Hej alle

Som nogen måske har bemærket, blev der d. xx. xxxx sendt en phishing-mail til alle medarbejdere i organisationen. Denne phishing-mail er udviklet i samarbejde med det danske IT-sikkerhedsfirma CyberPilot, som har specialiseret sig inden for simulerede phishing-angreb. Der er derfor ingen skade sket.

Formålet med det simulerede phishingangreb er at evaluere på vores reaktionsevne i sådanne situationer og finde ud af, hvor vi kan blive bedre. Meningen er ikke at slå nogen i hovedet, men at gøre jer opmærksomme på, hvordan I kan opdage phishing-mails og skal håndtere dette i tilfælde af et ægte phishingangreb.

Overordnet set (har I klaret jer godt/er der noget at arbejde videre med/status på kampagnen) Resultatet af kampagnen kan I se herunder:

* x modtog phishing-mailen
* x trykkede på linket i phishing-mailen
* x indsendte data

(Skriv her din egen kommentar til resultatet).

**Hvordan kan vi genkende en phishingmail, og hvad er det rigtige at gøre?**

De ledetråde, man kunne finde i mailen, er:

1. Ledetråd 1
2. Ledetråd 2
3. Ledetråd 3

**Hvad er det rigtige at gøre?**

* (Procedure: nævn jeres procedure)
* (Ansvarshavende: nævn ansvarshavende)
* (Politik: Hvad er den nu igen?)

Jeg vil gerne rose de medarbejdere, der har været skarpe og anmeldt mailen til (IT-afdelingen/DPO/etc.) - godt arbejde! Husk at I altid bør tage fat i (IT-afdelingen/DPO/etc.), hvis I er det mindste i tvivl. På den måde står vi stærkest :-)

Hvis I har nogle spørgsmål til ovenstående, er I meget velkomne til at svare på denne mail eller stikke hovedet ind til mig.