



Ministerie van Justitie en Veiligheid

Tips om online fraude te herkennen en te voorkomen

En wat te doen als je slachtoffer bent geworden



Integrale aanpak

online fraude



Medegefinancierd door
de Europese Unie

Deze brochure is ontwikkeld door het Ministerie van Justitie en Veiligheid en wordt u vandaag aangeboden in het kader van een brede samenwerking tussen diverse Noord-Hollandse gemeentes, de Rabobank, Veilig Internetten, de politie, NHVeilig en SeniorWeb. Het doel hiervan is om de veiligheid van onze inwoners te vergroten en hen te behoeden voor en te ondersteunen bij verschillende vormen van online criminaliteit.



Online fraude

Het kan iedereen overkomen

Bij fraude probeert een oplichter je te bedriegen of te misleiden. Veel fraude gebeurt online. Oplichters proberen je geld, wachtwoorden of persoonlijke gegevens te krijgen. Ze bedenken steeds nieuwe manieren om mensen op te lichten. Daardoor is het lastig om nepberichten of neptelefoontjes te herkennen. Lees daarom onze tips om online fraude te herkennen. Ontdek ook wat je kunt doen als je slachtoffer bent geworden.

Zes veelvoorkomende fraudevormen.
Zo herken en voorkom je ze.



1. Aankoopfraude

Bij aankoopfraude betaal je voor een product of dienst, maar krijg je er niets voor terug.

Zo herken je aankoopfraude

- De prijs is heel laag en lijkt te mooi om waar te zijn.
- Je vindt geen of alleen maar positieve reviews.
- Je kunt geen contactgegevens van het bedrijf vinden.

Zo voorkom je aankoopfraude

- Check vergelijkingssites, reviews of de ScamCheck op veiliginternetten.nl.
- Kijk of er een keurmerk op de website staat dat je kunt aanklikken en controleer op de site van het keurmerk of de webshop daar écht is aangesloten.
- Controleer of de webshop bekend is bij de politie via politie.nl/checkdeverkoper.



2. Bankhelpdeskfraude

Bij bankhelpdeskfraude belt een oplichter je op. Hij doet alsof hij bij jouw bank werkt en zegt dat je geld in gevaar is. Hij wil je helpen door snel je geld over te maken naar een veilige rekening. Soms vraagt de oplichter je om een programma op je computer, tablet of mobiele telefoon te installeren. Zo kan hij op afstand toegang krijgen tot je apparaat. Ook kan een oplichter zeggen dat hij je betaalpas thuis komt ophalen. Tegelijkertijd probeert hij je pincode te achterhalen. Geef die nooit door.

Zo herken je bankhelpdeskfraude

- Een nep-bankmedewerker belt je op en zegt dat je geld in gevaar is en dat je snel iets moet doen.
- Een nep-bankmedewerker vraagt je om geld over te maken naar een andere rekening om zo je geld veilig te stellen.
- Een nep-bankmedewerker vertelt je wat je moet zeggen als zijn 'collega' (de echte bankmedewerker) belt en vragen stelt.
- Een nep-bankmedewerker probeert een afspraak met je te maken om je betaalpas op te halen.
- Een nep-bankmedewerker vraagt je om een programma te installeren waarmee zij op afstand je computer, tablet of mobiele telefoon kunnen bedienen.

Zo voorkom je bankhelpdeskfraude

- Krijg je zo'n telefoontje? Hang op en meld het meteen bij je échte bank.
- Een bank vraagt je nooit om geld over te maken.
- Een bankmedewerker vertelt je nooit wat je moet zeggen.
- Een bank komt nooit thuis bij je langs om een betaalpas op te halen.
- Een bank vraagt je nooit om een programma te installeren (zoals Anydesk, Teamviewer en LogMeIn) waarmee zij op afstand jouw computer, tablet of mobiele telefoon kunnen bedienen.

