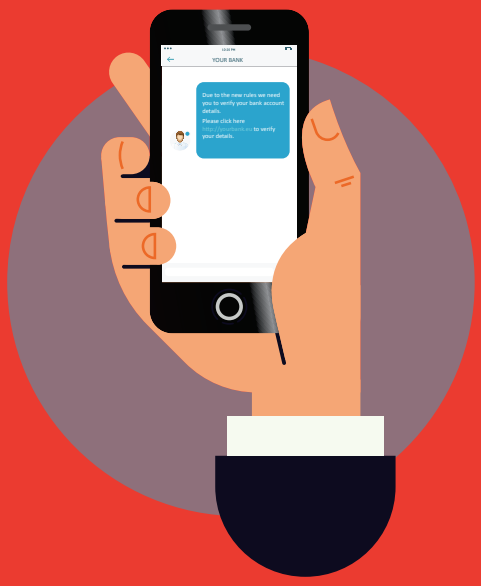
SMISHING: SMS'EN VAN EEN VALSE BANK

Smishing (combinatie van SMS en phishing) is een poging van fraudeurs om via sms persoonlijke, financiële of beveiligingsinformatie te verkrijgen.



HOE WERKT HET?

In de sms wordt er je meestal gevraagd op een link te klikken of een telefoonnummer te bellen om je account te 'verifiëren', te 'updaten' of 'opnieuw te activeren'. Maar de link leidt naar een valse website en het telefoonnummer naar een fraudeur die zich voordoet als het echte bedrijf.

WAT KAN JE DOEN?

- **Klik niet op links, bijlagen of afbeeldingen** die je ontvangt in ongevraagde sms-berichten zonder eerst de afzender te controleren.
- **Laat je niet opjagen.** Neem je tijd en voer de nodige controles uit voordat je reageert.
- **Reageer nooit op een sms-bericht** waarin je PIN of wachtwoord voor online bankieren of andere veiligheidsgegevens worden gevraagd.
- Als je denkt dat je op een smishingbericht hebt gereageerd en je bankgegevens hebt opgegeven, **contacteer onmiddellijk je bank.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | Politie Police | febelfin | CYBER SECURITY COALITION | #CyberScams