

Het oplichtings ABC

Verschillende manieren van oplichting uitgelegd in makkelijke taal.

Door: ABN AMRO, 2025



ABN·AMRO

Introductie

Oplichters proberen op allerlei manieren aan geld te komen.
Sommige manieren bestaan al heel lang. Andere manieren zijn nieuw.
Soms worden slachtoffers persoonlijk benaderd.
Maar vaak gaat het via de telefoon, via e-mail, via sms of via een app.

Het is belangrijk dat je weet hoe oplichters werken.
Dan heb je het misschien door als iemand jou oplicht.
De trucs van oplichters hebben vaak moeilijke namen.
De uitleg is soms ook lastig te begrijpen.
Daarom hebben we nu een lijst gemaakt in makkelijke taal.
In deze lijst staan veel verschillende soorten oplichting.

De namen van deze soorten oplichting zijn vaak nog steeds moeilijk.
Maar die namen hoef je niet te onthouden.
Het belangrijkste is dat je de trucs van de oplichters herkent.
Dan is de kans kleiner dat je slachtoffer wordt.

Is er iets gebeurd wat raar voelt?

Denk je dat je bent opgelicht?

Heb je iets vreemds meegemaakt?

Neem snel contact op met je bank.

Je kunt ons bellen met de ABN AMRO app of met je telefoon.

Bel je via de app? Dan spreek je meteen met de juiste afdeling. Dat is veilig en gaat snel.

Wil je liever bellen met de telefoon? Dat kan ook.

Bel naar 0900 - 00 24.

Bel je vanuit het buitenland? Dan kun je bellen naar +31 10 241 17 20.

Al deze gesprekken kosten evenveel als een normaal telefoongesprek.

Als je bent opgelicht, kun je dat ook melden op de website abnamro.nl/fraudemelden.

Lijst met trucs van oplichters

A

Uitleg wat **aankoopfraude** is:

Je ziet online een mooie aanbieding.

Bijvoorbeeld in een webshop of via sociale media zoals Facebook of Instagram.

De prijs is goed en je besluit om te betalen.

Maar je aankoop komt nooit aan en de website is ineens verdwenen.

De verkoper was een oplichter.

Je bent je geld kwijt.

Dit noemen we aankoopfraude.

Je denkt iets te kopen bij een echte winkel, maar het is een oplichter.

Soms is de webshop nep of bestaat het helemaal niet.

B

Uitleg wat **bankhelpdeskfraude** is:

Iemand belt je.

Deze persoon zegt dat hij of zij een medewerker van jouw bank is.

Hij of zij zegt bijvoorbeeld dat er iets mis is met je rekening.

Je krijgt het advies om je geld over te maken naar een andere rekening, die veilig is.

Je kunt ook de vraag krijgen om je pincode te geven of je computer over te laten nemen.

Dit is een truc om je geld te stelen.

De persoon die belt is geen medewerker van jouw bank, maar een oplichter.

Als je geld overmaakt, dan komt het op de rekening van deze oplichter.

Uitleg wat **boilerroomfraude** is:

Je krijgt een telefoontje of een e-mail.

Iemand zegt dat hij of zij een bijzondere kans voor jou heeft.

Je wilt dit niet missen. Je kunt er veel geld mee krijgen.

Je kunt bijvoorbeeld geld inleggen in een project.

De persoon die belt of mailt, weet vaak veel over jou.

Daardoor denk je misschien dat je de persoon kunt vertrouwen.

Eerst vraagt de persoon om een klein bedrag in te leggen.

Vaak levert dat gelijk winst op.

Daardoor leggen mensen vaak nog meer geld in.

Maar de persoon die jou belt of mailt is een oplichter.

Het geld dat je inlegt gaat rechtstreeks naar de oplichter.

Vaak bestaat er helemaal geen project.

B

Uitleg wat **betaalpasfraude** is:

Je ontvangt een e-mail, een brief of je wordt gebeld.

Je krijgt te horen dat je betaalpas niet meer werkt.

Je krijgt de vraag om je betaalpas op te sturen.

Of om de betaalpas mee te geven aan iemand die langskomt.

Het lijkt alsof het bericht van jouw bank komt. Maar dat is niet zo.