3. Datingfraude

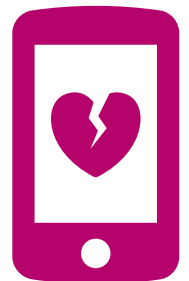
Bij datingfraude ontmoet je iemand online. Bijvoorbeeld via een datingsite, datingapp of sociale media. Deze persoon probeert je verliefd te laten worden. Daarna vraagt hij om geld vanwege een zogenaamd probleem of noodsituatie. Of hij vraagt je om geld te investeren in crypto.

Zo herken je datingfraude

- Je online liefde heeft altijd een smoes om je niet te ontmoeten. Afspraken worden steeds afgezegd.
- Je online liefde vraagt om geld. Bijvoorbeeld voor een vliegticket, een medisch noodgeval of een hotel- of ziekenhuisrekening voor een kind of ander familielid.
- Je online liefde wil geheimhouden dat jullie contact met elkaar hebben.

Zo voorkom je datingfraude

- Controleer of iemand echt bestaat. Bijvoorbeeld door onverwachts te videobellen. Je kunt ook de profielfoto checken of afspreken op een openbare plek.
- Maak nooit geld over. Investeer ook niet in crypto of andere beleggingen op advies van deze persoon.
- Praat met vrienden en familie over je nieuwe contact. Laat ook weten waar je afspreekt.
- Deel zo min mogelijk persoonlijke informatie op sociale media en scherm je account af voor onbekenden. Zo kunnen oplichters je gegevens niet gebruiken.



4. Hulpvraagfraude

Bij hulpvraagfraude of WhatsApp-fraude doen oplichters zich voor als een bekende (vriend of familielid). Ze zeggen in een appje dat ze een nieuw nummer hebben en dat je het oude nummer kunt verwijderen. Daarna vragen ze om geld vanwege een probleem dat snel opgelost moet worden.

Oplichters gebruiken soms voice cloning bij hulpvraagfraude: met behulp van AI (Artificial Intelligence of kunstmatige intelligentie) kopiëren ze de stem van een bekende (vriend of familielid). Zo lijkt het alsof je echt die bekende aan de telefoon hebt. Nu AI steeds vaker gebruikt wordt, kan voice cloning meer voorkomen. Let hier dus goed op.

Zo herken je hulpvraagfraude

- Een 'bekende' stuurt je een sms of appje vanaf een onbekend nummer. Vaak is het een bericht met de smoes dat hij een nieuw nummer heeft.
- Een 'bekende' vraagt je om geld over te maken voor een noodgeval. Vaak moet de betaling overgemaakt worden naar een vriend, omdat de bank app op de nieuwe telefoon (nog) niet werkt.
- Er is vaak haast bij.

Zo voorkom je hulpvraagfraude

- Maak nooit geld over op basis van een bericht. Bel de bekende op het nummer dat jij kent.
- Maak afspraken met bekenden (vrienden of familieleden) over wat jullie doen bij noodgevallen. Spreek bijvoorbeeld met elkaar een codewoord af.
- Deel zo min mogelijk persoonlijke informatie op sociale media en scherm je account af voor onbekenden. Zo kunnen oplichters je gegevens niet gebruiken.

5. Investeringsfraude

Investeringsfraude wordt ook wel beleggingsfraude genoemd. Oplichters proberen je via een aanbod of advertentie over te halen om geld te investeren in beleggingen of crypto. Ze beloven hoge winsten en weinig risico. Dat lijkt aantrekkelijk, maar uiteindelijk raak je je geld kwijt.

Zo herken je investeringsfraude

- Je krijgt een aanbod om snel veel geld te verdienen. Dit kan via de telefoon, e-mail of sociale media.
- Je ziet een advertentie met een mooi verhaal. Bijvoorbeeld van een bekende Nederlander of iemand die zegt snel rijk te zijn geworden met beleggen.
- Je moet snel beslissen en direct geld overmaken.
- Je kunt de winst of inleg niet opnemen. De oplichters beloven dat je je geld terugkrijgt als je extra betaalt, maar dat gebeurt niet.

