

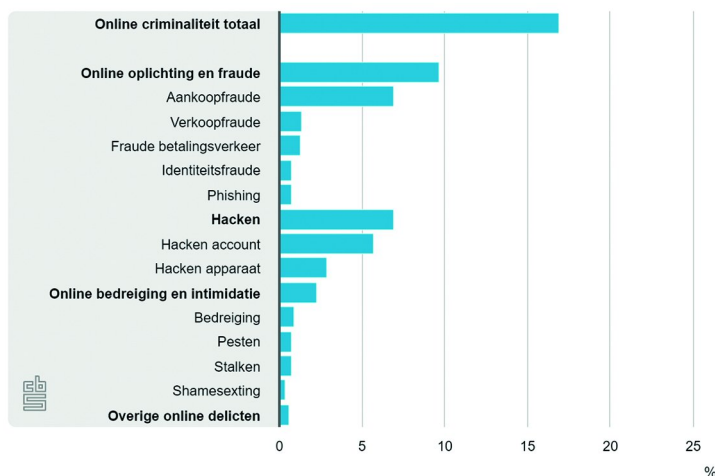
# ● Pas op voor online-zwandel! ●

Toon van Daele

Het is zuur als je te veel betaalt, maar veel erger is het wanneer je geld geeft aan oplichters. En helaas: online zijn er talrijke zwendelpraktijken. Om welke *scams* gaat het zoal, hoe herken en vermijd je ze, en wat als je er toch bent ingetuind?

Volgens het Centraal Bureau voor de Statistiek was in 2021 zo'n 17 procent van de Nederlanders van 15 jaar en ouder (dit zijn bijna 2,5 miljoen personen) slachtoffer van cybercriminaliteit, waaronder oplichting en transactiefraude. De laatste jaren zijn deze cijfers alleen maar gestegen en de verwachtingen voor 2022 zijn helaas niet anders.

Slachtoffers online criminaliteit, 2021



Onthutsende cijfers van het CBS over online zwendelpraktijken in Nederland

## Typische scenario's

Online oplichters maken frequent gebruik van *phishing*. Hierbij 'hengelen' criminelen naar je betaalgegevens of andere persoonlijke gegevens, zoals een pincode of een wachtwoord. Dit gebeurt doorgaans via e-mail, maar het kan ook via sms (*smishing*), sociale media (een bericht op bijvoorbeeld WhatsApp of Facebook) of zelfs telefonisch (*voice phishing* oftewel *vishing*).

Vaak gebruiken ze smoesjes om je in de val te lokken: je data zijn niet meer actueel en je moet ze actualiseren, je hebt recht op een terugbetaling, enzovoort. Meestal krijg je hiervoor een link die naar een - frauduleuze - site leidt, maar het gebeurt ook dat oplichters een valse advertentie van je bank op sociale media posten.

Een verwante vorm van oplichterij is die waarbij een crimineel via WhatsApp contact met je opneemt en zich als een kennis voordoot. Het kan zelfs gebeuren dat hij het WhatsApp-account van die kennis heeft gekaapt en op sociale media stemopnames heeft gevonden om je helemaal te overtuigen. Vaak hangt de oplichter dan een verhaal op waarbij je kennis zijn telefoon is kwijtgeraakt en dringend geld nodig heeft.

'Populair' is ook marktplaatsfraude. Malafide (ver)kopers versturen niet het beloofde product of ze voeren de betaling niet uit. Of ze gaan met jouw gegevens aan de haal om anderen op te lichten. Het gebeurt ook dat de frauduleuze

'verkoper' je geld laat overmaken naar een andere verkoper, die het bewuste product dan nietsvermoedend naar de fraudeur opstuurt.



Online oplichters trachten je op allerlei manieren persoonlijke gegevens te ontfutselen

## Hoe herkennen?

Phishing is dus een van de meest gebruikte technieken van online zwendelaars, en meestal gebeurt dit via e-mail. Het zou dus al veel helpen als je phishing-mails trefzekerder kunt herkennen. Leerzaam is alvast de 'valse berichten-quiz' op [www.fraudehulpdesk.nl/quiz/valse-berichten-quiz](http://www.fraudehulpdesk.nl/quiz/valse-berichten-quiz) waar je in diverse mails verdachte elementen moet aanwijzen.

Vaak begint zo'n phishing-mail met een onpersoonlijke aanhef (zoals Geachte klant), terwijl je bij bankzaken en aanverwanten toch een persoonlijker aanspreking zou verwachten. Helaas geeft ook deze laatste geen garanties: bij *spear phishing* maakt de oplichter namelijk gebruik van buitgemaakte persoonsgegevens, zoals je naam.

Taal- en typfouten of een bedenkelijke lay-out zijn doorgaans ook een goede indicatie van een oplichtingspoging, hoewel steeds meer phishing-mails zich van een fraaie vormgeving en keurig taalgebruik bedienen. Soms gaat het ook om *clone phishing*: er wordt dan een kopie van een authentieke mail gemaakt, maar wel aangevuld met malafide links of bijlagen.

Let tevens op de toon van het bericht: als je een gevoel van urgentie wordt aangepraat, is er vaak iets loos, zoals 'reageren binnen de twee dagen om hogere kosten of sancties te vermijden'.

Vaak blijkt ook het afzendadres niet met de vermeende afzender overeen te stemmen (bijvoorbeeld zoets als [mkr@cbnet.ru](mailto:mkr@cbnet.ru) voor een mail afkomstig van Post.nl). Houd er evenwel rekening mee dat sluwe oplichters zo'n adres kunnen vervalsen (*spoofing*), zodat het lijkt alsof het van de vermeende instantie afkomstig is.

Uw registratie bij Liantis

Liantis <info@pousadadocabra.com.br>  
aan info@websight.be Details tonen

Verdacht 10 okt (9 dagen geleden)  
Antwoord Acties

**liantis**

Geachte ondernemer,

U heeft tot op heden de digitale Liantis-sleutel nog niet bijgewerkt. