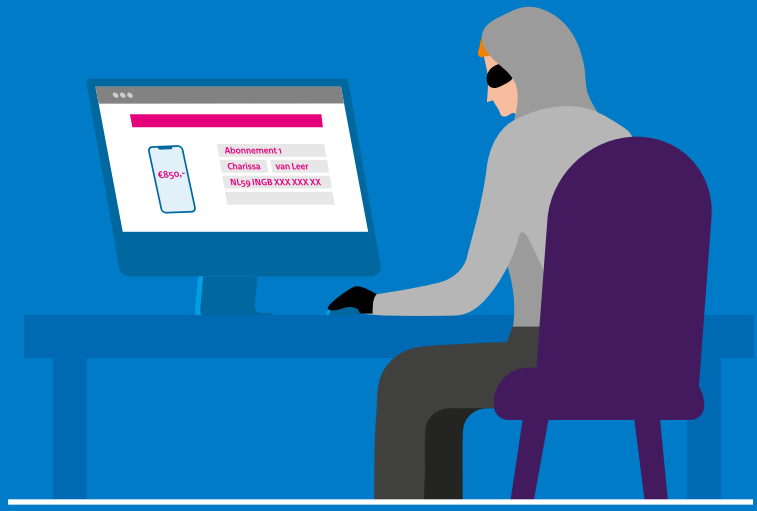
Wat is identiteitsfraude?

Online shoppen zonder te betalen. Geld lenen en van de aardbodem verdwijnen. Een telefoonabonnement afsluiten en ervandoor gaan met de nieuwste telefoon. Stel je eens voor dat een oplichter dit doet uit jouw naam. De oplichter is spoorloos en jij krijgt de rekening. Dit noemen we 'identiteitsfraude' en dit kan grote gevolgen hebben.

Hoe dat kan? Een oplichter steelt jouw identiteitsgegevens. Bijvoorbeeld via een online advertentie of met een phishingmail. Met deze gegevens bestelt een oplichter spullen op jouw naam of sluit hij een lening af.

Wat je kunt doen om identiteitsfraude te voorkomen, lees je in deze folder.

Maak het oplichters niet te makkelijk en wees alert.



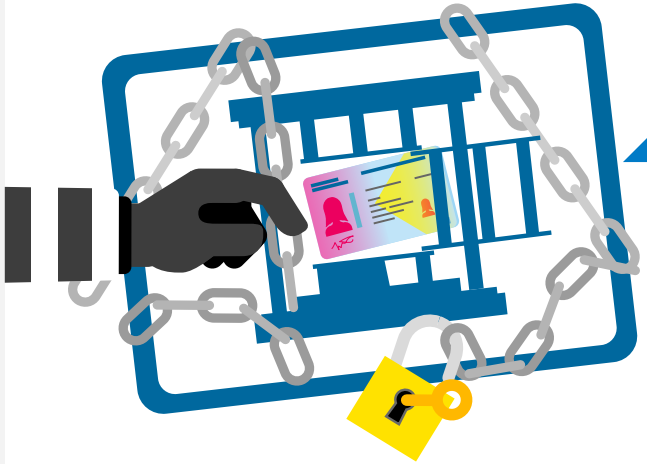
Ben je slachttoffer van identiteitsfraude? Meld het bij het **Centraal Meldpunt Identiteitsfraude (CMI)**. Het CMI geeft advies om identiteitsfraude te voorkomen en ondersteunt slachtoffers om het misbruik te stoppen en de gevolgen te herstellen.

Wat zijn identiteitsgegevens?
Identiteitsgegevens worden ook wel persoonsgegevens genoemd. Het gaat om alle informatie over jou, zoals je naam, adres, geboortedatum, pasfoto of burgerservicenummer (BSN).

Wist je dat...
het lenen en uitlenen van identiteitsdocumenten ook onder identiteitsfraude valt en strafbaar is?

Wat kunnen oplichters doen uit jouw naam?

Hoe komen oplichters aan jouw identiteitsgegevens?



Je gegevens en documenten worden gestolen uit je tas, computer of telefoon.

Lees op pagina 5. ›

Je deelt zelf gegevens en documenten via sociale media of internet.