Een echte bank vraagt je nooit om je betaalpas op te sturen of mee te geven.

Als je je betaalpas opstuurt of meegeeft, komt die bij oplichters terecht.

Zij gebruiken je bankgegevens om geld van jouw rekening te halen.

C

Uitleg wat **cryptofraude** is:

Iemand vraagt je om geld in te leggen in cryptovaluta, zoals bitcoin.

Hiervoor gebruikt hij of zij filmpjes of advertenties met bekende personen.

Je krijgt te horen dat je in korte tijd veel geld kunt verdienen.

Als je geld inlegt, lijkt het alsof je meteen winst maakt. Soms krijg je die winst ook.

Daardoor gaan mensen vaak nog meer geld inleggen.

Maar alles is nep.

De persoon die contact met jou opnam, is ineens niet meer te bereiken.

Je geld is naar oplichters gegaan.

Dit is crypto-fraude. Soms noemen ze dit crypto-scam.

D

Uitleg wat **datingfraude** is:

Je leert iemand kennen via een datingsite of sociale media.
Het klikt. Jullie praten veel en bouwen een band op.
Na een tijdje vraagt de ander om geld.
Bijvoorbeeld voor een noodgeval, een ziek familielid of een vliegticket om jou op te zoeken.
Vaak vraagt de andere persoon jou meerdere keren om geld.
Uiteindelijk blijkt het niet te kloppen.
De liefde was nep. De andere persoon is een oplichter.
Je voelt je verdrietig. Die persoon loog tegen jou. Nu ben je jouw geld kwijt en je liefde.

Oplichters gebruiken nepprofielen, gestolen foto's en valse verhalen.
Je moet daarom voorzichtig zijn met mensen die je online leert kennen.
Vooral als ze snel om geld of persoonlijke gegevens vragen.

Uitleg wat **deepfake-fraude** is:

Iemand stuurt jou een video waarin jij zelf te zien bent.
Je schrikt, want het lijkt echt.
Maar het is nep. Het is gemaakt met kunstmatige intelligentie.
Een oplichter zegt dat je geld moet betalen.
Anders verspreidt hij of zij de video.
Je voelt je machteloos, bang en onder druk gezet.

Soms krijgen je vrienden of familie een video waarin het lijkt alsof jij om geld vraagt.
Ook deze video is nep.
Als jouw vrienden of familie geld overmaken, dan gaat dat direct naar de oplichter.

Dit soort nepbeelden worden gebruikt bij verschillende soorten oplichting.
Het gebeurt bijvoorbeeld bij datingfraude.
Tijdens een videocall lijkt jouw nep-liefde dan echt.
Het gebeurt ook bij CEO-fraude.
Daarbij lijkt het alsof je contact hebt met een belangrijk persoon bij een bedrijf.
Ook komt het voor bij sextortion.
Deze manier van oplichting leggen we straks uit.

F

Uitleg wat **factuurfraude** is:

Je ontvangt een factuur of een boete.

Het kan ook een rekening van de Belastingdienst zijn.

Daarin staat dat je een bedrag moet betalen.

Het lijkt echt. Maar het is nep.

Als je het geld overmaakt, gaat dat naar oplichters.

Kijk daarom eerst goed naar het document voordat je betaalt.

Soms heeft de oplichter op een echte factuur het rekeningnummer veranderd.

Je denkt dan dat je aan een echt bedrijf betaalt.

Maar ook nu gaat het geld naar de oplichter.

Kijk altijd goed naar de factuur. Heb je dit product echt besteld?

Vergelijk het rekeningnummer op de factuur met jouw eigen aankoopbevestiging.

G

Uitleg wat een **geldezel** is:

Je krijgt een bericht via bijvoorbeeld Snapchat of Telegram. Of je ziet een vacature.

De vraag is vaak simpel: 'Wil je snel geld verdienen?'

Je hoeft alleen je bankrekening of je betaalpas uit te lenen.

In ruil daarvoor krijg je geld.

Dat klinkt als een makkelijke en snelle manier om geld te verdienen.

Een oplichter zet geld op jouw rekening.

De oplichter vraagt jou een deel door te sturen naar een andere rekening.

Het andere deel mag je houden.

Maar dit is niet goed. Je helpt criminelen.

