



Digitale fraude voorbeelden

met preventietips

Hulpvraag- fraude

Via bijvoorbeeld WhatsApp

Bij hulpvraagfraude doet een oplichter zich voor als een bekende via bijvoorbeeld WhatsApp. Het lijkt dan alsof uw (klein)zoon, (klein)dochter, of een vriend of vriendin u een bericht stuurt. Er wordt gevraagd om hem of haar snel te helpen door geld over te maken of te klikken op een betaalverzoek.

Vaak staat in het eerste bericht dat de 'bekende' een nieuw mobiel nummer heeft. Ook vragen criminelen soms zelfs om geld via het WhatsApp-account van degene die u kent. Doordat in het bericht staat dat er grote nood is en het geld direct nodig is, zijn veel mensen geneigd om het geld toch maar snel aan 'deze bekende' over te maken. Vertrouw zo'n bericht daarom niet zomaar.

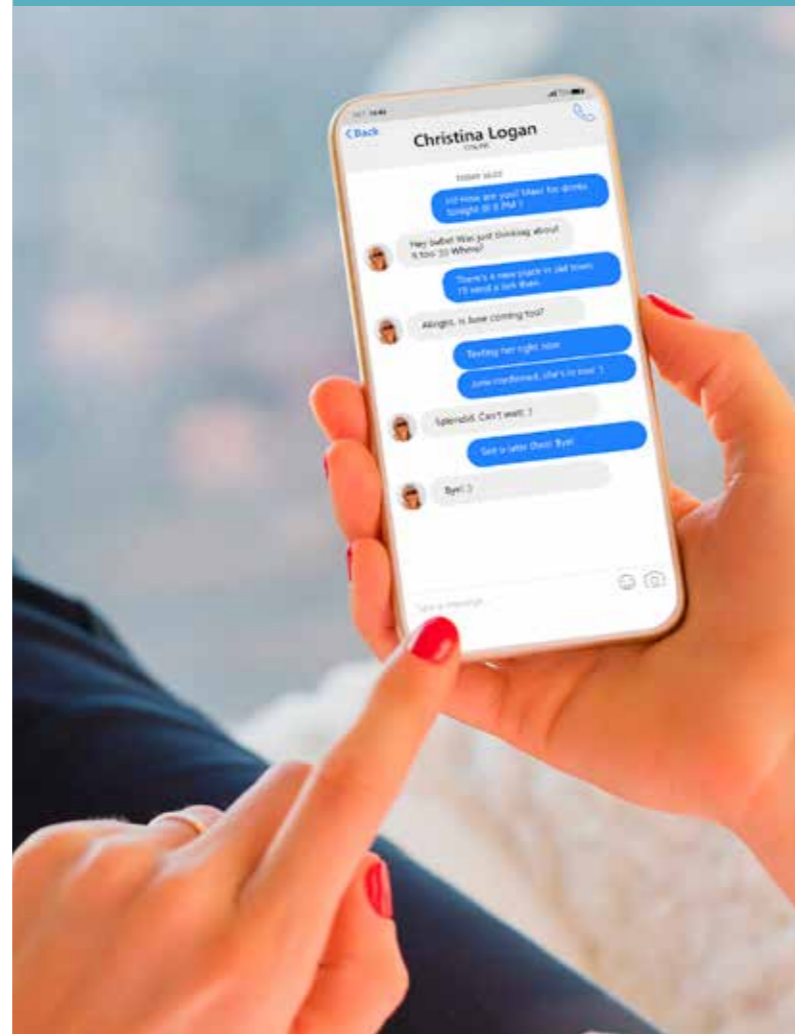
Bel altijd eerst de persoon zelf op het oude nummer en zorg dat u een normaal gesprek met hem of haar kunt voeren. Neem er geen genoegen mee als de persoon zegt u niet te kunnen horen.



Waar kunt u zelf op letten?

Maak nooit zomaar geld over zonder dat u iemand daadwerkelijk heeft gesproken of gebeld. Controleer altijd rechtstreeks bij de bekende door zijn/haar oude nummer te bellen.

Niet gebeld = geen geld.



Hoe voorkomt u dat oplichters u benaderen?

Plaats uw telefoonnummer niet openbaar op sociale media, website of online handelsplatformen, zoals Marktplaats.

