Word geen slachtoffer van spoofing

Samen met WhatsApp-fraude is het zogenoemde 'bank spoofing' of bankhelpdeskfraude een van de grootste oplichtingsgevaren van dit moment. Criminelen bellen u op met een echt lijkende vervalst telefoonnummer van de bank. Ze vertellen u dat uw bankrekening in gevaar is.

Trap er niet in
In werkelijkheid is dat niet zo. Maak geen geld over en stuur ook nooit een doorgeknipte pinpas op. De criminelen kunnen uw pas repareren en daarna uw bankrekening leeghalen.

Hoe werkt bankhelpdeskfraude?
- 'De bank' belt u.
- Het vervalste telefoonnummer lijkt op of is hetzelfde als dat van uw eigen bank.
- De nepbankmedewerker zegt dat er verdachte activiteiten zijn op uw rekening. Hij vertelt u dat u uw geld moet veiligstellen. Of dat u een nieuwe pinpas nodig heeft.
- Soms bieden de criminelen aan te 'helpen' door uw computer op afstand over te nemen, bijvoorbeeld via Teamviewer.

Hoe wordt u geen slachtoffer?
Wees altijd waakzaam. Communicatie per telefoon, e-mail, sms en brief kan nep zijn. Let bij bankhelpdeskfraude op het volgende:
- Als u twijfelt, vraag dan de 'medewerker' om zijn naam. Hang op en bel zelf naar uw bank.
- Trap niet in informatie waarmee de oplichter wil bewijzen dat hij echt een bankmedewerker is. Soms weet hij persoonlijke gegevens van u, bijvoorbeeld via social media.
- Zorg ervoor dat u niet teveel geld op uw betaalrekening heeft staan. De schade blijft dan beperkt. Ook als bijvoorbeeld uw pinpas wordt gestolen.
- Stel een lage daglimiet in. Verhoog deze ook niet onder druk van een (nep)medewerker.

Toch opgelicht?
Bent u toch slachtoffer van (poging tot) oplichting? **Bel direct uw bank!** Zo voorkomt u nog meer schade. En het helpt u bij het aanvragen van een vergoeding. Doe ook aangifte bij de politie via 0900-8844 of meld het via de website van de Fraudehelpdesk: https://www.fraudehelpdesk.nl/fraude-melden/ .

Bron: politie.nl