Lees op pagina 7. ›

Je wordt misleid via een online advertentie, babbeltruc, phishingmail, WhatsApp of sms.

Lees op pagina 6. ›

Laat identiteitsgegevens en documenten niet stelen

Identiteitsdocument

Oplichters gebruiken vaak gestolen identiteitsdocumenten. Hier kunnen ze aankopen mee doen of ze steken er de grens mee over. Omdat steeds meer zaken online geregeld worden, zijn ook kopieën van identiteitsdocumenten aantrekkelijk voor oplichters. Hiermee kan iemand bijvoorbeeld een telefoonabonnement op jouw naam afsluiten.

Computer of telefoon

Hackers kunnen inbreken op jouw computer of telefoon. Op die manier kunnen ze jouw identiteitsgegevens bekijken en misbruiken. Daarnaast kunnen ze je e-mailaccount hacken en e-mails vanuit jouw naam versturen om zo anderen te misleiden.

Tip 1: **Bewaar je identiteitsdocument op een veilige plaats. Kwijt of gestolen? Meld het direct bij de gemeente.**

Tip 2: **Beveilig je digitale accounts, zoals DigiD of sociale media, door in te loggen in 2 stappen (tweestapsverificatie). Je krijgt dan een extra inlogcode per sms of via een speciale app.**

Tip 3: **Zorg voor een goede basisveiligheid:**

- **gebruik veilige wachtwoorden;**
- **installeer de laatste updates;**
- **gebruik een goede virusscanner;**
- **maak regelmatig back-ups;**
- **klik niet zomaar op links.**

Kijk voor meer tips op www.veiliginternetten.nl.

Deel je gegevens en documenten niet met andere mensen

Babbeltruc aan de telefoon

Oplichters zijn meesters in het winnen van vertrouwen. Zij bellen je op en doen zich voor als medewerker van een bank, politieagent of de overheid. In het scherm van jouw telefoon staat vaak het werkelijke telefoonnummer van die organisatie. Hierdoor komt het geloofwaardig over. Dit heet spoofing. Met een overtuigend verhaal proberen ze je te misleiden. Zodat jij de oplichter toegang tot je computer of bankrekening geeft.

Online advertenties

Oplichters adverteren met iets wat jij graag wilt hebben: concertkaartjes, woonruimte, een leuke baan. Hoe groter de verleiding, hoe minder waakzaam je bent en daar profiteren oplichters van.

Tip 1: **Vertrouw je de situatie niet? Zoek zelf het goede telefoonnummer op van de organisatie en bel ze op om te horen of het verhaal klopt.**

Tip 2: **Online kopen of verkopen? Stuur nooit kopieën van je identiteitsdocument of bankpas.**

Ze vragen je om een kopie van je identiteitsdocument en een klein bedrag over te maken. Hiermee kan bijvoorbeeld een telefoonabonnement op jouw naam geactiveerd worden.

Phishingmail

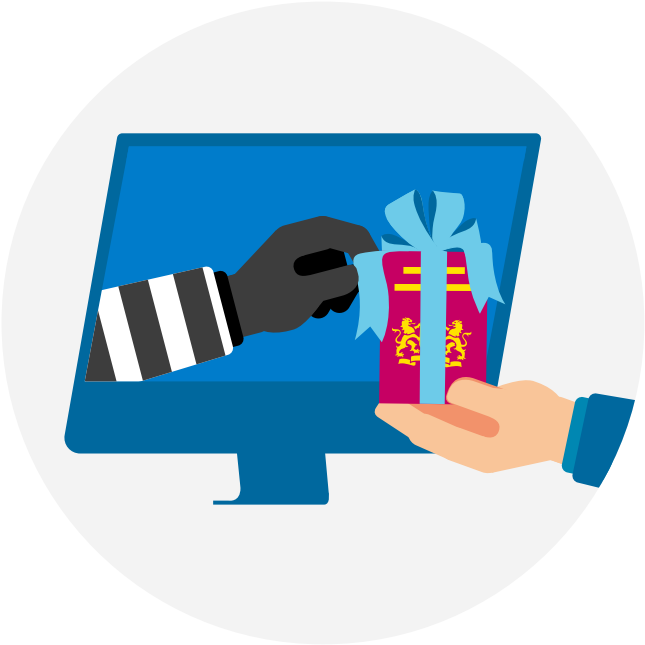
Oplichters sturen jou een ‘phishingmail’. Dit is een e-mail die lijkt op een e-mail van de overheid, een bank of een ander bekend bedrijf. Daarin vragen oplichters om je gegevens te mailen of in te loggen via een link. Zo word je naar een valse website geleid waar je jouw gegevens prijsgeeft. Hiermee komen ze bijvoorbeeld aan je DigiD inlognaam en wachtwoord.