Stel tweestapsverificatie in op WhatsApp om te voorkomen dat er misbruik wordt gemaakt van uw account. Dat is een extra beveiliging.

TIP U kunt uw WhatsApp account extra beveiligen door uw profielfoto af te schermen. Dit kan bij WhatsApp via **Instellingen > Privacy > Profielfoto**. Kies hier voor **Mijn contacten**. Dit betekent dat alleen uw contacten uw profielfoto kunnen zien.

TIP Op veiliginternetten.nl/inloggen-in-twee-stappen leest u hoe u tweestapsverificatie instelt.

Bent u toch slachtoffer geworden?

Meld het zo snel mogelijk bij uw bank (ook bij een poging) om het rekeningnummer van de oplichter te laten blokkeren en zo andere slachtoffers te voorkomen.

Doe altijd aangifte bij de politie (ook bij een poging). Dit kan via politie.nl/aangifte of bel **0900 - 8844** om een afspraak te maken.

TIP Maak een screenshot (schermafdruck) van het WhatsApp gesprek, zodat u die bij de aangifte kunt toevoegen.

Ook als u geen slachtoffer bent geworden, is het belangrijk dat u hier een melding van maakt bij de Fraudehelpdesk. Dit kan via fraudehelpdesk.nl/fraude-melden of via telefoonnummer **088 - 7867 372**.

Meer informatie en tips?

Kijk voor meer informatie over hulpvraagfraude op veiliginternetten.nl



Phishing

Via bijvoorbeeld nepmailtjes

Bij phishing (letterlijk: 'hengelen') proberen internet-criminelen toegang te krijgen tot uw computer of persoonlijke gegevens. Dat doen ze via een bericht, bijvoorbeeld een e-mail of sms, waarin u wordt gevraagd om te klikken op een link of om in te loggen. Die link kan bijvoorbeeld leiden naar een valse website van een bank, waarin u gevraagd wordt om uw gegevens in te vullen. Met die gegevens kunnen internetcriminelen u vervolgens veel geld afhandig maken.

Ook vraagt men soms direct om geld over te maken. Via valse e-mails proberen internet-criminelen aan uw geld te komen. Daarom eerst checken, dan klikken.



Waar kunt u zelf op letten

Controleer de link met checklinkje.nl. Klik nooit zomaar op een link die u niet vertrouwt en download geen bijlage.

Twijfelt u? Bel dan de organisatie waar het om gaat, zoals uw bank en zoek daarvoor zelf het telefoonnummer op.

Gaat het om geld? Gaat het om belangrijke gegevens? Is er haast bij? Let op! Eerst checken, dan klikken. Via de website van Fraude-helppdesk kunt u de e-mail controleren op echtheid en melden als fraude.

TIP Lees meer over phishing en wat u hiertegen kunt doen op: veiliginternetten.nl/thema/basisbeveiliging/ik-vertrouw-een-e-mail-niet



Bent u toch slachtoffer geworden?

Meld het onmiddellijk bij uw bank.

Op veiliginternetten.nl/thema/basisbeveiliging/ik-vertrouw-een-e-mail-niet staan speciale e-mailadressen genoteerd van diverse instanties, zoals de belastingdienst en DigiD, waar u een nep e-mail kunt melden.

Doe altijd aangifte bij de politie. Dit kan via politie.nl/aangifte of bel 0900 - 8844 om een afspraak te maken.

Ook als u geen slachtoffer bent geworden, is het belangrijk dat u hier een melding van maakt bij de Fraudehelppdesk. Dit kan via fraudehelppdesk.nl/fraude-melden of via telefoonnummer 088 - 7867 372.

Meer informatie en tips?

Kijk voor meer tips over veilig internetten op veiliginternetten.nl
En voor meer informatie over veilig bankieren op veiligbankieren.nl

Babbeltrucs

Oplichters komen vaak betrouwbaar over. Ze bellen bij u aan, spreken u op straat aan of bellen u op. Zogenaamd namens de bank, de thuiszorg, de gemeente, het waterbedrijf of zelfs om een toiletbezoek voor hun kind. Eenmaal binnen worden op die manier elk jaar vele mensen van hun bezittingen beroofd. Ook proberen oplichters mensen aan de deur te laten pinnenzodat ze uw pincode af kunnen kijken. Als het ze lukt om uw pas te beroven, halen ze zoveel mogelijk geld van uw rekening.

