

Phishing

Phishing ('hengelen' in het Nederlands) is een vorm van cybercriminaliteit waarbij de criminelen:

- Zich voordoen als iemand anders, bijvoorbeeld je bank, de overheid, je energieleverancier, maar even goed een vriend of familielid.
- Je benaderen via e-mail, sms, sociale media of telefoon.
- Proberen om gevoelige gegevens te krijgen, zoals jouw wachtwoorden, bank- of kredietkaartgegevens. Zo kunnen ze toegang krijgen tot jouw accounts en je geld of identiteit stelen.

Tips om phishing te voorkomen

Krijg je een verdachte mail, sms of telefoon? Stel je volgende vragen:

1. **Is het onverwacht?**
Krijg je zonder reden een bericht van iemand die je niet kent, bij wie je niets gekocht hebt, met wie je lang geen contact hebt gehad ...? Controleer het. Dat kan bijvoorbeeld door te bellen naar het bedrijf of de kennis van wie het bericht zagezegd kwam en hen te vragen of ze je echt iets hebben gestuurd.
2. **Is het dringend?**
Wees op je hoede als je onder druk wordt gezet. Zo proberen criminelen je minder tijd te geven om na te denken. Laat je niet opjagen.
3. **Ken je de afzender?**
Controleer het e-mailadres, ook op spellingsfouten. Maar let op: een echt e-mailadres is geen garantie. Onbekend nummer? Bel niet zomaar terug bij een gemiste oproep of bericht van een onbekend nummer? Dat kan je veel geld kosten.
4. **Vind je de vraag vreemd?**
Een officiële instantie zal je nooit via e-mail, sms of telefoon vragen naar je wachtwoord, bankgegevens of persoonlijke gegevens. Geef die gegevens nooit door via die kanalen.
5. **Heeft het bericht een link?**
Klik er niet op, maar zweef erover met je muis. Is de domeinnaam ook echt de naam van de organisatie? In een mail van de stad Maaseik kan je verwachten dat de link verwijst naar www.maaseik.be, waarbij 'maaseik.be' het domein is. Staat er iets anders dat erop lijkt, bijvoorbeeld 'maas3ik.be' of 'maaseik-be.be'? Dan gaat het om een vals domein. Klik je op de link, dan kom je op een nagemaakte website van criminelen terecht.
6. **Word je niet persoonlijk aangesproken?**
Berichten met algemene en vage aanspreektitels, of met je e-mailadres als aanspreking, vertrouw je beter niet.
7. **Bevat het bericht taalfouten?**
Vakkundige cybercriminelen zorgen voor correcte taal, maar taalfouten of het gebruik van een vreemde taal kunnen wijzen op een verdacht bericht.
8. **Herken je een vals bericht op tijd?**
Stuur het dan naar verdacht@safeonweb.be.

[Wees slimmer dan een phisher](#)

Doe aangifte

Ben je toch in de val gelopen?

1. **Heb je jouw bankgegevens doorgegeven?**
Neem dan onmiddellijk contact op met je bank. Die kan verdachte transacties soms nog blokkeren of je rekening bevroren.
2. **Heb je jouw kredietkaartgegevens doorgegeven?**
Waarschuw dan onmiddellijk [Cardstop](#). Als je een wachtwoord hebt doorgegeven dat je ook op andere plaatsen gebruikt, verander het meteen.
3. **Doe aangifte bij politie Maasland.**

[Je kan op verschillende manieren aangifte doen bij politie](#)

