Door @NicovanGog via AI gegenereerd
Alle reacties in AI kunnen fouten bevatten.

Na aanleiding van een grote data hack bij **Odido** is het voor 6,2 miljoen mensen oppassen geblazen.

Het lijkt veel deze handleiding, maar beter voorkomen dan genezen!

Handleiding:

Stel Odido schriftelijk aansprakelijk
Problemen en misbruik van uw gegevens die u nu en in de toekomst kan verwachten
Wat te doen bij misbruik

Als je door de recente hack bij Odido (februari 2026) schade lijdt of vreest voor je privacy, kun je de volgende stappen ondernemen om hen aansprakelijk te stellen:

1. Stel Odido schriftelijk aansprakelijk

Stuur een formele brief of e-mail (bij voorkeur aangetekend of via een officieel klachtkanaal) waarin je Odido aansprakelijk stelt voor de gevolgen van het datalek.

- **Inhoud:** Vermeld je klantgegevens, welke data van jou gelekt zijn (zie de mail die je van Odido hebt ontvangen) en dat je hen verantwoordelijk houdt op basis van de AVG (Privacywet).
- **Schade:** Geef aan welke schade je hebt geleden (bijv. kosten voor een nieuw identiteitsbewijs, financiële schade door fraude, of immateriële schade zoals stress).

2. Dien een formele klacht in

Gebruik de officiële kanalen van de provider om je onvrede vast te leggen:

- **Klachtenformulier:** Dien een officiële klacht in via de Odido Service pagina.
- **Privacy Officer:** Je kunt specifiek contact opnemen met de functionaris voor gegevensbescherming
  via privacy@odido.nl of bij ontdekte kwetsbaarheden
  via datalek@odido.nl.

3. Melding bij de Autoriteit Persoonsgegevens (AP)

Hoewel Odido het lek zelf al heeft gemeld, kun je als betrokkene ook een eigen tip of klacht indienen bij de Autoriteit Persoonsgegevens. Dit helpt de toezichthouder om de impact op individuen in kaart te brengen.

4. Juridische hulp inschakelen

- **Rechtsbijstand:** Heb je een rechtsbijstandverzekering? Zij kunnen je helpen bij het opstellen van de aansprakelijkheidsstelling en het claimen van een vergoeding.
- **Collectieve claims:** Bij grote lekken zoals deze (mogelijk 6,2 miljoen klanten) ontstaan vaak collectieve schadevergoedingsacties waarbij je je kunt aansluiten.

Belangrijk: Let scherp op phishing-berichten die misbruik maken van deze hack. Odido zal je **nooit** via mail vragen om betalingen te doen of wachtwoorden te delen.

Heb je al een **officiële bevestigingsmail** van Odido ontvangen waarin staat welke van jouw gegevens precies betrokken zijn bij dit lek?

Odido beheert een aantal bekende telecommerken in Nederland. Sinds de rebranding van T-Mobile en Tele2 Mobiel in september 2023, vallen de volgende labels onder het portfolio:

- Ben: Gericht op voordelige sim-only abonnementen en smartphones voor de consumentenmarkt.
- **Simpel**: Een "no-nonsense" aanbieder die zich uitsluitend focust op goedkope sim-only deals.
- **Tele2 Thuis**: Hoewel de mobiele tak van Tele2 is opgegaan in Odido, blijft de merknaam Tele2 voorlopig nog bestaan voor internet- en TV-diensten voor thuis.

Belangrijke wijziging:
De merken **T-Mobile Nederland** en **Tele2 Mobiel** zijn volledig verdwenen en direct vervangen door de merknaam Odido.

Wanneer criminelen beschikken over deze specifieke combinatie van gegevens, hebben ze in feite een **"identiteitsset"** in handen. Hiermee kunnen ze zich zowel online als offline als jij voordoen. De gevolgen kunnen variëren van irritant tot financieel catastrofaal.