Telefonische babbeltruc

Ook via de telefoon benaderen oplichters mensen, bijvoorbeeld om een bezoek aan te kondigen. Of ze doen zich voor als de bank en proberen u te overtuigen om overboekingen te maken, in te loggen of uw gegevens, pincodes of beveiligingscodes te geven. Soms wordt zelfs gevraagd om direct toegang te geven tot uw computer. Banken vragen nooit via de telefoon of sms om uw gegevens, pin- of beveiligingscode of om overboekingen te doen. Ook vragen banken u niet om directe toegang tot uw computer te krijgen.

Nepagent babbeltruc

Criminelen doen zich ook regelmatig voor als nepagenten. Ze bellen slachtoffers en zeggen dat ze van de politie zijn. Vervolgens vertellen ze dat er een risico is dat er bij het slachtoffer wordt ingebroken. Ze geven daarbij aan dat een agent langs kan komen om waardevolle spullen op te halen, zodat ze deze veilig kunnen opbergen in een kluis op het politiebureau. Korte tijd later staat deze nepagent aan de deur. Soms in burgerkleding, soms in een uniform of iets dat daar sterk op lijkt. De politie zal u nooit bellen om te vragen naar uw waardevolle spullen en komt deze nooit bij u thuis ophalen.

6.



Waar kunt u zelf op letten?

Doe niet zomaar de deur open voor een onbekende. Of gebruik bijvoorbeeld een kierstandhouder om de deur op een kier te kunnen zetten.

Laat nooit een onbekende binnen en sluit de deur als u binnen iets gaat halen.

Pin nooit zomaar aan de deur als u niet zelf iets heeft besteld waarvan u weet dat u het moet afrekenen.

Geef uw pinpas nooit uit handen. Ook niet als iemand u op die manier aanbiedt om te helpen bij het pinnen. Pin ook niet wanneer iemand anders de betaalautomaat wil vasthouden. Op die manier kan iemand mogelijk meekijken met uw pincode.

Vertrouwt u het niet helemaal? Bel de betreffende organisatie op om het zelf te controleren. Zoek zelf het telefoonnummer op. Ook kunt u vragen of de persoon aan de deur zich kan legitimeren.

TIP Stel een dagopnamelimiet in. Deze staat automatisch op ongeveer 1000 euro. Stel dit limiet bij naar bijvoorbeeld 200 euro. Zo is de schade minder groot als ze uw pinpas en pincode stelen.

TIP Een agent kan zich altijd identificeren met een legitimatiebewijs van de politie. Hierop staan onder andere een foto en een dienstnummer.

Bent u toch slachtoffer geworden?

Meld het direct bij uw bank en laat uw pas blokkeren.

Doe altijd aangifte bij de politie. Dit kan via [politie.nl/aangifte](https://www.politie.nl/aangifte) of bel **0900 - 8844** om een afspraak te maken.

Is de oplichter nog in de buurt? Bel direct **112**.

U kunt de fraude melden bij Fraudehulpdesk via [fraudehulpdesk.nl/fraude-melden](https://www.fraudehulpdesk.nl/fraude-melden) of via telefoonnummer **088 - 7867 372**.

TIP Zo hoort een politielegitimatiebewijs eruit te zien.



Meer informatie en tips?

Slachtofferhulp Nederland biedt gratis emotionele ondersteuning of praktische hulp. Kijk voor meer informatie op [slachtofferhulp.nl](https://www.slachtofferhulp.nl) of bel **0900 - 0101**.

7.



Bankhelpdesk- fraude

Helpdeskfraude is een vorm van oplichting waarbij oplichters zich voordoen als bankmedewerker van uw bank. De crimineel misbruikt hierbij de naam of het telefoonnummer van de bank.

De oplichter probeert uw vertrouwen te winnen zodat u een betaling doet. Om uw vertrouwen te winnen maakt de oplichter gebruik van 'social-engineering'. Dat houdt in dat deze criminelen (social engineers) misbruik maken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen en angst. Criminelen proberen daarmee vertrouwelijke informatie van iemand te krijgen.

