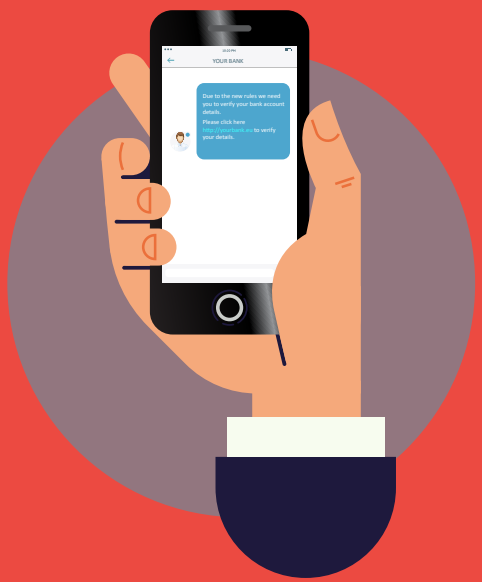
BANK PHISHING SMS'ER

Smishing (en kombination af ordene sms og phishing) anvendes af bedragerne i forsøg på at indhente personlige, finansielle eller sikkerhedsmæssige oplysninger via sms.



HVORDAN FOREGÅR DET?

Sms-beskeden vil typisk bede dig om at klikke på et link eller ringe til et telefonnummer for at 'bekræfte', 'opdatere' eller 'genaktivere' din konto. Men ... linket fører til en falsk hjemmeside og telefonnummeret fører til en bedrager som foregiver at være et legitimt selskab.

HVAD KAN DU GØRE?

- **Klik ikke på links, vedhæftede filer eller billeder,** som du modtager i uopfordrede tekstbeskeder uden først at verificere afsenderen.
- **Forhast dig ikke.** Tag din tid og foretag de nødvendige tjek, før du svarer.
- **Besvar aldrig en tekstbesked,** der anmoder om din PIN-kode eller din adgangskode til bank eller andre sikkerhedsoplysninger.
- Hvis du tror, at du måske har besvaret en smishing sms og oplyst dine bankoplysninger, skal du **straks kontakte din bank**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | POLITI | FINANS DANMARK | #CyberScams