Hier is een overzicht van de risico's, nu en in de toekomst:

1. Directe risico's (Nu)

- **Spear Phishing:** Omdat ze je naam, e-mail en klantnummer hebben, kunnen ze zeer overtuigende nepmails sturen (bijvoorbeeld namens je bank of telecomprovider). Ze noemen je klantnummer, wat de mail betrouwbaar doet lijken, om je zo te verleiden op malafide links te klikken.
- **Sim-swapping:** Met je mobiele nummer en geboortedatum kunnen criminelen proberen je provider te overtuigen om je

telefoonnummer over te zetten naar een nieuwe simkaart. Zodra zij je nummer hebben, kunnen ze sms-verificatiecodes (2FA) onderscheppen en zo toegang krijgen tot je bank-app of e-mail.

- **Identiteitsfraude bij aankopen:** Met je adres, naam en geboortedatum kunnen ze spullen bestellen op afbetaling (zoals via Klarna of Riverty). De rekening komt bij jou terecht, terwijl de spullen naar een afhaalpunt gaan.

---

2. Risico's op de middellange termijn

- **Aanvragen van leningen of abonnementen:** Met je paspoortnummer en IBAN kunnen criminelen proberen online leningen af te sluiten of dure telefoonabonnementen te nemen op jouw naam.
- **Bankrekeningen openen:** In sommige (buitenlandse) EU-landen is het proces om een rekening te openen minder streng. Met jouw identificatiegegevens kunnen ze een rekening openen die vervolgens wordt gebruikt voor witwassen (je wordt dan een onvrijwillige 'geldezel').
- **Social Engineering:** Ze kunnen de klantenservice van bedrijven bellen en zich als jou voordoen. Door je klantnummer en geboortedatum te noemen, "bewijzen" ze wie ze zijn en kunnen ze bijvoorbeeld je adres of wachtwoorden laten wijzigen.

---

3. Gevolgen in de toekomst

- **BKR-registratie en Schulden:** Als er op jouw naam leningen zijn afgesloten die niet worden betaald, krijg je een negatieve BKR-registratie. Dit kan betekenen dat je in de toekomst

geen hypotheek of lening meer kunt krijgen, zelfs jaren nadat de fraude is gepleegd.

- **Strafrechtelijk onderzoek:** Als jouw naam en identificatiegegevens gekoppeld worden aan illegale praktijken (zoals oplichting op Marktplaats of witwassen), kun jij door de politie als verdachte worden aangemerkt. Het bewijzen van je onschuld is een langdurig en stressvol proces.
- **Doxing en chantage:** Je privégegevens kunnen worden doorverkocht op het 'dark web', waardoor je jarenlang last kunt blijven houden van gerichte spam, ongewenste telefoontjes of zelfs pogingen tot afpersing.

Wat kun je nu doen om jezelf te beschermen?

Actie	Waarom?
Tweestapsverificatie (2FA)	Gebruik een authenticator-app (zoals Google of Microsoft) in plaats van SMS voor je belangrijkste accounts.
Meldpunt Identiteitsfraude	Als je weet dat je gegevens op straat liggen, meld dit bij het Centraal Meldpunt Identiteitsfraude (CMI).
Bank inlichten	Geef bij je bank aan dat je gegevens mogelijk gecompromitteerd zijn; zij kunnen extra waakzaam zijn op verdachte transacties.

ID-bewijs blokkeren	Als je paspoort- of rijbewijsnummer gelekt is, kun je overwegen deze als vermist op te geven en een nieuwe aan te vragen. Het oude documentnummer wordt dan internationaal als ongeldig geregistreerd.

Heb je het vermoeden dat je gegevens op dit moment al door iemand anders worden gebruikt?

Als je vermoedt dat je slachtoffer bent van identiteitsfraude, is het essentieel om **direct** in actie te komen. Volg dit stappenplan om de schade te beperken:

1. Directe acties bij de juiste instanties

- **Meld het bij het CMI:** Maak direct melding bij het Centraal Meldpunt Identiteitsfraude (CMI) van de Rijksdienst voor Identiteitsgegevens. Zij ondersteunen slachtoffers en helpen bij het herstellen van de gevolgen.
- **Doe aangifte bij de Politie:** Identiteitsfraude is een misdrijf. Je kunt bij de Politie aangifte doen, vaak ook online met je DigiD. Dit is je officiële bewijsstuk voor banken en bedrijven.
- **Informeer de Fraudehelpdesk:** Voor advies over de specifieke fraudemethode en om anderen te waarschuwen, kun je contact opnemen met de Fraudehelpdesk.

