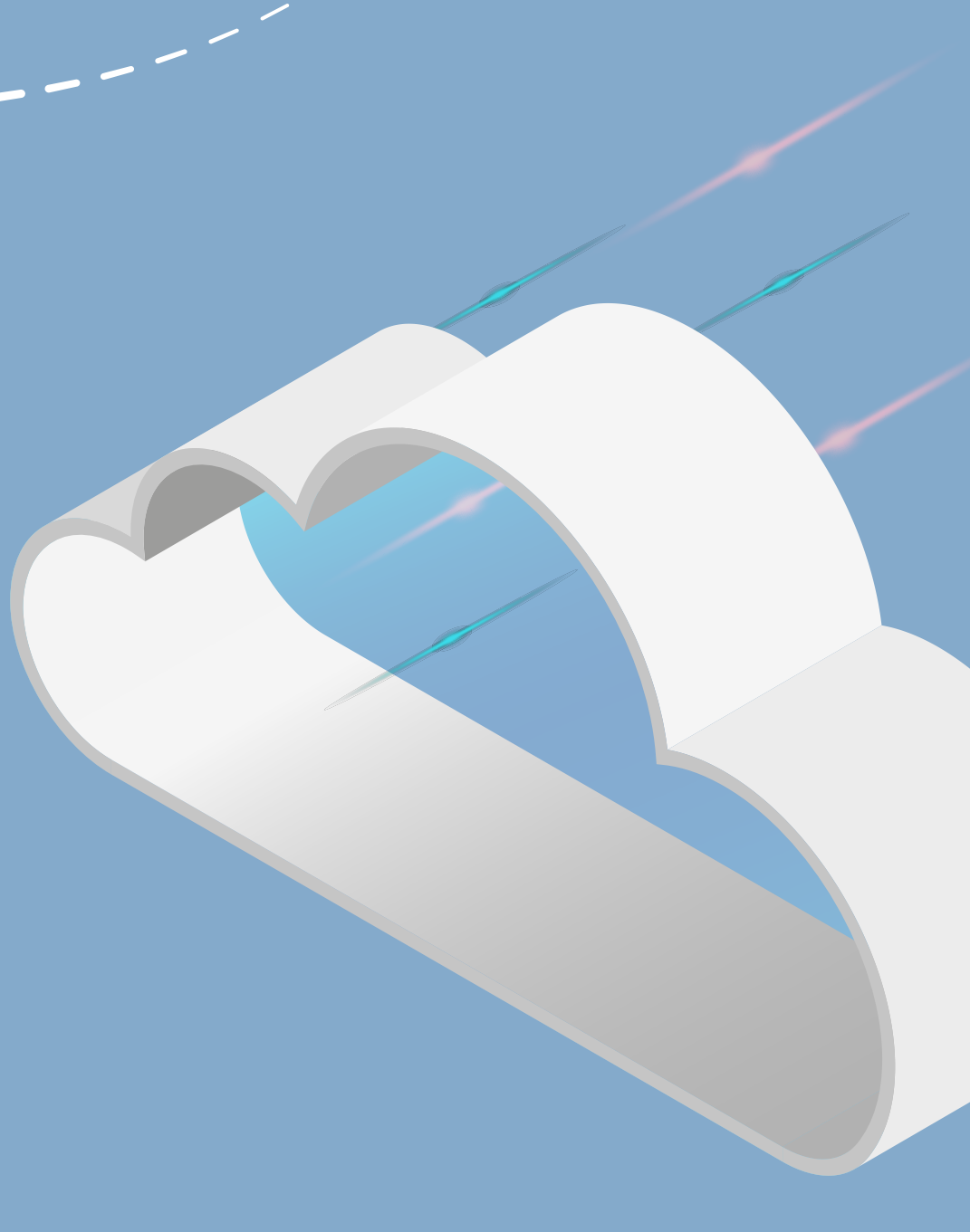
03.

Glem ikke sikkerheden på hjemmeenheden

Jeres team vil bruge den printer eller scanner, de har til rådighed derhjemme

Disse enheder har sandsynligvis **ikke de standardsikkerhedsfunktioner**, der leveres af virksomhedens netværksudstyr

Mere end **25 %** af alle enheder har en eller flere tjenester, der er udsat på internettet[6], og derfor er de mere sårbare over for angreb



For at beskytte virksomhedens vigtige data skal I yde medarbejderne support til at sikre, at deres netværk er privat og kun kan tilgås med en **sikker**, ikke-standardiseret adgangskode

04.

Og fortrolige papirer

Sørg for, at jeres medarbejdere, der arbejder hjemmefra, behandler virksomhedens papirarbejde med samme omhu som deres egne kontoudtog, så de makulerer eller opbevarer **alt fortroligt materiale**, indtil de kan vende tilbage til kontoret

MAKULÉR DEM!

05.

Den bedste politik er at have en

At arbejde hjemmefra **betyder ikke**, at virksomhedens politikker kan lempes

Mind jeres team om kun at bruge programmer, netværk og cloud-placeringer, **der leveres af virksomheden**

Alle gratis cloud-samarbejds- og lagringsværktøjer, medarbejderne kunne være fristet til at bruge, er muligvis ikke sikre, **hvis de ikke er blevet kontrolleret** af jer

Hvis nogen af jeres medarbejdere fjernarbejder, skal I sikre jer, at de har en klar forståelse af, hvordan de kan opretholde den samme standard for sikkerhed, uanset om de befinder sig inden for kontorets fire vægge eller sidder på sofaen derhjemme.

Kontakt Canon for at lære, hvordan I ikke kun kan overleve, men trives i disse usædvanlige tider.

Canon

See the bigger picture

---

1 https://www.raconteur.net/technology/covid-19-cybersecurity

2 https://threatpost.com/malware-risks-triple-for-remote-workers/154735/

3 https://www.cbi.org.uk/articles/phishing-coronavirus-and-working-from-home/

4 https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march

5 https://www.thebusinessdesk.com/westmidlands/news/2040001-the-perils-of-remote-working-the-next-normal-in-data-protection

6 https://www.bitsight.com/blog/identifying-unique-risks-of-work-from-home-remote-office-networks