



Handwijzer bij online beleggingsfraude

Herken de val. En wat je doet als het toch is gebeurd.

Deze handwijzer is voor jou als je bent opgelicht via een nep-belegging: een advertentie, een WhatsApp-groep, een app of een "begeleider" die je hielp beleggen. Hij is ook voor wie twijfelt of het nu gebeurt. Lees eerst wat je vandaag doet. De rest kan morgen.

Ik schreef hem omdat ik het zelf heb meegemaakt. In zes maanden verloor ik mijn spaargeld aan oplichters die mij via een advertentie op Facebook vonden. Wat ik toen had willen weten, staat hier.

Jan-Willem van Rijnberk

auteur van In Zes Maanden naar Nul

NET OPGELICHT?

Direct fraude melden →

fraudehelpdesk.nl/fraude-melden
of bel 088-786 73 72

Eerst bellen

Je bank	nummer op je pas
Politie	0900-8844
Slachtofferhulp	0900-0101

EERST DIT Het is niet jouw schuld

Je bent niet dom en je bent niet de enige.

1 op de 10

Nederlanders van 15+ werd in 2025 slachtoffer van online oplichting en fraude: anderhalf miljoen mensen (CBS)

€ 750 mln

schade door beleggingsfraude per jaar (schatting AFM).
Ongeveer een tiende daarvan komt bij de politie terecht.

Oplichters werken met stress en tijdsdruk. Dan valt het heldere denken letterlijk weg, legt hoogleraar neuropsychologie Erik Scherder uit. Dat overkomt verstandige, ervaren mensen. Vertrouwen is geen zwakte. Het is precies waar zij op mikken.

Schaam je niet. Praat erover. En lees verder.

1

Stop met betalen

Maak niets meer over, ook niet om "je winst vrij te maken", "belasting te betalen" of "verlies terug te winnen". Elke nieuwe betaling is weg.

2

Bel je bank

Vraag of een betaling nog te stoppen of terug te halen is. Bel ook als je denkt dat het te laat is. Gebruik het nummer op je bankpas, niet een nummer uit een bericht.

3

Leg alles vast

Maak schermafbeeldingen van de advertentie (met de naam van de adverteerder), de chats, de app, de website en je saldo. Exporteer WhatsApp-gesprekken. Noteer telefoonnummers, walletadressen (het adres van een cryptoportemonnee), rekeningnummers, datums en bedragen. Doe het nu: advertenties en sites verdwijnen snel.

Bewaar alles overzichtelijk in één aparte map op je computer.

4

Sluit de deur

Verwijder apps die anderen toegang tot je computer of telefoon gaven (zoals AnyDesk of TeamViewer). Wijzig je wachtwoorden en zet tweestapsverificatie aan. Blokkeer de oplichters, maar pas nadat je alles hebt vastgelegd.

Phishing of beleggingsfraude?

Heeft iemand anders met jouw gegevens geld van je rekening gehaald (phishing)? Dan moet je bank je volgens het Europees Hof van Justitie in principe uiterlijk de volgende werkdag terugbetalen, ook als ze vindt dat je onvoorzichtig was (uitspraak van 15 oktober 2026, zaak C-70/25). Banken leggen dit nog verschillend uit: vraag er schriftelijk naar.

Heb je zelf geld overgemaakt, zoals bij beleggingsfraude meestal het geval is? Dan geldt deze regel meestal niet. Bel je bank toch: zij hebben vaak nog extra tips of advies.

5

Doe aangifte bij de politie

Bereid je voor met een lijst van alle betalingen: datum, bedrag, rekeningnummer of walletadres. Neem je schermafbeeldingen mee. Aangifte is niet zinloos: elk dossier telt mee voor de opsporing, en je bank of verzekering vraagt er vaak om.

Heb je identiteitsgegevens gedeeld, zoals een kopie van je paspoort, ID-kaart of rijbewijs, of je telefoonnummer? Meld dat uitdrukkelijk in je aangifte.

6

Meld het bij de AFM en de Fraudehelpdesk

De AFM verzamelt meldingen over beleggingsfraude via haar [contactformulier voor consumenten](#). De [Fraudehelpdesk](#) geeft advies en waarschuwt anderen.

7

Meld de oplichter bij het platform

De DSA (Digital Services Act) is de Europese wet die grote online platforms verplicht om illegale inhoud, zoals oplichting, aan te pakken. Facebook, Instagram en andere platforms moeten jouw melding daarom beoordelen. Zo pak je het aan:

- Meld de advertentie, het profiel of de groep via de knop "Rapporteren" en kies "Oplichting of fraude".
- Wordt je melding afgewezen? Maak bezwaar via je meldingenoverzicht (bij Facebook: het Postvak In voor ondersteuning).
- Blijft het account online? Meld het dan bij de [ACM](#), de Nederlandse toezichthouder voor de DSA.

