LANDSTRA DE GROOT ONLINE MEDIA

Odido Datalek:
Bescherm Je Inbox in 5 Minuten

Een praktische gids om phishing mails automatisch te herkennen

Gert de Groot - LG Online Media
Februari 2026

Wat is er gebeurd?

Begin februari 2026 werd het klantcontactsysteem van Odido gehackt. Criminelen hebben toegang gekregen tot persoonlijke gegevens van miljoenen klanten.

Gelekte gegevens

Voor de meeste klanten zijn de volgende gegevens buitgemaakt:

- ***Volledige naam***
- ***Klantnummer***
- ***Adres en woonplaats***
- ***Telefoonnummer***
- ***E-mailadres***
- ***IBAN*** *(rekeningnummer)*
- ***Geboortedatum***

Bij een beperkte groep klanten zijn ook identificatiegegevens (nummer en geldigheid paspoort/rijbewijs) gestolen. Dat wordt specifiek per account hack in de Odido e-mail benoemd.

Wat is NIET gelekt

- Je wachtwoord van 'Mijn Odido'
- Belgegevens (wie je hebt gebeld of wanneer)
- Locatiegegevens (waar je was)
- Factuurgegevens
- Scans van identiteitsbewijzen

Waarom is dit zo gevaarlijk?

Met de gestolen gegevens kunnen criminelen zeer overtuigende phishingmails, -sms'jes en telefoontjes versturen. Ze beschikken over:

- **Je correcte naam en adres** (lijkt authentiek)
- **Je klantnummer** (kunnen zich voordoen als Odido)
- **Je IBAN** (kunnen valse betalingsverzoeken sturen)
- **Je geboortedatum** (voor identiteitscontrole)

Belangrijkste risico: Een mail die begint met "Beste [jouw naam]", je correcte adres noemt en refereert aan je klantnummer lijkt 100% echt.

Precies daar rekenen criminelen op.

Het grootste probleem: elk woord "Odido" is nu verdacht

Veel mensen denken: "Ik let wel op mails van vreemde afzenders."

Maar dat is niet genoeg.

Criminelen gebruiken lookalike-domeinen

Niet alleen mails van @odido.nl zijn gevaarlijk. Criminelen registreren domeinnamen die echt lijken:

- odido-service.nl
- odido.support
- klantenservice-odido.com
- mijnodido.net
- verificatie.odido-info.com

Typfouten die je over het hoofd ziet

- oidido.nl (o en i verwisseld)
- odid0.nl (laatste o is een nul)
- 0dido.nl (eerste O is een nul)
- odldo.nl (i wordt een l)

Het echte domein staat vaak achterin

Een url als `verificatie.odido.mijndiensten.com` lijkt veilig, maar het echte domein is `.com`, niet `.odido.nl`. Het woord "odido" is hier gewoon onderdeel van een subdomein.

Conclusie: Je kunt niet meer op het oog zien of een mail echt is. Daarom heb je een automatisch filter nodig.

De oplossing: een slim mailfilter

In plaats van elke Odido-mail handmatig te beoordelen, kun je een automatisch filter instellen. Dit filter vangt:

- **Alle mails met "odido" in het afzenderadres** (welke extensie dan ook)
- **Alle mails met "odido" in het onderwerp**
- **Veelvoorkomende typfouten en varianten**
- **Verdachte phishingwoorden in combinatie met Odido**
- **Ook T-Mobile** (oude merknaam die criminelen kunnen gebruiken)

Deze mails komen dan in een speciale map/label waar je ze bewust en met extra argwaan bekijkt.

Gmail / Google Workspace: stap-voor-stap

Stap 1: Open Gmail-instellingen

1. Open Gmail in je browser
2. Klik rechtsboven op het tandwiel ⚙️
3. Kies "Alle instellingen bekijken"
4. Ga naar het tabblad "Filters en geblokkeerde adressen"
5. Klik op "Nieuw filter maken"

Stap 2: Kopieer de filtercriteria

Plak de volgende tekst in het veld "Bevat de woorden":

```
from:(odido) OR from:(oidido) OR from:(0dido) OR from:(odid0) OR from:(tmobile) OR from:(t-mobile) OR subject:(odido) OR subject:(oidido) OR subject:(0dido) OR subject:(odid0) OR subject:(t-mobile) OR subject:(tmobile) OR subject:(datalek) OR subject:(cyber aanval) OR subject:(cyberaanval) OR subject:(verificatie) OR subject:(verifieer je) OR subject:(account geblokkeerd) OR subject:(klik hier odido) OR subject:(log in odido) OR subject:(dringend odido)
```

Wat doet dit filter?

