Hej alle

I forbindelse med vores IT-sikkerhedstræning har vi valgt at gennemføre simulerede phishing-angreb i samarbejde med CyberPilot, et anerkendt dansk IT-sikkerhedsfirma, som vi også samarbejder med om vores Awareness-træning

**Hvad er et simuleret phishing-angreb?**

Et simuleret phishing-angreb indebærer udsendelse af en e-mail, der ligner en typisk spam/phishing/falsk-email. E-mailen kan indeholde et link, og modtagerne kan blive bedt om at indtaste data.

Vi vil kunne følge med i:

* Antallet af modtagere
* Antallet af klik på linket
* Antallet af personer, der indtaster data

**Hvorfor?**

Formålet med disse simulerede phishing-angreb er at teste vores evne til at identificere phishing-e-mails og at træne vores organisation i, hvordan man skal reagere på et sådant angreb. Det vil give os mulighed for at identificere områder, hvor IT-afdelingen kan forbedre sig.

Det er vigtigt at understrege, at formålet ikke er at hænge nogen ud, men derimod at træne i at opdage phishing-mails, reagere hensigtsmæssigt og håndtere situationen i tilfælde af et reelt phishing-angreb.

**Hvornår?**

Vi vil gennemføre en eller flere phishingsimuleringer inden for den nærmeste fremtid på et vilkårligt tidspunkt.

Vi håber, at I vil opfatte dette som en lærerig øvelse, der kan give jer indsigt i, hvordan forskellige phishing-angreb kan se ud, og hvordan man kan opdage dem.

Hvis I har spørgsmål angående øvelsen, er I velkomne til at kontakte xxx.

Vi ser frem til at se, hvordan vi klarer os, og husk, at vi gør dette for at styrke voressikkerhed i fællesskab.