Zo voorkom je investeringsfraude

- Vertrouw geen aanbiedingen waarbij je veel winst kunt maken.
- Controleer altijd wie de aanbieder is. Lees reviews op onafhankelijke websites en check de aanbieder via de ScamCheck op veiliginternetten.nl.
- Controleer in het register van de AFM (Autoriteit Financiële Markten) of de aanbieder een vergunning heeft.
- Controleer of er een waarschuwing is via checkjeaanbieder.nl.
- Investeer nooit onder druk. Moet je snel beslissen? Dan is de kans op fraude groot.



6. Phishing

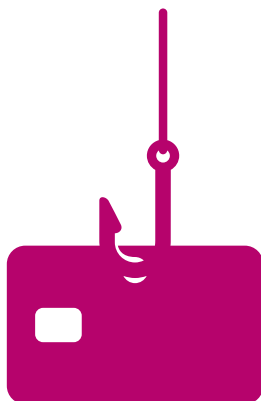
Bij phishing sturen oplichters een nepbericht dat echt lijkt. Bijvoorbeeld van de bank, de overheid of een webwinkel. Deze berichten zijn zo goed nagemaakt dat ze moeilijk te herkennen zijn. In het bericht vragen oplichters je om via een link je gegevens te controleren of bij te werken op een nepwebsite. Vul je daar je persoonlijke gegevens in? Dan krijgen oplichters toegang tot jouw informatie.

Zo herken je phishing

- Je moet snel op een link klikken volgens het nepbericht.
- Het e-mailadres van de afzender klopt **nét** niet. Er is bijvoorbeeld 1 cijfer of letter anders.
- Je moet je gegevens controleren, bijwerken of een kopie van je identiteitsbewijs of betaalpas delen op hun nepwebsite.

Zo voorkom je phishing

- Klik nooit zomaar op een link die je niet kent. Controleer de link eerst op checkjelinkje.nl: kopieer de link zonder te klikken.
- Deel nooit je identiteitsbewijs of betaalpas met onbekende personen of op onbeveiligde websites.
- Twijfel je? Zoek zelf het telefoonnummer van de organisatie op hun echte website. Bel nooit het telefoonnummer uit het nepbericht.



Met deze veiligheidsregels bankier jij veilig online

- 1 Houd je beveiligingscodes geheim.
- 2 Laat niemand je betaalpas of creditcard gebruiken.
- 3 Zorg ervoor dat je mobiele telefoon, tablet of computer goed is beveiligd.
- 4 Controleer regelmatig je bankrekening.
- 5 Meld verdachte situaties meteen bij je bank en volg de aanwijzingen van je bank op.



Slachtoffer van online fraude

Wat moet ik doen?

- **Meld fraude meteen bij je bank**

Ben je gebeld door iemand die zegt dat je geld moet overmaken, omdat je rekening in gevaar is? Of heb je een nepbericht of e-mail met een betaallink ontvangen? Meld dit dan meteen bij je bank.

Hoe? Ga naar de website van je bank en zoek op 'fraude melden'. Daar lees je hoe je fraude kunt melden. Dat kan bijvoorbeeld via de telefoon, de bank app, e-mail of de website. Bewaar de contactgegevens van je bank op een handige plek, zoals in je telefoon of portemonnee.

- **Doe aangifte bij de politie**

Ben je opgelicht, doe dan (online) aangifte bij de politie. Meld het ook als je géén schade hebt. Door aangifte te doen help je oplichters te stoppen. Samen voorkomen we dat meer mensen slachtoffer worden.

Hoe? Tel: 0900-8844 (lokaal tarief). Website: www.politie.nl

- **Ga voor hulp en advies naar Slachtofferhulp Nederland**

Je hoeft het niet alleen te doen. Veel mensen voelen zich boos, onzeker of schamen zich na oplichting. Dat is normaal. Maar het is niet jouw schuld. Slachtofferhulp Nederland kan helpen bij praktische zaken, emotionele en juridische ondersteuning.