Dit filter vangt:

- Alle afzenders met "odido", "oidido", "0dido" of "odid0"
- Alle afzenders met "tmobile" of "t-mobile"
- Alle onderwerpregels met bovenstaande varianten
- Verdachte woorden: "datalek", "cyber aanval", "verificatie", "verifieer je"
- Typische phishingzinnen: "account geblokkeerd", "klik hier", "log in", "dringend"

Stap 3: Test het filter

1. Klik op "Zoeken" of "Filter maken met deze zoekopdracht"
2. Je ziet nu alle mails in je inbox die aan de criteria voldoen
3. Check of dit klopt (waarschijnlijk zie je echte Odido-mails én mogelijk al phishing)

Stap 4: Stel filteracties in

Klik op "Filter maken" en vink de volgende opties aan:

WEL aanvinken:

- ✅ Label toepassen: kies "Nieuw label" → vul in: ⚠️ ODIDO - VERIFICATIE NODIG
- ✅ Markeer als belangrijk (optioneel)
- ✅ Ster toepassen (optioneel, voor extra visuele waarschuwing)

NIET aanvinken:

- ❌ Overslaan van Postvak IN (anders zie je de mails niet!)
- ❌ Markeren als gelezen
- ❌ Verwijderen

Stap 5: Maak het label opvallend

1. Ga in je Gmail naar de labels in de linker zijbalk
2. Beweeg je muis over het label "⚠️ ODIDO - VERIFICATIE NODIG"
3. Klik op de drie puntjes (⋯)
4. Kies "Labelkleur"
5. Selecteer ROOD

Nu vallen alle Odido-gerelateerde mails direct op.

Stap 6: Activeer het filter

1. Klik op "Filter maken"
2. Je kunt optioneel aanvinken: "Filter ook toepassen op bestaande gesprekken" (als je oude Odido-mails ook wilt labelen)
3. Klik nogmaals op "Filter maken"

Het filter is nu actief en werkt automatisch voor alle nieuwe mails.

Andere mailpakketten

De bovenstaande stappen zijn specifiek voor Gmail en Google Workspace, maar het principe werkt overal:

Outlook / Outlook.com

1. Ga naar Instellingen → Regels → Nieuwe regel
2. Voorwaarde: "Onderwerp of hoofdtekst bevat"
3. Voeg toe: odido, oidido, 0dido, odid0, tmobile, verificatie, datalek
4. Actie: "Verplaatsen naar map" → maak nieuwe map "⚠️ ODIDO CHECK"
5. Of: "Categoriseren als" → maak rode categorie

Apple Mail

1. Mail → Voorkeuren → Regels
2. Nieuwe regel
3. Voorwaarde: "Van" of "Onderwerp" bevat
4. Voeg varianten toe (odido, oidido, 0dido, etc.)
5. Actie: "Verplaats naar mailbox" of "Wijzig kleur"

Thunderbird

1. Extra → Berichtfilters
2. Nieuw
3. Voorwaarde: "Onderwerp" of "Van" bevat
4. Actie: Label toewijzen of verplaatsen naar map

Dagelijkse routine: zo check je Odido-mails

Nu het filter actief is, krijg je automatisch waarschuwingen. Volg deze stappen elke keer als je een gelabelde mail ziet:

Controleer de afzender EXACT

- Klik op de afzendernaam om het volledige e-mailadres te zien
- Check letter voor letter: is het echt @odido.nl of @odido.com?
- Let op: @0dido.nl, @odido-service.nl of @odido.info zijn NEP

Beweeg je muis over links (maar klik NIET!)

- Hover met je cursor over elke link in de mail
- Linksonder in je browser zie je de echte bestemming
- Echte Odido-links beginnen met https://www.odido.nl of https://mijn.odido.nl
- Links naar odido-verificatie.com of odido.info-login.nl zijn NEP

Let op urgentietaal

Phishingmails gebruiken vaak druk en paniek:

- "Verifieer binnen 24 uur"
- "Je account wordt geblokkeerd"
- "Dringend actie vereist"
- "Klik hier om toegang te behouden"

Echte bedrijven geven je ruim de tijd en blokkeren accounts niet zomaar[4][5].