Een bekend voorbeeld van bankhelpdeskfraude is dat oplichters u proberen te overtuigen om geld over te boeken. Ze bellen u dan op met de boodschap dat ze iets onveiligs of vreemds zien gebeuren op uw rekening en dat u tijdelijk uw geld moet overboeken naar een 'veilige kluisrekening'.

Een ander voorbeeld is dat u gebeld wordt met de mededeling dat uw betaalpas niet meer veilig is en dat iemand van de bank of koeriersdienst deze op komt halen. Vaak staat er dan al verdacht snel iemand bij u op de stoep om uw pas op te halen. Maar een combinatie van beide voorbeelden is ook mogelijk!



Waar kunt u zelf op letten?

Een bank vraagt nooit aan de telefoon of in een tekstbericht om geld over te boeken naar andere rekeningen, ook niet in noodgevallen.

Een bank stuurt nooit een medewerker thuis langs om een bankpas, inlogapparaat voor internetbankieren of pincodes af te halen.

Een bank vraagt nooit om een bankpas of inlogapparaat voor internetbankieren per post op te sturen.

Een bank vraagt nooit aan de telefoon of in een tekstbericht om uw pincodes, wachtwoorden of andere beveiligingscodes af te geven.

Een bank vraagt nooit om toegang tot uw computer of telefoon. Ook vraagt een bank nooit om software of apps op de computer, tablet of telefoon te installeren.

Twijfelt u, bel dan uw bank en zoek daar zelf het telefoonnummer voor op.

Verbreek de verbinding als u het niet vertrouwt.

TIP De ING heeft op het inlogscherf van de app staan: 'Belt ING? Check het gesprek'. U kunt daarop klikken en het telefoonnummer invullen van de beller. Hiermee controleert u of u daadwerkelijk door de ING wordt gebeld of door een oplichter.



Bent u toch slachtoffer geworden?

Meld het onmiddellijk bij uw bank.

Doe altijd aangifte bij de politie. Dit kan via [politie.nl/aangifte](https://www.politie.nl/aangifte) of bel **0900 - 8844** om een afspraak te maken.

Veel mensen schamen zich nadat zij slachtoffer zijn geworden van oplichting, dat hoeft absoluut niet. Criminelen gaan heel geraffineerd te werk. Ze maken misbruik van het vertrouwen dat u heeft in een familielid of bekende. Iedereen kan slachtoffer worden.

U kunt de fraude melden bij Fraudehelpdesk via [fraudehelpdesk.nl/fraude-melden](https://www.fraudehelpdesk.nl/fraude-melden) of via telefoonnummer **088 - 7867 372**.

TIP Sla het nood- of fraudenummer van uw bank op. Mocht u deze nodig hebben, dan kunt u deze direct bellen.

Meer informatie en tips?

Kijk voor meer tips over veilig internetten op [veiliginternetten.nl](https://www.veiliginternetten.nl)
En voor meer informatie over veilig bankieren op [veiligbankieren.nl](https://www.veiligbankieren.nl)

Spoofting

Bij spoofting wordt er een trucje gebruikt om een andere identiteit aan te nemen. Spoofting betekent letterlijk 'nabootsen'. Een oplichter kan zich via veel kanalen voordoen als iemand anders. Zo bestaat er e-mailspoofting, telefoonnummerspoofting en website spoofting. Bankhelpdeskfraude is een vorm van spoofting die veel voorkomt en waarbij iemand in korte tijd veel geld kan kwijtraken.

De oplichter doet zich voor als een medewerker van de bank, een helpdesk, webwinkel of van een overheidsinstantie. De oplichter kan een medium zo aanpassen dat het sprekend lijkt op het origineel.

Het doel van spoofting is om het slachtoffer te laten geloven dat een e-mail, telefoontje, website of IP-adres van een persoon of organisatie komt die betrouwbaar is.

De belangrijkste redenen waarom criminelen aan spoofting doen zijn:

- Mensen overhalen persoonlijke informatie, zoals bankgegevens, te delen;
- Computervirussen op een apparaat installeren;
- Het computersysteem van een persoon of grote organisatie platleggen.



Waar kunt u zelf op letten?

