# Phishing

PDF Versie

## Wat is Phishing ?

**Phishing** (afgeleid van *fishing*: "vissen", "hengelen") is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar een valse website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met persoonlijke gegevens (paswoorden, nummer van een bank-/kredietkaart, nummer of fotokopie van de identiteitskaart, geboortedatum). Hierdoor krijgt de fraudeur de beschikking over deze gegevens met alle gevolgen van dien. De fraudeur doet zich hierbij voor als een vertrouwde instantie, zoals een bank.

De meeste vormen van phishing gebeuren via e-mail of tekstbericht. De slachtoffers worden hierbij met een email naar deze valse website gelokt. Het bericht bevat een link naar de (valse) website met het verzoek om zogenaamd "de inloggegevens te controleren" of "een achterstallige betaling uit te voeren".

Eens de verdachte toegang heeft verkregen tot de bankrekening van het slachtoffer zal hij trachten geld over te maken naar rekeningen van moneymules die op voorhand werden gerecruteerd en die werken in opdracht van de verdachte.

## Wat heb je nodig om klacht neer te leggen?

- Alle beschikbare informatie omtrent de gevoerde communicatie
    - gsm-nummers, e-mailadressen en technische headers (https://mxtoolbox.com/public/content/emailheaders/)
    - Afdruk van het phishingbericht

    - De URL of link waarop u hebt geklikt
- Alle beschikbare informatie omtrent de gevoerde betalingen
    - rekeningnummers
    - schermafdrukken van de betaling

## Wat kan je nog doen?

- de bank op de hoogte te brengen van het ontvangen bericht en van de phishingactie;
- wachtwoorden van de online bankaccount te veranderen of deze te blokkeren;
- voer een anti-virus en anti-malware scan uit;
- contacteer indien nodig CardStop via 070/344.344

## Hoe vermijd je om opnieuw slachtoffer te worden?

Aanwijzingen dat het gaat om een phishing-e-mail :

- De e-mail verwijst naar een website die sterk lijkt op een vertrouwde website.
- Het bericht komt onverwacht of houdt geen steek.
- Het onderwerp en de aanspreking van de e-mail is vaag.
- Hij is in je spam beland.
- De toon is alarmerend, bedreigend of intrigerend. Je moet zo snel mogelijk reageren of er zullen gevolgen zijn.

Neem de juiste reflexen aan bij phishing :

- Beantwoord het bericht niet!
- Controleer de correctheid van het emailadres van de verzender: zweef over de afzender zodat het volledige e-mailadres zichtbaar wordt. De 2 laatste woorden achter @ geven het het domein van het bedrijf weer. Controleer of dit overeenstemt met het officiële domein van dit bedrijf.
- Overloop de links om de betrouwbaarheid ervan na te gaan: zweef over de link zodat het webadres dat erachter zit zichtbaar wordt.
- Wantrouw bijlagen, bestanden en afbeeldingen. Doe deze niet zomaar open en gebruik een degelijke virusscanner.

- Doe geen transacties via een onbekend systeem of een ander dan gebruikelijk betalingssysteem, of via een gewijzigd rekeningnummer.
- Tik altijd zelf het webadres van de site die je wilt bezoeken in.

**Bij twijfel: neem het zekere voor het onzekere!**
**Zet alle transacties stop en contacteer onmiddellijk uw bank.**

## Waar vind je meer informatie?

https://campagne.safeonweb.be/nl/phishing