# Svar på spørgsmål stillet af Arne Bech (H) på Økonomiudvalgets møde den 13. juni 2022

# NOTAT

HVIDOVRE KOMMUNE

Center for Digitalisering
Kommunikation og Erhverv
IT- og Digitalisering
IT- og Digitaliseringschef:
Lasse Wamsler

Dato: 07. juli 2022/lqw

**Spørgsmål:**
Arne Bech (H) spurgte til spamfilter – det sorterer for meget fra.

**Besvarelse:**
Center for Cybersikkerhed har fornyeligt hævet trusselsniveauet for cyberaktivisme. Angriberne bliver stadig smartere og udnytter i større stil medarbejdernes e-mail til at skabe sig adgang til it-infrastrukturen.
I Hvidovre Kommunes it-afdeling er vi løbende opmærksomme trusler og håndterer jævnligt hændelser, som kan betragtes som forsøg på uautoriseret adgang til kommunens it-infrastruktur eller systemer.

Et af de vigtige områder for en styrket cybersikkerhed er medarbejdernes bevidsthed omkring links i e-mails. Er e-mails ikke fra en kendt modtager, kan det vise sig at det er et forsøg på angreb via Phishing.
Phishing er en speciel type it-kriminalitet, hvor hackere prøver at lokke brugeren til at give dem fortrolige oplysninger. Det kan være alt fra navn og adresse over passwords til Facebook-sider, e-mailkonti eller linker til hjemmesider med skadelig kode.

Hvidovre Kommune modtager i gennemsnit ca. 1100 Phishing e-mails dagligt. I it-afdelingen har vi sikret kommunen på flere niveauer. Et spamfilter, som analyserer alle indkomne e-mail, og som automatisk frasorterer de helt åbenlyse forsøg på Phishing. I en promille af disse e-mails kan sikkerhedsløsningen ikke vurdere indholdet og i tvivlstilfælde sættes e-mailen i karantæne. Sikkerhedsløsningen lærer løbende hvilke e-mails som frigives. Det betyder, at man hen over tid får færre og færre e-mails nogen skal forholde sig til.

It-afdelingen åbnede i starten af juni måned op for at brugerne selv kunne komme ind i karantæneområdet (man fik et link tilsendt) og frigive eller slette e-mails.

Det viser sig dog at det for brugerne opleves som et forstyrrende element i hverdagen og det er derfor besluttet i DKE at rulle denne mulighed tilbage. Dette betyder nu, at brugerne ikke egenhændigt skal frigive karantæneramte e-mails, da IT-afdelingen hver morgen gennemgår karantænelisten og frigiver e-mails fra sikre afsender-domainer (fx kbh@**avisen.dk**).