E-mailspoofting

Controleer altijd het e-mailadres als u een e-mail niet vertrouwt. Heeft u eerder e-mails ontvangen van die afzender en komt het e-mailadres overeen? Bekijk ook of er taalfouten of gekke zinnen in de e-mail staan. Staat er een logo in de e-mail? Kijk dan of het overeenkomt met dat van de echte organisatie. Kijk ook waar de linkjes naartoe leiden, door er met de muis overheen te bewegen.

Websitespoofting

Controleer het adres van de website. Ga bijvoorbeeld in de browser naar de website die u kent, door het adres handmatig in te typen.

TIP Lees hier meer over op fraudehelpdesk.nl/fraude/is-dit-een-vals-websiteadres/

Telefoonnummerspoofting

Wordt u gebeld door een organisatie en vraagt een medewerker om persoonlijke gegevens, zoals een wachtwoord of pincode? Hang dan op, zoek het nummer van de betreffende organisatie op en bel om te vragen of zij echt contact met u hebben opgenomen. Stuur iemand u een bericht om te laten weten dat hij een nieuw telefoonnummer heeft? Neem dan eerst contact op via het oude telefoonnummer om te zien of het klopt of bel naar het nieuwe nummer om zijn of haar stem te horen.

TIP Lees hier meer over op seniorweb.nl/tip/hoe-herken-ik-een-neptelefoontje



Bent u toch slachtoffer geworden?

Doe altijd aangifte bij de politie. Dit kan via politie.nl/aangifte of bel **0900 - 8844** om een afspraak te maken.

U kunt de fraude melden bij Fraudehelpdesk via fraudehelpdesk.nl/fraude-melden of via telefoonnummer **088 - 7867 372**.

Meer informatie en tips?

Kijk voor meer tips over veilig internetten op veiliginternetten.nl
En voor meer informatie over veilig bankieren op veiligbankieren.nl



Datingfraude

Bij datingfraude wordt u opgelicht door iemand die u heeft leren kennen op een datingsite, sociale media of online game.

Bij datingfraude wordt u al snel overladen met liefde en complimenten door een oplichter. Na deze intensieve vorm van contact weten ze goed uw vertrouwen te winnen.

Toch zijn er al snel signalen dat iets niet helemaal klopt. Ze willen al snel van de datingsite af, zodat de datingsite de oplichter niet meer kan controleren. Ze praten dan graag met u verder via sms of WhatsApp. Het is vaak heel moeilijk om deze persoon via video-gesprek te spreken. Elkaar in het echt ontmoeten is onmogelijk.

De oplichter vraagt vaak na een tijd om geld. Omdat ze bijvoorbeeld te maken hebben met een noodgeval of omdat ze zeggen u te willen bezoeken. De oplichter weet hierbij goed hoe hij of zij met uw gevoelens kan spelen.

Wees daarom op uw hoede. Houd altijd de mogelijkheid open dat u te maken heeft met een fraudeur.



Waar kunt u zelf op letten?

Wees terughoudend met het delen van gevoelige informatie. Bijvoorbeeld met (seksueel getinte) foto's. Wacht bijvoorbeeld een eerste ontmoeting af om te zien met wie u écht te maken heeft.

Maak nooit geld over. Als u met een oplichter te maken heeft, vraagt deze vroeg of laat om geld. Betaal nooit, want u bent het geld kwijt. Oplichters vragen steeds opnieuw om geld.

Wees alert op taalfouten. Google Translate wordt veel gebruikt door oplichters in het buitenland. Helaas voor deze oplichters is deze functie niet foutloos en kan een bericht taalfouten hebben.

Houd familie en vrienden op de hoogte. Oplichters proberen u vaak te isoleren. Dan kunnen ze u makkelijker beïnvloeden. Voorkom dat u in zo'n positie komt en praat met familie en vrienden over uw nieuwe liefde of vriendschap.

Deel niet teveel persoonlijke informatie op sociale media. Oplichters lijken hun slachtoffers zorgvuldig uit te zoeken. Vooral mensen die hun partner hebben verloren of gescheiden zijn. Vertel dit soort informatie dus niet op sociale media. Scherm bijvoorbeeld uw Facebook-profiel af voor onbekenden.



Bent u toch slachtoffer geworden?