Iemand die dit doet is een geldezel. Soms heet dit een money mule.

Je kunt een boete krijgen. Of zelfs naar de gevangenis gaan.

De kans dat je wordt gepakt is erg groot.

De politie en de banken letten goed op.



Uitleg wat **identiteitsfraude** is:

Een bedrijf of een organisatie neemt contact met je op.

Je kent de naam van het bedrijf of de organisatie.

Je krijgt de vraag om bijvoorbeeld een kopie van je identiteitsbewijs online op te sturen.

Maanden later krijg je ineens rekeningen.

Je moet betalen voor dingen die je nooit hebt besteld.

Een oplichter heeft jouw naam, geboortedatum, adres of een kopie van je identiteitsbewijs gebruikt.

Met die gegevens kan de oplichter spullen kopen of zelfs een bankrekening openen.

Je moet daarom altijd voorzichtig zijn met het delen van je gegevens. Ook online.

Uitleg wat **internetoplichting** is:

Internetoplichting is bedrog via het internet.

Je ziet een website van een betrouwbaar bedrijf.

Of je krijgt een e-mail van iemand die je kent.

Maar dit blijkt nep te zijn. Het zijn oplichters.

Oplichters gebruiken slimme trucs om je te misleiden.

Je denkt bijvoorbeeld dat je iets koopt in een webshop of via Marktplaats.

Of je denkt dat je iemand helpt.

Maar in werkelijkheid heb je contact met een oplichter.

Hij of zij probeert via het internet jouw geld of persoonlijke gegevens te stelen.

M

Uitleg wat **malware** is:

Je krijgt een e-mail met een link of een bijlage.

Of je krijgt een sms of een ander soort bericht.

Als je op de link klikt of iets downloadt, wordt malware actief.

Malware is een computervirus.

Oplichters kunnen dan in jouw laptop, telefoon of tablet.

Dat gebeurt zonder dat je het merkt.

Op jouw apparaten staan vaak documenten, wachtwoorden of bankinformatie.

Daar zijn de oplichters naar op zoek.

Met die gegevens kunnen ze verschillende dingen doen.

Soms wordt er geld van je rekening gestolen.



Uitleg wat **opnieuw opgelicht** is:

Nadat je bent opgelicht, word je weer benaderd.

Iemand zegt dat hij of zij je kan helpen om je geld terug te krijgen.

Daarvoor moet je deze persoon wel geld betalen.

Nadat je dat bedrag hebt betaald, hoor je niets meer van deze persoon.

Je bent niet geholpen en je bent nog meer geld kwijt.

Je bent opnieuw opgelicht. Soms heet dit recovery fraude.

P

Uitleg wat **phishing** is:

Je krijgt een e-mail.

Hij lijkt te zijn gestuurd door jouw bank, de overheid of een bekend bedrijf.

In de e-mail staat vaak dat je snel iets moet doen, zoals inloggen of iets betalen.

Als je op de link klikt, kom je op een website.

De website is vals. Je inloggegevens worden er gestolen.

Vervolgens stelen oplichters geld van je bankrekening.



Uitleg wat **QR-code fraude** is:

Je scant een QR-code om bijvoorbeeld iets te betalen of te bestellen.
Je wordt doorgestuurd naar een website waar je je gegevens moet invullen.
Je vertrouwt het bericht of de link. Maar de website is nep.
Het geld gaat naar de oplichters.

Soms wordt er ook software op je telefoon gezet.
Met die software kunnen oplichters toegang krijgen tot jouw gegevens.
Zo kunnen ze geld van je stelen.
Dit is oplichting met QR-codes. Soms heet dit quishing.

Niet elke QR-code is gevaarlijk.
Scan je een QR-code? Kijk dan goed wat er op je scherm staat.
Betaal pas als het klopt.

S

Uitleg wat **sextortion** is:

Je krijgt foto's of een video toegestuurd.
Je bent daarin zelf te zien.
De beelden zijn vaak seksueel. Je schrikt enorm.
Meestal zijn de beelden nep.
Ze zijn gemaakt met kunstmatige intelligentie.