2. Beveilig je financiën en identiteit

- **Bank en Creditcard:** Neem contact op met je bank om je rekeningen extra te laten monitoren of tijdelijk te blokkeren. Controleer je afschrijvingen dagelijks op onbekende posten.
- **ID-bewijs blokkeren:** Als je paspoort- of rijbewijsnummer gelekt is, ga dan naar je gemeente om dit document als

vermist/fraudegevoelig op te geven. Je krijgt dan een nieuw document met een ander nummer, waardoor het oude waardeloos wordt voor fraudeurs.

- **Wachtwoorden wijzigen:** Verander direct de wachtwoorden van je belangrijkste accounts (e-mail, DigiD, bank) en stel, waar mogelijk, **tweestapsverificatie (2FA)** in via een authenticator-app.

3. Schade beperken bij bedrijven

- **Lopende abonnementen:** Heb je een klantnummer gedeeld? Bel die specifieke organisatie (bijv. je provider of energieleverancier) en laat een aantekening maken dat er sprake is van mogelijke fraude.
- **Bestellingen op jouw naam:** Krijg je rekeningen voor spullen die je niet hebt besteld? Betaal deze niet, maar stuur direct een kopie van je politie-aangifte naar de webshop of het incassobureau.

Tip: Houd vanaf nu een logboek bij van alle contactmomenten met instanties en bewaar kopieën van alle aangiftes en meldingen.

Wanneer je al verdachte transacties ziet en brieven van incassobureaus ontvangt, bevind je je in een actieve fraudesituatie. In **2026** is het cruciaal om onmiddellijk de volgende stappen te nemen om verdere financiële schade en juridische problemen te voorkomen:

1. Beveilig direct je bankrekening

- **Neem contact op met de bank:** Bel direct de fraudeafdeling van je bank om de verdachte transacties te melden. Vraag hen om je rekening te monitoren of tijdelijk te bevriezen om verdere opnames te voorkomen.

- **Melding Onterechte Incasso (MOI):** Voor onterechte automatische incasso's kun je bij je bank een MOI-procedure starten om het geld terug te laten boeken.
- **Nieuwe rekening:** Overweeg de huidige rekening te sluiten en een nieuwe te openen met een ander IBAN-nummer om herhaling te voorkomen.

2. Reageer op incassobrieven

Betaal de rekeningen **niet**, maar negeer ze ook niet. Dit kan leiden tot een negatieve registratie of rechtszaak.

- **Betwist de vordering:** Stuur een schriftelijke reactie (bij voorkeur aangetekend) naar het incassobureau. Geef aan dat er sprake is van identiteitsfraude en dat je de schuld niet erkent.
- **Stuur bewijslast mee:** Voeg een kopie van je politie-aangifte en de melding bij het CMI toe aan je brief. Dit is je juridische bewijs dat jij de aankoop niet hebt gedaan.
- **Controleer de echtheid:** Er circuleren ook valse incassobrieven van oplichters (phishing). Controleer de gegevens van het bureau via de Rijksoverheid.

3. Juridische en officiële stappen

- **Doe aangifte:** Als je dit nog niet hebt gedaan, doe dan direct online aangifte van identiteitsfraude bij de politie. Zonder proces-verbaal sta je juridisch zwak tegenover schuldeisers.
- **BKR-check:** Vraag je gegevens op bij het BKR om te zien of er al onterechte leningen of achterstanden op jouw naam zijn geregistreerd.
- **Juridisch Loket:** Voor hulp bij het opstellen van brieven aan incassobureaus kun je terecht bij het Juridisch Loket.

Belangrijke hulpbronnen:

- Centraal Meldpunt Identiteitsfraude (CMI) voor ondersteuning bij het herstellen van je identiteit.
- Fraudehelpdesk voor specifiek advies over incassofraude.