



Bron: <https://safeonweb.be/nl/leer-valse-mails-herkennen>

Phishing is oplichting via valse e-mails, sms'jes, websites of andere berichten. Cybercriminelen doen zich voor als een organisatie of persoon die je kent of vertrouwt, en spelen vaak in op tijdsdruk of angst. Zo proberen ze je te laten klikken, gegevens te laten delen of een betaling te laten uitvoeren. Met de onderstaande tips herken je verdachte berichten sneller. Twizzit en je club zullen je nooit via e-mail, sms of telefoon naar je wachtwoord vragen.

Hoe verdachte berichten herkennen?

Vind je een mail of telefoontje verdacht? Beantwoord dan deze vragen:

- **Is het onverwacht?**
Krijg je zonder reden een bericht van deze afzender: je kocht niets, had lang geen contact, enz. Controleer zeker verder.
- **Is het dringend?**
Hou je hoofd koel: kreeg je echt een eerste aanmaning tot betaling? Ken je die 'vriend in nood' wel?
- **Ken je de afzender?**
Controleer het e-mailadres, ook op spellingsfouten. Maar let op: een legitiem e-mailadres is geen garantie.
- **Vind je de vraag vreemd?**
Een officiële instantie zal je nooit via e-mail, sms of telefoon vragen om je wachtwoord, bankgegevens of persoonlijke gegevens.
- **Naar waar leidt de link waar je moet op klikken?**
Zweef met je muis over de link. Is de domeinnaam, het woord voor .be, .com, .eu, .org, ... en voor de allereerste slash "/", ook echt de naam van de organisatie?
Een voorbeeld:
 - Bij de link **www.safeonweb.be/tips** is het domein safeonweb.
 - Bij de link **www.safeonweb.tips.be/safeonweb** is 'tips' het domein en word je naar een andere website geleid.
- **Staat er een QR-code in het bericht?**
Als er een QR-code wordt getoond, moet je goed nakijken naar welke website die doorverwijst. Als je de code scant, krijg je de URL te zien. Controleer het domein zoals hierboven beschreven.
- **Word je persoonlijk aangesproken?**
Berichten met algemene en vage aanspreektitels, of je e-mailadres als aanspreking, die wantrouw je beter.
- **Bevat het bericht veel taalfouten?**
Ook al zorgen doorgewinterde cybercriminelen voor correcte taal, taalfouten of een vreemde taal kunnen wijzen op een verdacht bericht.
- **Zit het bericht in je Spam/Junk folder?**
Indien ja, wees extra voorzichtig. Je kan ook zelf verdachte berichten markeren als Spam of Junk en zo anderen waarschuwen.

- **Probeer iemand je nieuwsgierig te maken?**

Iedereen zou nieuwsgierig worden bij berichten met een link als "Kijk wat ik over jou las ..." of "Ben jij dit op deze foto?", maar laat je niet vangen.

- **Wordt er gevraagd om een betaling uit te voeren?**

Als er gevraagd wordt om een betaling uit te voeren die je niet verwacht, moet je altijd voorzichtig zijn. Is het rekeningnummer hetzelfde nummer als je gewoonlijk gebruikt om die organisatie of persoon te betalen? Als dat niet het geval is, voer de betaling dan niet uit. Vaak worden in phishingmails buitenlandse rekeningnummers gebruikt of wordt gevraagd om betalingen te doen via een cryptowallet. Dit is verdacht.

Als je twijfelt over een betaling, informeer je dan eerst bij je bank, of bij de instelling die de betaling opeist. Doe dit niet via de contactgegevens in de e-mail, maar ga rechtstreeks naar de website van de organisatie zelf.

Voorbeelden van valse berichten

<https://safeonweb.be/nl/leer-valse-mails-herkennen>

Wat te doen als je een verdacht bericht krijgt?

- Klik niet op een link in een verdacht bericht, open de bijlages niet en download geen applicaties als daar om gevraagd wordt.
- Verdachte e-mails kan je doorsturen naar verdacht@safeonweb.be.
- Verdachte sms'jes kan je ook doorsturen. Maak een screenshot en verstuur die naar verdacht@safeonweb.be. De inhoud wordt dan automatisch verwerkt.

Heb je op een verdachte link geklikt?

- Heb je toch geklikt? Vul dan verder niets in en breek elke interactie af.
- Geef NOOIT persoonlijke gegevens of codes door.
- Als je een wachtwoord hebt doorgegeven dat je ook op andere plaatsen gebruikt, verander het dan onmiddellijk.
- Als je op een link hebt geklikt die opent in een website waar je bankgegevens moet invullen, controleer dan eerst of dit de echte website van je bank is. Bij de minste twijfel voer je geen betaling uit.
- Merk je dat er namens jou rare berichten verstuurd worden? Waarschuw je contacten dat er vanuit jouw account valse berichten verstuurd zijn.

Ben je opgelicht?

- Onderneem snel actie en volg het advies op:
<https://safeonweb.be/nl/opgelicht>