Tip 3: **Klik in e-mails niet zomaar op een link naar een inlogpagina. Zoek zelf naar het juiste webadres. De overheid stuurt geen e-mails of sms-berichten met daarin een link naar een inlogpagina.**

Tip 4: **Verander regelmatig je wachtwoorden en deel deze gegevens niet. Houd in gedachten dat relaties kunnen veranderen, ook als je mensen vertrouwt. Bij ruzies kunnen mensen rare dingen doen, ook met jouw inloggegevens.**

Veilig je bankzaken regelen? Kijk voor tips op www.veiligbankieren.nl.

Geef je identiteitsgegevens niet ‘cadeau’



Datalekken

Veel organisaties vragen om een kopie van je identiteitsdocument. Vaak worden deze goed bewaard, maar niet altijd. Het komt voor dat oplichters door slechte beveiliging toegang hebben tot kopieën van identiteitsdocumenten of andere persoonsgegevens. Dan is er sprake van een datalek. Maak kopieën daarom onbruikbaar voor oplichters: schrijf de naam van de ontvanger, het doel en de datum op de kopie en streep de gegevens door die de ontvanger niet nodig heeft. Dit kan bijvoorbeeld met de KopieID-app.

Ook is het verstandig om terughoudend te zijn met het delen van gegevens aan personen en bedrijven. Is het niet verplicht om gegevens, zoals geboortedatum of bankrekeningnummer, te geven? Doe het dan niet.

Tip 1: **Verwijder bestanden en accounts van oude telefoons en computers voordat je ze weg doet.**

Tip 2: **Maak een veilige kopie van je identiteits-document met de KopieID-app. Download deze gratis in de Play Store of de App Store.**

Tip 3: **Scherm je socialemediaprofielen af. Zo bepaal je zelf wie jouw berichten kan zien.**

Sociale media en internet

Oplichters zijn goed thuis op het internet. Daar verzamelen ze gegevens over jou, bijvoorbeeld via Google, Facebook, Instagram, LinkedIn en Twitter. Dat zijn vaak gegevens die je zelf deelt of gegevens waarvan je niet wist dat ze op het internet te vinden zijn. Oplichters brengen zorgvuldig jouw profiel in kaart en vervolgens handelen ze vanuit jouw naam.

Tip 4: **Weet wat je deelt via sociale media. Toon zeker geen foto’s van je paspoort, identiteitskaart of rijbewijs. En deel ook je telefoonnummer of e-mailadres niet in het openbaar.**

Herken identiteitsfraude

Staat jouw situatie hier niet tussen? Ga naar het algemene stappenplan

Fraude met (kopie) identiteitsdocument (paspoort, identiteitskaart of rijbewijs)

- Er staat bijvoorbeeld een bankrekening, telefoonabonnement, lening, creditcard of woonruimte op jouw naam, waar je niets van weet.
- Je ontvangt boze berichten van mensen die jou als oplichter zien, bijvoorbeeld omdat je hen via een online marktplaats zou hebben opgelicht.
- De politie verdenkt jou van iets dat je niet hebt gedaan.
- Je wordt aangehouden bij een grensovergang.
- Je kunt geen lening afsluiten of een hypotheek krijgen omdat er een registratie op je naam staat bij Stichting BKR.

Fraude met DigiD

- Je ziet onbekende werkgevers op pensioen- of belastingoverzichten staan.
- Je ontdekt op **mijn.overheid.nl** dat jouw gegevens bij de overheid zijn aangepast zonder dat je het weet. Bijvoorbeeld omdat je staat ingeschreven op een ander adres.
- Wanneer je inlogt op www.digid.nl zie je in je gebruikshistorie dat er is ingelogd op een moment dat je dat niet hebt gedaan.