Meld uw oplichting bij de Fraudehulpdesk. Dit kan via fraudehulpdesk.nl/fraude-melden of via telefoonnummer **088 - 7867 372**.

Doe altijd aangifte bij de politie. Dit kan via politie.nl/aangifte of bel **0900 - 8844** om een afspraak te maken.

Blokkeer het telefoonnummer van de oplichter en de sociale media accounts.

Neem geen contact meer op.

Stop met het overmaken van geld.

Informeer de organisatie achter de datingsite, sociale media of online game.

Meer informatie en tips?

Kijk voor meer tips over veilig internetten op veiliginternetten.nl
En voor meer informatie over veilig bankieren op veiligbankieren.nl

Aan- en verkoopfraude

Bij aankoopfraude maakt u geld over naar een persoon of bedrijf, maar ontvangt u de dienst of het product niet waarvoor u heeft betaald. Bij verkoopfraude worden de goederen die u verstuurt wel geleverd, maar betaalt de ontvanger niet voor de spullen.

Criminelen maken bij aan- en verkoopfraude gebruik van verschillende soorten webwinkels. Dit kunnen handelssites zijn zoals Marktplaats en Ebay, maar ook reguliere webwinkels. Sommige valse webwinkels lijken precies op bestaande webwinkels. Dit soort webwinkels komt vaak voor op sociale mediaplatformen zoals Facebook en Instagram.

Vormen van oplichting bij aan- en verkoopfraude:

- U koopt iets via een handelssite, maar na betaling wordt het product niet geleverd. Dit gebeurt vaak bij nepwebshops die bekende namen gebruiken of advertenties op sociale media die u naar een niet-bestaande webshop sturen. Deze webshops verdwijnen vaak snel weer.
- U verkoopt iets via een handelssite, maar na verzending krijgt u geen betaling.
- U bestelt een product, maar u krijgt een heel ander product dan u had gekocht.



Waar kunt u zelf op letten?

Controleer de verkoper. U kunt de gegevens van de verkoper controleren via [politie.nl/checkdeverkoper](https://www.politie.nl/checkdeverkoper). Let op: geen melding betekent niet dat er geen risico is.

Als iets te mooi is om waar te zijn, dan is dat meestal ook zo. Laat u niet verleiden door prijzen die veel lager zijn dan die van andere aanbieders.

Lees de feedback van andere klanten op beoordelings- en vergelijkingswebsites zoals [trustpilot.nl](https://www.trustpilot.nl) en [kieskeurig.nl](https://www.kieskeurig.nl).

Controleer of er een Kamer van Koophandel (KvK) nummer op de website staat. U kunt het nummer of de bedrijfsnaam controleren via het handelsregister van de KvK op [kvk.nl/zoeken](https://www.kvk.nl/zoeken).

Controleer of er verschillende betalingsmogelijkheden zijn, zoals creditcard of achteraf betalen.

TIP Als u met een creditcard betaalt, bieden de meeste banken een aankoopverzekering. Dit betekent dat u uw geld terug kunt krijgen bij een foute aankoop.



Bent u toch slachtoffer geworden?

Doe altijd aangifte bij de politie. Dit kan via [politie.nl/aangifte](https://www.politie.nl/aangifte) of via telefoonnummer **0900 - 8844** om een afspraak te maken.

Meld uw oplichting bij de Fraudehelpdesk. Dit kan via [fraudehelpdesk.nl/fraude-melden](https://www.fraudehelpdesk.nl/fraude-melden) of via telefoonnummer **088 - 7867 372**.

Laat een review achter via [trustpilot.nl](https://www.trustpilot.nl) of via [kieskeurig.nl](https://www.kieskeurig.nl) om ook anderen te waarschuwen.

Meld de verkoper bij de handelssite (zoals Marktplaats), zodat de verkoper van het platform kan worden verwijderd.

Meer informatie en tips?

Kijk voor meer tips over veilig internetten op [veiliginternetten.nl](https://www.veiliginternetten.nl)
En voor meer informatie over veilig bankieren op [veiligbankieren.nl](https://www.veiligbankieren.nl)



Pig butchering

Pig butchering is een combinatie van dating- en beleggingsfraude. Bij deze vorm van oplichting wordt eerst een relatie opgebouwd met het slachtoffer.