De afzender zegt dat hij of zij de foto's of video met je vrienden, familie of collega's gaat delen.
Als je dat niet wilt, moet je geld betalen.
Je schaamt je en voelt je machteloos en angstig. Je durft er vaak niet over te praten.
Dat jij er niet over praat, is precies wat oplichters willen.
Deze vorm van oplichting komt steeds vaker voor, vooral bij jonge mensen.
Het kan zorgen voor paniek, stress en depressie.

Uitleg wat **shouldering** is:

Je voert je pincode of de code van je telefoon in. Iemand kijkt over je schouder mee.
Dit gebeurt bijvoorbeeld bij een geldautomaat. Of bij een pinautomaat in de supermarkt.
Of bij het afrekenen op een terras.
Na het meekijken steelt de oplichter jouw telefoon of betaalpas.
Je hebt dat vaak niet in de gaten.
De oplichter kan dan makkelijker jouw geld stelen.
Dit is shouldering. Soms heet dit shoulder surfing.

Uitleg wat **sim-swapping** is:

Een oplichter belt jouw telefoonbedrijf en gebruikt jouw naam.
Hij of zij kent jouw naam, geboortedatum en adres.
De oplichter vraagt het telefoonbedrijf om jouw telefoonnummer over te zetten naar een nieuwe simkaart.
Nu ontvangt de oplichter jouw sms'jes, berichten en codes.
Hij of zij kan nu in jouw accounts en soms zelfs jouw bankrekening.

S

Uitleg wat **skimming** is:

Je rekent af bij een pinautomaat of neemt geld op bij een geldautomaat.
Maar er is een opzetstukje op de pinautomaat of de geldautomaat geplaatst.
Of er is een camera verstoppt.
De oplichter komt zo aan jouw gegevens of jouw pincode.
Hij of zij kan nu geld van je rekening halen.

Uitleg wat **smishing** is:

Je ontvangt een sms of WhatsApp-bericht met een link naar een website.
Het lijkt alsof het bericht van jouw bank of een ander bekend bedrijf komt.
Maar het komt van oplichters.
De oplichters zeggen dat je snel moet reageren.
Dat doen ze expres, want dan heb je geen tijd om goed na te denken.
Klik je op de link? Dan kom je op een nepwebsite.
Op die website moet je je gegevens invullen of geld overmaken.
Als je dat doet, ben je je geld of je gegevens kwijt.

Uitleg wat **social media fraude** is:

Je krijgt een bericht via bijvoorbeeld WhatsApp of Facebook.
Het bericht lijkt van een bekende te zijn.
Die persoon zegt dat hij of zij in de problemen zit en snel geld nodig heeft.
Het bericht komt niet van een bekende, maar van een oplichter.
Nadat je geld hebt overgemaakt, vraagt de oplichter vaak om meer geld.
Daarna hoor je niets meer van hem of haar.
De oplichter is verdwenen en jij bent je geld kwijt.
Dit is social media fraude. Het heeft ook andere namen.
Soms heet het hulpvraagfraude, WhatsApp-fraude of vriend-in-nood-fraude.

S

Uitleg wat **spoofing** is:

Je wordt gebeld door een persoon.

De persoon zegt bijvoorbeeld dat hij bij jouw bank, de overheid of de politie werkt.

Op het scherm verschijnt het echte telefoonnummer.

Daardoor denk jij dat je bijvoorbeeld echt jouw bank aan de telefoon hebt.

Je krijgt te horen dat er iets niet goed is.

Er ontbreken bijvoorbeeld gegevens of je moet iets aanpassen.

De oplichters sturen je naar een nepwebsite.

Daar moet je je gegevens invullen of geld overmaken.

Dat geld gaat naar de oplichters.

Dit is spoofing.

V

Uitleg wat **vacaturefraude** is:

Je krijgt de vraag of je een nieuwe baan wil.

Het lijkt een heel mooie baan.

Maar het is nep. De baan bestaat niet.

Oplichters doen alsof ze een werkgever zijn.

Ze vragen bijvoorbeeld om persoonlijke gegevens of een kopie van je identiteitsbewijs.

Soms laten ze je klikken op een link met malware (een computervirus).

Soms moet je iets betalen. Bijvoorbeeld voor een training of voor een werkpas.

Nadat je hebt betaald of je gegevens hebt gedeeld, hoor je niets meer.

De oplichters hebben jouw geld of jouw gegevens.