PHISHING-E-POSTER FRA "BANKEN"

Phishing er bruk av falske e-poster for å lure mottakerne til å dele personopplysninger eller informasjon om økonomi eller sikkerhetstiltak.

HVORDAN FUNGERER DET?

Disse e-postene:

ser kanskje ut som en type korrespondanse en faktisk bank ville sendt ut.

etterligner logoene, layouten og tonen i ekte e-poster.

ber deg laste ned et vedlegg eller klikke på en lenke.

bruker et språk som antyder at det haster.

HVA KAN DU GJØRE?

- **Hold all programvare oppdatert,** som nettleseren din, antivirusprogrammet og operativsystemet.
- Vær særlig **oppmerksom** hvis du i en e-post fra banken blir bedt om å oppgi sensitive opplysninger (f.eks. passordet til nettbanken din).
- **Se nøye på e-posten:** Sammenlign adressen med tidligere ekte meldinger fra banken din. Se etter dårlig språk og stavefeil.
- **Ikke svar på mistenkelige e-poster,** men videresend dem til banken din og skriv inn adressen selv.
- **Ikke klikk på lenken eller last ned vedlegget,** men skriv inn adressen i nettleseren.
- Er du i tvil, **dobbeltsjekk** informasjonen på bankens nettsider eller ta en telefon til banken.

Datakriminelle utnytter det faktum at folk har det travelt – ved første øyekast ser disse falske e-postene ekte ut.

Vær forsiktig når du bruker mobile enheter. Det kan være vanskeligere å oppdage et phishing-forsøk fra en telefon eller et nettbrett.

#CyberScams

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLITIET KRIPOS | NorSIS Norsk senter for informasjonssikring | mnemonic SECURING YOUR BUSINESS