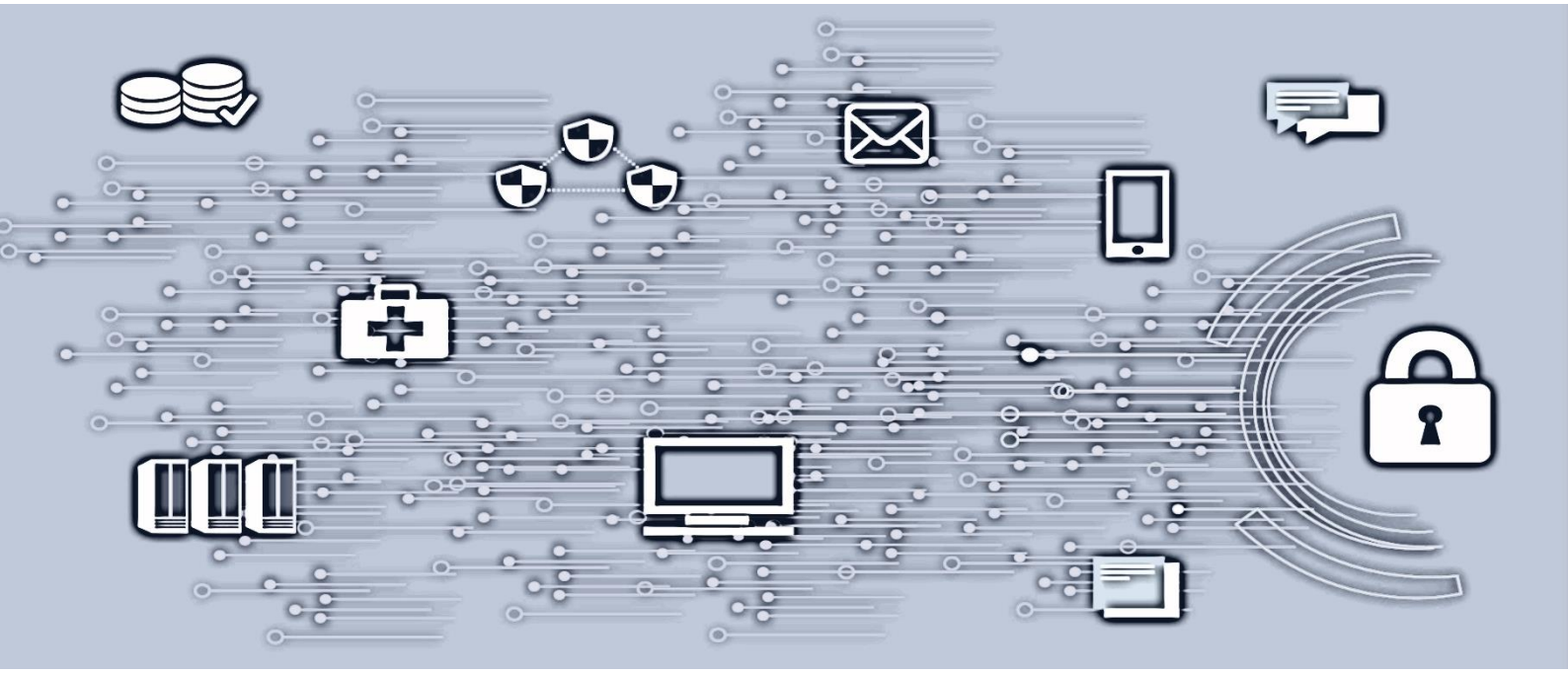
SYKEHUSPARTNER

Rapportering av ondsinnet e-post



Innhold

Versjon	Dato	Godkjent av
1.0	21.05.2020	Christian Jacobsen
1.1	11.11.2022	Christian Jacobsen

1. Hensikt

Dette dokumentet inneholder prosedyre hvordan sluttbruker («mottaker av ondsinnet e-post») skal rapportere denne.

2. Tips for å gjenkjenne ondsinnet e-post

Sykehuspartner HF har implementert en rekke tiltak og kontroller for å forhindre ondsinnet e-post fra å nå sluttbruker, men det er likevel sannsynlig at ondsinnet e-post vil nå sluttbruker. Det er derfor viktig at sluttbruker gjenkjenner ondsinnet e-post, og følger denne prosedyren.

Hvem som helst kan sende e-post, og utgi seg for å være noen andre. Den som mottar e-post må derfor være kritisk til at e-posten kan være falsk, selv om den ved første øyekast fremstår å være fra en kjent avsender.