Hoe? Tel: 0900-0101. Van maandag t/m vrijdag: 8.00 tot 20.00 uur en zaterdag: 10.00 tot 17.00 uur. Website: www.slachtofferhulp.nl

- **Meld fraude bij de Fraudehelpdesk**

Heb je te maken met fraude? Twijfel je over een bericht, ben je slachtoffer geworden of heb je een andere vraag? Bij de Fraudehelpdesk krijg je gratis advies over alles wat met fraude te maken heeft. Ze helpen je met het herkennen van fraude en wat je moet doen. Ook kijken ze hoe je de schade beperkt. Kijk op de website van de Fraudehelpdesk voor voorbeelden van valse e-mails én de laatste waarschuwingen voor werkwijzen van fraudeurs.

Hoe? Tel: 088 - 786 7372. Telefonisch bereikbaar op maandag, dinsdag, donderdag en vrijdag van 09:00-12:00 en van 13:00-15:30 uur. Op woensdag bereikbaar van 13:00-15:30 uur. Kijk voor actuele tijden op de website. Via de website kan 24/7 melding gedaan worden. Website: www.fraudehelpdesk.nl

- **Meld identiteitsfraude bij het Centraal Meldpunt Identiteitsfraude**

Denk je dat iemand jouw gegevens gebruikt? Meld dit bij het Centraal Meldpunt Identiteitsfraude (CMI) van de Rijksoverheid. Zij helpen je de schade te beperken en geven advies op maat. Ook het delen van een kopie van je identiteitsbewijs kan zorgen voor fraude. Deel een kopie van je identiteitsbewijs daarom altijd via de KopieID-app. Meer informatie en tips om identiteitsfraude te herkennen en te voorkomen vind je op de website van het CMI.

Hoe? Tel: 088-900 1000. Van maandag t/m vrijdag tussen 9:00 tot 16:30 uur. Meld identiteitsfraude 24/7 via het formulier op de website. Website: www.rvig.nl/cmi

Online fraude is een groeiend maatschappelijk probleem. Het veroorzaakt veel financiële, emotionele en psychische schade bij burgers en bedrijven. Een groot aantal organisaties* werkt samen om zo sneller, flexibeler en effectiever op te kunnen treden in de aanpak van online fraude. Zes van deze organisaties: de politie, de Nederlandse Vereniging van Banken, de Fraudehulpdesk, Slachtofferhulp Nederland, ministerie van Justitie en Veiligheid en het Centraal Meldpunt Identiteitsfraude, stelden deze brochure samen.

Belangrijke websites over online fraude

Ga voor meer tips en informatie over online fraude naar de volgende websites:

www.fraudehulpdesk.nl

www.slachtofferhulp.nl

www.veiligbankieren.nl

www.veiliginternetten.nl

www.voorkomfraude.nl

Integrale aanpak

online fraude

Samen sterk tegen online fraude



Ministerie van Justitie en Veiligheid



Rijksdienst voor Identiteitsgegevens
Ministerie van Binnenlandse Zaken
en Koninkrijksrelaties

*De samenwerkingspartners in de aanpak van online fraude zijn: de politie, het Openbaar Ministerie, VNO-NCW/MKB Nederland, de Consumentenbond, de Nederlandse Vereniging van Banken (NVB), COIN, Thuiswinkel.org, de Vereniging Nederlandse Gemeenten (VNG), De Nederlandsche Bank, de Fraudehulpdesk, het ministerie van Economische Zaken, het ministerie van Financiën en het ministerie van Justitie en Veiligheid.

Verder stellen de volgende organisaties expertise ter beschikking: het Centrum voor Criminaliteitspreventie (CVV), het Landelijk Meldpunt Internet Oplichting (LMIO), Electronic Crimes Taskforce (ECTF), het Centraal Meldpunt Identiteitsfraude, Autoriteit Consument en Markt (ACM), Slachtofferhulp Nederland, Marktplaats, ECP, SeniorWeb, Algemeen Nederlandse Bond voor Ouderen (ANBO), SIDN, Veiligheidsalliantie Rotterdam en verschillende wetenschappers.