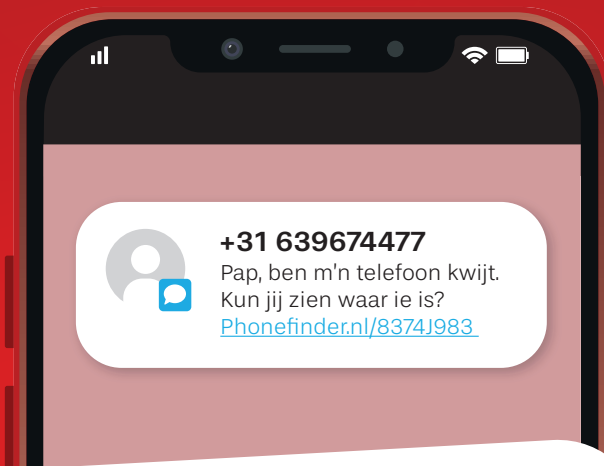




Rijksoverheid



**Laat je niet
interneppen.**

Check de afzender en
bij twijfel: **klik weg!**

laatjenietinterneppen.nl

Laat je niet interneppen.

Zo'n 2,2 miljoen mensen kregen vorig jaar te maken met online criminaliteit. Door de slimme manieren van online misleiding kan iedereen in de val trappen. Criminelen, ofwel interneppers doen zich voor als iemand anders om jouw gegevens te stelen of om je op te lichten via e-mail, sms of WhatsApp. Als ze voor je staan trap je er misschien niet zo snel in, maar online is dat een stuk lastiger. Check daarom altijd de afzender en als je twijfelt: klik weg.

De internepper

Door zich voor te doen als iemand anders en door handig in te spelen op persoonlijke situaties, krijgen criminelen het voor elkaar om je op het verkeerde been te zetten. Een internepper doet aan 'Social Engineering'. Dit is een term voor wisselende trucjes waarmee mensen online worden bedrogen.

Hoe herken je nepberichten?

- **Je krijgt weinig bedenktijd:** de internepper geeft je geen tijd om na te denken, dringt constant aan, blijft vriendelijk en benadrukt dat je direct moet handelen.
- **Het bericht heeft een dwingende toon:** de zogenaamde 'bekende' of 'instantie' verwacht dat je iets betaalt, je wordt gevraagd om op een link te klikken, of je wordt aangespoord om iets te downloaden.
- **De situatie loopt uit de hand:** je krijgt een aanbieding die te mooi is om waar te zijn, je bent nieuwsgierig naar een filmpje of er wordt dringend om jouw hulp gevraagd.

Wat kan je zelf doen?

- Check de afzender: controleer altijd van wie het bericht komt.
- Neem via het bij jou bekende telefoonnummer of e-mailadres contact op als je de afzender niet herkent.
- Let extra goed op bij vreemde e-mailadressen en links, nooit direct klikken.
- Deel niet te veel informatie op social media.
- Deel je wachtwoord niet met anderen.
- Bij twijfel: klik weg.

Kijk op laatjenietinterneppen.nl