Let op: de ACM lost je eigen probleem niet op. Ze gebruikt je melding om te controleren of platforms de wet overtreden, en kan hun daarvoor een boete opleggen.

8

Meld de app

Kwam je via een app uit de App Store of Google Play? Meld hem daar als oplichting. Een plek in de App Store zegt niets over de betrouwbaarheid van de app. Maak ook hier schermafbeeldingen: hoe de app in de App Store werd aangeboden en hoe hij op je telefoon stond (icoon, openingsscherm).

9

Meld de website

Gebruikte de oplichter een eigen website? Dan werkt het net zo: leg de website vast in schermafbeeldingen, met het webadres in beeld. Noteer de gegevens van iedereen die contact met je had, ook als je denkt dat het om nepnamen gaat.

Wat de wet wel en niet doet

Het platform moet de oplichter aanpakken, maar het hoeft je schade niet te vergoeden. Je geld terughalen loopt via je bank, de politie en soms een advocaat. Verwacht niet te veel, maar meld wel: zo maak je het oplichters moeilijker en help je de volgende.

LET OP De tweede klap: herstellfraude

Na je verlies, soms al binnen een paar dagen, kun je worden benaderd door iemand die belooft je geld terug te halen. Een "herstelbureau", een "advocaat", een "opsporingsdienst" of zelfs de "AFM". Oplichters misbruiken daarvoor de namen en logo's van echte organisaties, ook van bestaande bureaus die slachtoffers helpen.

- **Betaal nooit vooraf** om je geld terug te krijgen. Geen kosten, geen "vrijgavebelasting", geen borg.
- **Neem zelf contact op** met een organisatie, via gegevens die je zelf hebt opgezocht. Nooit via het nummer of de link in het bericht dat je kreeg.
- **Echte instanties** zoals de politie, de AFM en je bank vragen nooit om geld om een zaak op te lossen.
- **Identiteitsfraude.** Heb je persoonlijke gegevens met de oplichters gedeeld? Houd er dan rekening mee dat ze die opnieuw gebruiken. Ze verkopen je dossier door, of benaderen je later opnieuw onder een andere naam.

JIJ Zorg ook voor jezelf

Oplichting raakt meer dan je bankrekening. Schaamte, boosheid, rouw en wantrouwen zijn normale reacties. Ze gaan niet vanzelf over door te zwijgen.

Praat erover

met je partner, je kinderen of een goede vriend.
Zwijgen beschermt de oplichters, niet jou.

Blijf onder de mensen

ook als je er niet over wilt praten. Contact met anderen helpt.

Zoek lotgenoten of een professional

Slachtofferhulp Nederland biedt gratis steun:
0900-0101.

Richt je op wat je wel kunt doen

melden, vastleggen, je beveiliging op orde brengen.

Zit je erg in de put of denk je aan de dood? Praat erover met 113 Zelfmoordpreventie: bel **113** of gratis **0800-0113**, of chat via 113.nl.

VOORKOMEN Herken de val: tien signalen

Niemand is immuun. Maar wie de signalen kent, ziet de val eerder. Deel deze lijst met wie je lief is.

#	Je ziet of hoort	Wat je doet
1	Een advertentie of video met een bekende Nederlander, of een "expert" die je steeds vaker tegenkomt	Bekende mensen worden vaak nageemaakt. Zoek de persoon zelf op. Niets te vinden? Niet volgen.
2	Je wordt toegevoegd aan een "exclusieve" WhatsApp- of Telegramgroep met beleggingstips	Echte partijen doen dat nooit ongevraagd. Een volle groep bewijst niets: deelnemers zijn makkelijk na te maken.
3	Een vriendelijke "assistent" vraagt naar je situatie, je spaargeld en je doelen	Dit is profilering, geen vriendschap. Deel nooit je financiële gegevens.
4	De eerste kleine beleggingen leveren echt winst op	Kleine winsten zijn lokaas. Ze kosten de oplichter niets. Leg nooit meer in dan je kunt missen.
5	Je moet overstappen naar hun eigen app of platform, "gewoon uit de App Store"	Een App Store-plaatsing is geen keurmerk. Controleer of de partij een vergunning heeft in het AFM-register.
6	Je mag handelen met "leverage": 25, 100 of 200 keer je inleg	Bij 200 keer ben je alles kwijt bij een daling van een half procent. Doe het niet.
7	Je saldo in de app groeit snel	Een saldo in een nep-app bestaat niet. Probeer een klein bedrag op te nemen. Lukt dat niet, of moet je eerst betalen? Stop direct.
8	"Deze kans sluit vanavond." "Je moet nu beslissen."	Tijdsdruk zet je verstand uit. Neem altijd minstens 48 uur bedenktijd.
9	"Jij bent geselecteerd." "Alleen voor onze VIP-leden."	Hoe exclusiever het klinkt, hoe kritischer je moet zijn. Echte aanbieders zijn openbaar en geregistreerd.
10	Alles klopt: de site, de app, de mensen, de winst	Juist dan stel je drie vragen: kan ik vandaag geld opnemen? Staat deze partij in het AFM-register? Heb ik dit met iemand buiten de groep besproken? Eén keer nee: stop.

