

Online en offline oplichting in 2026: deze trucs moet u kennen!

Auteur [Aukeline van Dorp](#); Bron AVROTROS Radar

Oplichters worden steeds slimmer. Waar fraude vroeger vaak makkelijk te herkennen was, maken criminelen in 2026 gebruik van WhatsApp, nepagenten en zelfs gekloonde stemmen door kunstmatige intelligentie (AI).

1. Phishing: valse link in mails of sms

Phishing is nog altijd de bekendste vorm van online oplichting. U krijgt een e-mail, sms of appje die afkomstig lijkt van uw bank, de Belastingdienst of een bekende organisatie. U wordt gevraagd om op een link te klikken en in te loggen.

Let op deze signalen:

- U moet 'direct' iets doen.
- Er wordt bedreigd met afsluiten of boetes.
- De afzender lijkt echt, maar klopt nét niet.

2. Qishing: oplichting via QR-codes

Bij qishing gebruiken oplichters QR-codes in plaats van links. Die codes ziet u bijvoorbeeld op parkeerautomaten, flyers of zelfs op een briefje in de brievenbus. Na scannen komt u op een nepsite terecht. QR-codes lijken betrouwbaar, maar dat zijn ze niet altijd.

3. WhatsApp-fraude: 'Dit is mijn nieuwe nummer'

Een zeer bekende truc die nog steeds veel slachtoffers maakt. U krijgt een WhatsApp-bericht van iemand die zich voordoeft als uw zoon, dochter of kleinkind. Het oude nummer is 'kwijt' en er is dringend geld nodig.

Belangrijk om te weten:

- Oplichters spelen in op emoties.
- Er is altijd haast.
- Er wordt gevraagd om geld over te maken
- Twijfel? Bel uw familielid altijd eerst zelf.

4. Cadeaukaartfraude

Bij deze vorm vraagt iemand u om cadeaukaarten te kopen (bijvoorbeeld van Bol.com of Apple) en de codes door te sturen. Dat gebeurt vaak uit naam van een bekende of 'instantie'.

Onthoud:

- Geen enkele organisatie vraagt om betaling met cadeaukaarten.
- Deel nooit de codes van cadeaukaarten.
- Vertrouw telefoontjes of berichten niet zomaar. Controleer altijd eerst het verzoek.

5. Marktplaats- en betaalverzoekfraude

Koopt of verkoopt u iets via Marktplaats of Facebook Marketplace? Dan kunnen oplichters u een nep-betaalverzoek sturen. Dat lijkt op een iDEAL-link, maar leidt naar een valse website. Ook komt het voor dat u betaalt, maar nooit iets ontvangt.

Tips:

- Gebruik alleen de officiële betaalfunctie.
- Controleer het webadres.
- Wees extra voorzichtig bij 'spoedkopers'.

6. Nepagenten: aan de telefoon of aan de deur

Oplichters doen zich voor als politieagenten. Ze waarschuwen voor zogenaamd gevaar in de buurt en bieden aan uw spullen 'veilig te bewaren'.

Weet dit:

- De politie vraagt nooit om sieraden, geld of pincodes.
- Agenten kunnen zich altijd legitimeren.

7. Onbekende of buitenlandse telefoontjes

U wordt gebeld door een onbekend of buitenlands nummer. Soms hangt de beller direct op, soms krijgt u iemand aan de lijn die zich voordoeft als helpdeskmedewerker.

Doe dit niet:

- Bel niet terug.
- Deel geen gegevens.
- Installeer geen apps.

8. Datingfraude: pig butchering

Bij deze geraffineerde vorm van datingfraude bouwen oplichters langdurig contact met u op, vaak via sociale media. Pas later komt het verzoek om geld te investeren, bijvoorbeeld in crypto. Het lijkt betrouwbaar, maar dat is niet zo: alles is nep.

9. Voice cloning en deepfake-fraude (nieuw)

Acht op de tien Nederlanders heeft moeite om echte berichten te onderscheiden van neppe nu kunstmatige intelligentie (AI) steeds slimmer wordt, [meldde BNR](#) eerder. En dat is niet gek, want met AI kunnen oplichters tegenwoordig zelfs stemmen namaken. Hiervoor hebben ze slechts een paar seconden van uw stem nodig. U krijgt bijvoorbeeld een paniekerig telefoontje van iemand die klinkt als uw (klein)kind of partner.

Zo beschermt u zich:

- Hang op en bel zelf terug.
- Spreek een familiewachtwoord af.
- Laat u niet onder druk zetten.

Daarnaast kunt u ook opgelicht worden met deepfake-afbeeldingen of -video's. Hierbij wordt met AI het gezicht van u, een familielid, kennis of een bekend persoon gebruikt - soms in combinatie met een gekloonde stem - om geld afhandig te maken.

Bent u opgelicht? Dit kunt u doen

1. Neem direct contact op met uw bank

Is er geld afgeschreven? Bel uw bank zo snel mogelijk. Soms kan een betaling nog worden tegengehouden.

2. Doe altijd aangifte

Ook als u denkt dat het geen zin heeft. Aangiftes helpen de politie patronen te herkennen.

3. Verzamel bewijs

Bewaar e-mails, telefoonnummers, screenshots en betaalgegevens.

4. Meld online fraude

Via [Fraudehulpdesk.nl](https://www.fraudehulpdesk.nl) kunt u fraude melden en advies krijgen.