

Herken de scammail



De allerkorste

Security Awareness Training



Wees niet naïef over cybersecurity

7 rode vlaggen

1. Is de email op enige manier RAAR?
2. Gaat het over geld of iets van waarde?
3. Speelt het in op hebzucht, gewoonte of angst.
4. Komt het van een bank, autoriteit of groot bedrijf?
5. Staat er een (gevaarlijke) link in?
6. Zit er een (gevaarlijke) bijlage bij?
7. Waarom krijg IK deze mail?

- **Autoriteit** (directeur, politie, deurwaarder, incassoburo)
- **Grote bedrijven** (Bol.com, Ziggo, KPN, Microsoft, Office365)

- **Geld / waarde** (Euro, bitcoin, kadokaart, telefoonkaart)
- **Schuldgevoel** (Factuur, invoice, aanmaning, boete)

Gebruik **NOOIT** de login-link en open nooit zomaar de bijlage

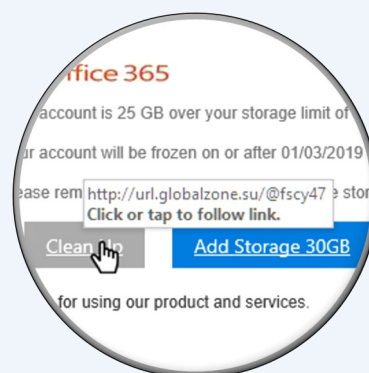
Bij geringste twijfel NIET klikken en gewoon DELETEN

Klopt het adres van de afzender 100%:

- Is er niets aan de naam toegevoegd (letter of woord) of is er niet een letter anders (l ipv 1 of rn ipv m)

Herken een scamlink in de e-mail:

- **Hover** (plaats zonder te klikken je muis op de link) in je emails. Dan zie je het werkelijke webadres van de link verschijnen.
- **Kijk goed naar het afzenderadres.** Vooral naar het adres tussen < >. Als je die niet ziet, doe dan een forward van de mail (zonder te verzenden en kijk dan in de **From** regel in de tekst.



Wantrouw **ELKE** bankrekeningnummer wijziging:

- Elk email verzoek voor wijziging van het rekeningnummer van een factuur of voor salarisbetaling is verdacht. Ook afwijkend lettertypes op een email factuur en stickers op papieren facturen zijn verdacht.

1. **Bel een wijzigingsverzoek altijd na.**
Wijzig niet eerder dan dat u daadwerkelijk de juiste person heeft gesproken.
2. Vergelijk het bankrekeningnummer op elke factuur met het nummer in uw administratie.



Nog meer Security tips

5 wachtwoord tips die de hack kans met 99% verminderen:

- Log nooit in via een link in een email.
- Gebruik multifactor authenticatie waar mogelijk.
- Gebruik altijd een sterk (lang) wachtwoord.
- Gebruik overall een verschillend wachtwoord.
- Gebruik een wachtwoordmanager om alle wachtwoorden te beheren.

5 PC security tips voor je prive situatie die je zeker niet mag vergeten:

- Gebruik altijd een goed anti-virus / anti-malware programma.
- Update de PC en je applicaties regelmatig.
- Download & Installeer nooit gekraakte software of freeware van een onbekende site.
- Maak regelmatig een backup van alle bestanden. Koppel de backup daarna los van de PC.
- Laat nooit een laptop in je auto, zelfs niet op standby of afgesloten. Dieven kunnen deze dan nog detecteren.

Denk ook hier aan:

- Wees voorzichtig met gratis wifi. Je weet nooit wie er meekijkt. Log daar nooit in op je email of bankaccount. Of gebruik tenminste een private VPN.
- Maak regelmatig een backup van de foto's op je telefoon. Die herinneringen zijn onvervangbaar.

Security wijsheid:

- Als het te mooi is om waar te zijn, dan is het dat ook waarschijnlijk.
- Geloof nooit een zielig of onwaarschijnlijk verhaal -> controleer.
- Banken vragen niet je login, je pas op te sturen of ivm fraude je geld over te maken naar een kluisrekening.
- Je klant heeft niet ineens een nieuw bankrekeningnummer omdat ze problemen hebben met hun oude bankrekening.
- Je kinderen/partner/vrienden hebben geen nieuw 06 nummer om daarna via whatsapp vragen geld over te maken.

Bij maar de minste twijfel delete of controleer

Better safe than sorry