Fraude met persoonsgegevens (zoals naam, adres en telefoonnummer)

- Je ontvangt pakketjes die je niet hebt besteld.
- Je ontvangt brieven of e-mails van incassobureaus of gerechtsdeurwaarders over schulden waar je niets van weet.
- Je kunt geen lening afsluiten of een hypotheek krijgen omdat er een registratie op je naam staat bij Stichting BKR.
- Met jouw naam en/of foto is een profiel aangemaakt op sociale media zonder dat jij hier vanaf weet.

Overige fraude (zoals gehackt account)

- Je contacten ontvangen e-mails van jou die je niet zelf hebt verstuurd.
- Op je rekeningoverzichten staan uitgaven die je niet herkent.
- Je krijgt een bevestiging van een bestelling die je niet zelf hebt gedaan.
- Je computer is gehackt, hierdoor hebben oplichters toegang tot je accounts en bestanden.
- De wachtwoorden van accounts zijn gewijzigd zonder dat je dit zelf hebt gedaan.

Fraude met (kopie) identiteitsdocument?

1 Meld identiteitsfraude bij het CMI. En doe aangifte bij de politie, maak hiervoor een afspraak via 0900 88 44. Neem zoveel mogelijk bewijsmateriaal mee.

2 Heb je het idee dat een kopie van je identiteitsdocument (paspoort, identiteitskaart, rijbewijs) in handen is gevallen van een oplichter? Overweeg dan om dit document uit voorzorg te vervangen. Is jouw orginele identiteitsdocument vermist of gestolen? Meld het direct bij de gemeente.

3 Vertel je privé- en/of zakelijke contacten dat je identiteitsgegevens gestolen zijn of dat je slachtoffer bent van identiteitsfraude.

4 Controleer je rekening-overzichten en overleg met je bank of verdere actie nodig is.

5 Controleer bij Stichting BKR of er onbekende kredietregistraties op jouw naam staan. Herhaal dit na een tijdje. Kijk voor meer informatie op www.bkr.nl.

6 Controleer op mijn.overheid.nl of je gegevens juist geregistreerd staan.

7 Heb je je gegevens gedeeld via een phishingbericht? Controleer met een virusscanner of er schadelijke software op je computer staat. Zorg er altijd voor dat je de laatste versie van de virusscanner hebt gedownload.

8 Bekijk ook het algemene stappenplan voor andere stappen die misschien bij jouw situatie passen.

Meld identiteitsfraude altijd bij het Centraal Meldpunt Identiteitsfraude (CMI) via www.rvig.nl/cmi.

Fraude met DigiD?

1 Controleer of iemand anders met jouw DigiD heeft ingelogd. Dit kun je zien in de gebruiksgeschiedenis van jouw DigiD. Ga naar de website van DigiD:

- Log in bij Mijn DigiD
- Kies voor 'Gebruiksgeschiedenis'

2 Zie je in jouw geschiedenis dat er is ingelogd vanaf een onbekende plek of klopt het tijdstip van inloggen niet? Dan is het mogelijk dat iemand anders uit jouw naam zaken heeft aangevraagd of veranderd. Neem contact op met de Helpdesk DigiD, via 088 123 65 55 of www.digid.nl/contact.

3 Heb je DigiD-gegevens ingevuld op een valse website (phishing)? Controleer of je nog kunt inloggen. Als dat lukt, wijzig dan direct je wachtwoord via Mijn DigiD. Kun je je wachtwoord niet wijzigen? Neem contact op met de Helpdesk DigiD.

4 Zorg dat je bewijsmateriaal, zoals screenshots, verzamelt. Meld misbruik bij DigiD, het CMI en de betreffende organisatie waar jouw gegevens zijn misbruikt. Doe ook aangifte bij de politie, maak hiervoor een afspraak via 0900 88 44, en neem bewijsmateriaal mee.

5 Controleer met een virusscanner of er schadelijke software op je computer staat. Zorg er altijd voor dat je de laatste versie van de virusscanner hebt gedownload.