Neem belangrijke beslissingen met financiële gevolgen nooit in je eentje. Bespreek ze vooraf met je naaste, je familie of een goede vriend.

Let op: ook online romantiek leidt vaak tot oplichting.

HULP EN MELDEN

Organisatie	Waarvoor	Waar
Politie	Aangifte van oplichting	politie.nl/aangifte · 0900-8844
Fraudehulpdesk	Advies en melden van fraude	fraudehulpdesk.nl · 088-786 73 72
AFM	Melden van beleggingsfraude	afm.nl > contactformulier consumenten
Slachtofferhulp Nederland	Gratis steun na oplichting	slachtofferhulp.nl · 0900-0101
113 Zelfmoordpreventie	Als je het niet meer ziet zitten	113.nl · 113 of 0800-0113

HET PLATFORM AANSPREKEN

Organisatie	Waarvoor	Waar
ACM	Melden als een platform je melding negeert (DSA)	acm.nl > melden bij de ACM
Consumentenbond	Advies en collectieve acties	consumentenbond.nl
IC3 (FBI)	Melden als een Amerikaanse instantie de site van je oplichters in beslag nam	ic3.gov

CONTROLLEREN VOORDAT JE IETS DOET

Hulpmiddel	Waarvoor	Waar
AFM-register	Heeft deze partij een vergunning in Nederland?	afm.nl/register
FINRA BrokerCheck	Is deze broker of adviseur in de VS geregistreerd?	brokercheck.finra.org
ScamCheck	Is deze website of link betrouwbaar?	veiliginternetten.nl/scamcheck
ScamAdviser	Idem, internationaal	scamadviser.com

MEER WETEN

Bron	Wat het is	Waar
Digitale Weerbaarheid	Gratis online cursus over veilig online leven	digitale-weerbaarheid.nl
Operation Shamrock	Informatie en video's over pig butchering en scamcompounds	operationshamrock.org
"Hello, is this Anna?"	Onderzoek naar pig butchering, met 26 slachtoffers (Oak en Shafiq, 2025)	arxiv.org/abs/2503.20821
Het Digitale Slachthuis	Achtergrond, nieuws en de boeken van Jan-Willem van Rijnberk	digitaleslachthuis.nl

Pig butchering: oplichters bouwen eerst langzaam vertrouwen op, "mesten het varken vet", en halen je daarna in één keer leeg.

Voor het kwartje valt, *wist het algoritme het al.*

Een waargebeurd verhaal over digitale fraude.



- ✓ **Zie hoe je feed jou vindt** voordat je zelf weet wat je zoekt.
- ✓ **Begrijp hoe vertrouwen groeit** en stap voor stap wordt misbruikt.
- ✓ **Doorzie het jargon** leverage en stop-loss, helder uitgelegd.
- ✓ **Weet waar je terechtkunt** als het jou of een naaste overkomt.

Met voorwoord van Ellie Lust

Nu verkrijgbaar · digitaleslachthuis.nl

HET VERHAAL ACHTER DEZE HANDWIJZER

In Zes Maanden naar Nul

In zes maanden verloor Jan-Willem van Rijnberk zijn spaargeld aan een nep-belegging die begon met één advertentie op Facebook. In dit boek vertelt hij hoe het gebeurde, stap voor stap. Zo herken jij de val eerder.

132 pagina's · € 19,95 · ISBN 978-94-6561-153-2

Lees meer op
digitaleslachthuis.nl →

Deel deze handwijzer vrij. **Elke lezer die de val eerder ziet, telt.**

Deze handwijzer is een uitgave van TRILOGIE, Eindhoven. Tekst: Jan-Willem van Rijnberk. Meer in *In Zes Maanden naar Nul* (2026) en op digitaleslachthuis.nl. Versie oktober 2026.

Cijfers: CBS, Veiligheidsmonitor 2025; AFM, *Van piramide tot ijsberg* (december 2025). Uitspraak: Hof van Justitie van de EU, 15 oktober 2026, zaak C-70/25 (ECLI:EU:C:2026:852).

Dit is geen juridisch of financieel advies. Het is een wegwijzer op basis van eigen ervaring en openbare bronnen. Twijfel je over je situatie? Vraag advies aan je bank, de Fraudehelpdesk of een advocaat.