

# BANK PHISHINGMAILS

Phishing verwijst naar frauduleuze e-mails die de ontvangers misleiden om hun persoonlijke, financiële of beveiligingsinformatie te delen.

## HOE WERKT HET?

Deze e-mails:

kunnen er identiek **uitzien** als de correspondentie die echte banken uitsturen.

**kopiëren** de logo's, lay-out en toon van echte e-mails.



**vragen** je een bijlage te downloaden of op een link te klikken.



**gebruiken** dwingende taal.

## WAT KAN JE DOEN?

- > Hou je software up-to-date, inclusief je browser, antivirus en besturingssysteem.
- > Wees vooral **waakzaam** als een 'bank' via mail gevoelige informatie van je vraagt (bv. je wachtwoord voor online bankieren).
- > **Kijk goed naar de e-mail:** vergelijk het adres met eerdere echte berichten van je bank. Controleer op slechte spelling en grammatica.
- > **Antwoord nooit op een verdachte e-mail**, maar stuur het door naar je bank door het adres zelf in te typen.
- > **Klik niet op de link of download de bijlage niet**, maar typ het echte adres van je bank over in je browser.
- > **Controleer** in geval van twijfel de website van je bank of bel de bank.



Cybercriminelen rekenen erop dat mensen het druk hebben; op het eerste gezicht lijken deze nepmails echt.



Kijk uit wanneer je een mobiel toestel gebruikt. Het kan moeilijker zijn om een phishingpoging op je telefoon of tablet te herkennen.

#CyberScams

