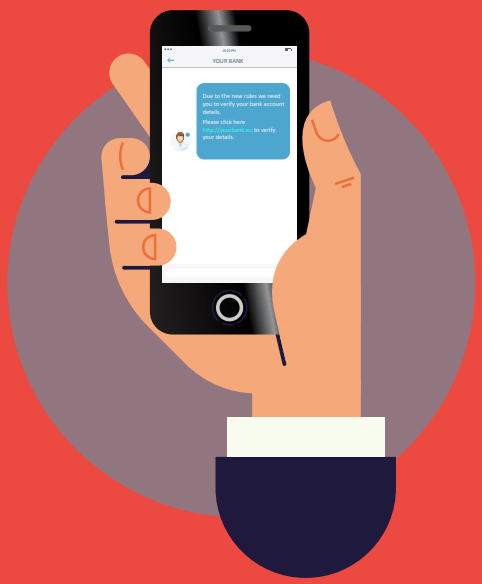
SMISHING-SMS-ER FRA "BANKEN"

Smishing (som kombinerer ordene "SMS" og "phishing") er når svindlere forsøker å innhente personopplysninger eller informasjon om økonomi eller sikkerhetstiltak via tekstmeldinger.



HVORDAN FUNGERER DET?

I tekstmeldingen bes du typisk om å klikke på en lenke eller ringe et telefonnummer for å "verifisere", "oppdatere" eller "reaktivere" kontoen din. Lenken fører imidlertid til en falsk nettside, mens telefonnummeret leder til en svindler som utgir seg for å representere det aktuelle firmaet.

HVA KAN DU GJØRE?

- **Ikke klikk på lenker, vedlegg eller bilder** du mottar i uventede tekstmeldinger, uten først å sjekke avsenderen.
- **Ikke ha det travelt.** Ta deg god tid til å foreta nødvendige undersøkelser før du svarer.
- **Ikke svar på tekstmeldinger** som ber deg oppgi PIN-koden din, passordet til nettbanken eller annen sikkerhetsinformasjon.
- Hvis du tror at du kan ha svart på en smishing-SMS og oppgitt bankopplysninger, må du **kontakte banken din umiddelbart.**

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