6 Bekijk ook het algemene stappenplan voor andere stappen die misschien passen bij jouw situatie.

Meld identiteitsfraude altijd bij het Centraal Meldpunt Identiteitsfraude (CMI) via www.rvig.nl/cmi.

Fraude met persoonsgegevens (zoals naam, adres en telefoonnummer)?

1 Meld identiteitsfraude bij het CMI. En doe aangifte bij de politie, maak hiervoor een afspraak via 0900 88 44. Neem bewijsmateriaal mee, zoals een koopovereenkomst of e-mails van incassobureaus.

2 Zijn jouw gegevens gebruikt voor het doen van bestellingen en ontvang jij hiervoor de rekening? Neem dan contact op met het bedrijf of het incassobureau dat jou de rekening stuurt. Geef aan dat jij de bestelling niet hebt gedaan. Vraag om schriftelijk bewijs van de bestelling.

3 Stuur een kopie van de aangifte naar het bedrijf of incassobureau en vraag om de openstaande rekening in te trekken.

4 Controleer bij Stichting BKR of er onbekende kredietregistraties op jouw naam zijn binnengekomen. Herhaal dit na een tijdje. Kijk voor meer informatie op www.bkr.nl.

5 Bekijk ook het algemene stappenplan voor andere stappen die misschien passen bij jouw situatie.

Meld identiteitsfraude altijd bij het Centraal Meldpunt Identiteitsfraude (CMI) via www.rvig.nl/cmi.

Algemeen stappenplan Hoe herstel je identiteitsfraude?

1 Meld identiteitsfraude bij het CMI. En doe aangifte bij de politie, maak hiervoor een afspraak via 0900 88 44. Neem zoveel mogelijk bewijsmateriaal mee.

2 Neem contact op met de betrokken instanties waar je gegevens zijn misbruikt. Vraag om zoveel mogelijk bewijs waaruit blijkt dat er sprake is van identiteitsfraude. Denk hierbij aan kopieën van rekeningoverzichten, brieven van incassobureaus of contracten van abonnementen.

3 Ben je slachtoffer van identiteitsfraude? Doe dan aangifte bij de politie. Met een aangifte kan de politie een opsporingsonderzoek instellen en kun je duidelijk maken dat je slachtoffer bent van identiteitsfraude.

4 Wijzig wachtwoorden van je accounts regelmatig en gebruik voor elk account een ander wachtwoord. Deel je wachtwoorden niet met anderen. Log zoveel mogelijk in met 2 stappen (tweestapsverificatie). Je logt dan niet alleen in met je inlognaam en wachtwoord, maar gebruikt een extra toegangscode die je via een sms of speciale app ontvangt. Zie veiliginternetten.nl voor meer tips.

5 Heeft iemand anders op jouw naam een profiel aangemaakt op sociale media, een datingsite of een online marktplaats? Meld dit bij de organisatie en vraag ze om het profiel te verwijderen.

6 Vertel je privé- en/of zakelijke contacten dat je slachtoffer bent van identiteitsfraude.

7 Controleer bij Stichting BKR of er onbekende kredietregistraties op jouw naam zijn binnengekomen. Herhaal dit na een tijdje. Kijk voor meer informatie op www.bkr.nl.

8 Controleer met een virusscanner of er schadelijke software op je computer staat. Zorg er altijd voor dat je de laatste versie van de virusscanner hebt gedownload.

Meld identiteitsfraude altijd bij het Centraal Meldpunt Identiteitsfraude (CMI) via www.rvig.nl/cmi.

Wat is identiteitsfraude?
Voorkomen
Herkennen
Herstellen
Melden

Slachtoffer van identiteitsfraude?

Doe aangifte bij de politie wanneer je slachtoffer bent van identiteitsfraude, maak hiervoor een afspraak via **0900 88 44** (24/7 bereikbaar).

Meld het daarnaast bij het **Centraal Meldpunt Identiteitsfraude (CMI)**, dat kan met het meldingsformulier op onze **website**.
Het CMI denkt met je mee over de mogelijke risico's en helpt je om het misbruik te stoppen en de gevolgen te herstellen. Kom je er zelf niet uit met de betrokken organisaties? Dan kan het CMI ondersteunen door te bemiddelen.