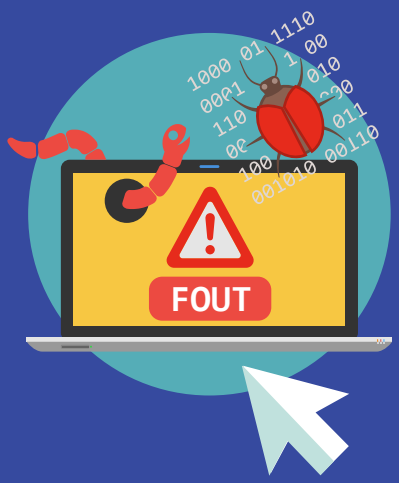
VALSE BANKWEBSITES

Phishingmails van fraudeurs die zich voordoen als banken bevatten meestal links naar een valse bankwebsite waar je wordt gevraagd om je financiële en persoonlijke gegevens te geven.



HOE HERKEN JE HET?

Valse bankwebsites zien er bijna hetzelfde uit als echte websites.

Kenmerken van deze websites:

Dwingende taal: je bank gebruikt dergelijke taal niet op haar website.

Pop-upvensters: ze worden vaak gebruikt om gevoelige informatie van jou te verzamelen. Klik er niet op en geef je persoonsgegevens niet via deze vensters.

Slechte opmaak: wees voorzichtig met websites die design-, spelling- of grammaticafouten vertonen.

WAT KAN JE DOEN?

Klik nooit op links in e-mails die lijken te leiden naar de website van je bank.

Typ de link van je bank altijd handmatig of gebruik een bestaande link uit je 'favorieten' lijst.

Stel je browser zo in dat **pop-upvensters worden geblokkeerd.**

Als iets belangrijks echt je aandacht vereist, zal je bank je waarschuwen **wanneer je je onlinerekening raadpleegt.**

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