Oplichters manipuleren hun slachtoffer totdat ze een vertrouwens- of zelfs een liefdesband hebben opgebouwd. Vaak vinden ze hun slachtoffers op datingapps zoals Tinder.

De oplichter verleidt het slachtoffer om te investeren in cryptomunten, zoals Bitcoin. De oplichter vertelt hoe makkelijk het is om te investeren en hoe rijk u ermee kunt worden. Vervolgens stuurt de oplichter een link naar een website die er betrouwbaar uitziet en vraagt om daar te investeren.

Als u eenmaal heeft geïnvesteerd, maakt u paar keer een kleine winst. Dit zorgt ervoor dat u steeds meer wilt investeren en de bedragen snel oplopen. Maar wanneer u genoeg heeft geïnvesteerd, verdwijnt de website en hoort u ook niets meer van uw 'potentiële toekomstige partner'.



Waar kunt u zelf op letten?

Maak geen geld over naar een cryptomunt website die niet echt is. Controleer de link met checkjelinkje.nl.

Blijf in contact met uw dierbaren. Vertrouwt u het niet? Praat eerst met een vriend of familielid erover.

Geeft iemand u overdreven veel aandacht of complimenten? Wees dan op uw hoede.

Als een aanbod te mooi lijkt om waar te zijn, is dat meestal ook zo.

Deel uw bankgegevens niet met iemand anders.

Teken nooit een (online) contract zonder goed na te denken en de voorwaarden goed door te lezen. Controleer ook altijd of het contract, het bedrijf of de cryptomunt echt is.



Bent u toch slachtoffer geworden?

Meld uw oplichting bij de Fraudehelpdesk. Dit kan via fraudehelpdesk.nl/fraude-melden of via telefoonnummer **088 - 7867 372**.

Doe altijd aangifte bij de politie. Dit kan via politie.nl/aangifte of bel **0900 - 8844** om een afspraak te maken.

Maak screenshots (schermafdrucken) van de cryptowebsite en uw contactpersoon. Dit kan later helpen als bewijs.

Blokkeer het telefoonnummer van de oplichter en de sociale media accounts.

Neem geen contact meer op.

Meer informatie en tips?

Kijk voor meer tips over veilig internetten op veiliginternetten.nl
En voor meer informatie over veilig bankieren op veiligbankieren.nl



Stem nabootsing

Cybercriminelen gebruiken kunstmatige intelligentie (AI) om mensen telefonisch op te lichten. Met zogenaamde 'voice cloning' kopiëren ze de stem van een vriend of familielid. Met de gekloonde stem vragen ze bijvoorbeeld om snel geld over te maken of ze vragen naar persoonlijke gegevens.

Deze vorm van oplichting komt nog niet veel voor in Nederland, maar is al wel te zien in landen zoals de Verenigde Staten en het Verenigd Koninkrijk.



Waar kunt u zelf op letten?

Hang op bij verdachte telefoongesprekken.
Vertrouw op uw onderbuikgevoel!

Bel de persoon terug op het nummer dat u al kent.
Gebruik niet het nummer dat u tijdens het gesprek heeft gekregen.

Gebruik videogesprekken als u twijfelt over de identiteit van de beller. De oplichter kan zich dan moeilijker verbergen achter een gekloonde stem.

Spreek een codewoord af met vrienden en familie. Dit is een soort wachtwoord waarmee u snel kunt checken of de persoon aan de telefoon daadwerkelijk is wie hij of zij zegt te zijn.



Bent u toch slachtoffer geworden?

Doe altijd aangifte bij de politie. Dit kan via [politie.nl/aangifte](https://www.politie.nl/aangifte) of via telefoonnummer **0900 - 8844** om een afspraak te maken.

U kunt de fraude melden bij Fraudehulpdesk via [fraudehulpdesk.nl/fraude-melden](https://www.fraudehulpdesk.nl/fraude-melden) of via telefoonnummer **088 - 7867 372**.

Meer informatie en tips?

Kijk voor meer tips over veilig internetten op [veiliginternetten.nl](https://www.veiliginternetten.nl)

En voor meer informatie over veilig bankieren op [veiligbankieren.nl](https://www.veiligbankieren.nl)