Ved mottak av e-post må sluttbruker derfor utøve kritisk sans, man kan ikke automatisk stole på at e-posten er ekte. Mottaker kan anvende noen raske visuelle kontroller ved e-poster:

- Er e-posten uventet eller unormal?
- Er det språklige svakheter i e-posten som kan indikere maskinoversetting?
- Har e-posten en annen avsenderadresse enn avsender normalt sett bruker?
- Pleier avsender å sende slike e-poster?
- Ber avsender om at du skal utføre noe ikke-spesifikt eller noe som normalt sett ikke er innenfor ditt ansvarsområde?
- Inneholder e-posten linker eller vedlegg som fremstår som unormale?
- Har du en mageføelse om at e-posten kanskje ikke er ekte?

Vedlagte er en eksempel på en e-post, sammen med 5 indikatorer for å avdekke at e-posten er falsk:

1. Avsenderadressen er ikke avsenders normale adresse.
2. Underlig emnefelt – ingen relasjon til innholdet i e-posten.
3. «Hvordan går dagen din» er litt haltende norsk, kan tyde på maskinoversatt fra «How's your day».
4. Vanlig taktikk er å ikke være for spesifikk med en gang – men få startet en dialog med sluttbruker, hvor omfanget av «noe» gradvis vil øke.
5. Vanlig taktikk er å skape en «sense of urgency» hos sluttbruker, og en måte å oppnå dette på er å si at e-posten er sendt fra en annen enhet enn normal PC.

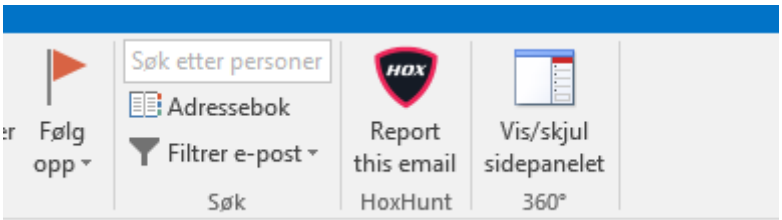
3. Hvem mottar ondsinnet e-post?

Alle vil i utgangspunktet være et mål for ulike typer ondsinnet e-post, men erfaringsmessig vil personer i ledende stillinger være mer utsatt. Toppledelse og andre medarbeidere med betalingsfullmakt vil være attraktive mål for ulike typer økonomisk svindel. Andre typer medarbeidere med ulike typer kjernekompetanse kan være utsatt for andre typer trusler, f.eks. etterretningsaktiviteter som industrispionasje.

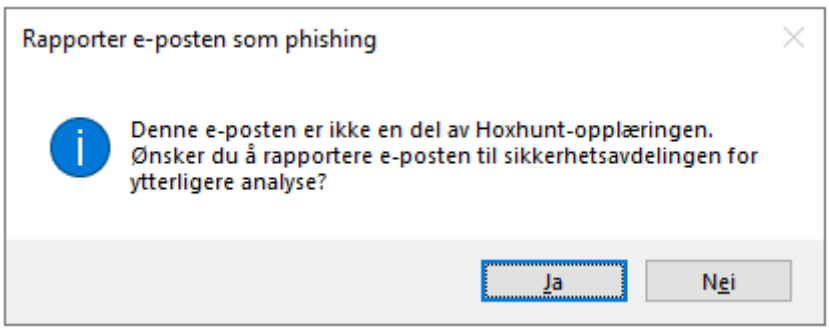
4. Rapportere ondsinnet e-post

Sykehuspartner HF benytter opplæringsprogramvare for simulering av ondsinnet e-post. Dette programmet er også egnet for å rapportere potensiell ondsinnet e-post på en enkel måte.

Ved mottak av potensiell ondsinnet e-post, så kan brukeren klikke på Hoxhunt-ikonet.



Om e-posten ikke er en del av simuleringen fra Hoxhunt, vil brukeren få en ny informasjonsboks:



Ved å bekrefte, videresendes den mistenkelige e-posten til Sykehuspartner CERT.

Husk å ikke svare på e-post som du tror kan være falsk. Ikke klikk på linker eller åpne vedlegg som du mener er unormale. Aldri aksepter bruk av e-post som grunnlag for utbetalinger av refusjoner, faktura e.l., bruk alltid godkjente systemer for slike transaksjoner.