Zoek naar spelfouten en vreemde zinnen

Veel phishingmails bevatten:

- Spelfouten ("verficatie" in plaats van "verificatie")
- Vreemde zinsconstructies (vaak vanuit vertalers)
- Generieke aanhef ("Geachte klant" in plaats van je naam)

Als je twijfelt: dit doe je WEL en NIET

❌ NOOIT doen

- Klikken op links in verdachte mails
- Inloggen via een link in een mail
- Bellen naar telefoonnummers uit de mail
- Persoonlijke gegevens of wachtwoorden invullen
- Bijlagen openen uit onverwachte mails

✅ WEL doen

- **Typ zelf** https://www.odido.nl **in je browser**
- **Log in via de officiële website of app**
- **Bel 1200 (vanuit je Odido-toestel) of 0800-0092 (vast nummer)**
- **Check je Mijn Odido-account voor echte berichten**
- **Meld verdachte mails via spam@odido.nl**

Extra bescherming

Controleer je bankrekening regelmatig

Met je IBAN kunnen criminelen geen geld afschrijven (daarvoor is een machtiging nodig), maar ze kunnen wel:

- Valse facturen sturen met jouw IBAN erop
- Proberen incasso's te starten (die jouw bank gelukkig moet controleren)

Check wekelijks je rekening op vreemde transacties.

Schakel tweefactorauthenticatie in

1. Log in op mijn.odido.nl
2. Ga naar Accountinstellingen → Beveiliging
3. Schakel tweestapsverificatie in

Zo kan niemand in je account komen, zelfs niet met je wachtwoord[3].

Wijzig je wachtwoord (uit voorzorg)

Hoewel Odido meldt dat wachtwoorden niet zijn gelekt, is het verstandig om:

- Je Odido-wachtwoord te wijzigen
- Voor elke website een uniek wachtwoord te gebruiken
- Een wachtwoordmanager te gebruiken (1Password, Bitwarden, Dashlane)

Voor bedrijven: bescherm je hele team

Als je Google Workspace gebruikt voor je bedrijf, kun je dit filter organisatiebreed uitrollen:

Google Workspace Admin Console

1. Log in op admin.google.com
2. Ga naar Apps → Google Workspace → Gmail
3. Klik op Compliance → Content compliance
4. Voeg nieuwe regel toe met bovenstaande criteria
5. Pas toe op hele organisatie

Zo krijgen alle medewerkers automatisch dezelfde bescherming.

Instructie voor medewerkers

Deel deze gids met je team en zorg dat iedereen:

- Het filter heeft geïnstalleerd
- Weet hoe je verdachte mails herkent
- Weet bij wie ze twijfelgevallen kunnen melden

Conclusie

Het Odido-datalek maakt phishingaanvallen gevaarlijker dan ooit. Criminelen hebben genoeg informatie om zeer overtuigende mails te sturen.

Door een slim mailfilter in te stellen, creëer je een automatische waarschuwingszone. Je hoeft niet meer te gokken of een mail echt is: elke Odido-gerelateerde mail wordt gelabeld en krijgt extra aandacht.

Belangrijkste lessen:

1. Elk gebruik van "odido" in een mail is nu verdacht
2. Domeinextensies maken niet uit (niet alleen .nl en .com)
3. Klik nooit op links in Odido-mails
4. Typ altijd zelf odido.nl in je browser
5. Bij twijfel: bel 1200 of 0800-0092

Neem 5 minuten om het filter in te stellen.
Het scheelt je straks veel ellende.

Hulp nodig?

Weet je niet goed hoe je dit moet instellen of wil je dat we dit voor je bedrijf regelen?

Landstra de Groot Online Media
Wijkstraat 69
9901 AH Appingedam

Tel: 0596 - 683328
Mail: gertdegroot@landstradegroot.nl
Web: www.landstradegroot.nl

We helpen MKB-bedrijven in Eemsdelta met webdesign, SEO en online beveiliging. Neem contact op voor advies of ondersteuning.

References

- Security.nl. (2026, 11 februari). Odido waarschuwt miljoenen klanten voor datalek na hack klantcontactsysteem. https://www.security.nl/posting/924257/

- NieuweMobiel.nl. (2026, 11 februari). Groot datalek bij Odido: klantgegevens en IBAN-nummers buitgemaakt na cyberaanval. https://www.nieuwemobiel.nl/025325/26031/

- iCreate Magazine. (2026, 12 februari). Groot lek bij Odido: zo check je of jouw data gelekt is. https://www.icreatemagazine.nl/nieuws/groot-lek-bij-odido-zo-check-je-of-jouw-data-gelekt-is/

- De Orkaan. (2026, 12 februari). Datalek Odido: phishing die gaat komen. https://www.deorkaan.nl/datalek-odido-phishing-die-gaat-komen/

- RvIG. (2026, 11 februari). Datalek Odido veroorzaakt ongerustheid – CMI geeft advies. https://www.rvig.nl/nieuws/12-02-2026-datalek-odido-veroorzaakt-ongerustheid-cmi-geeft-advies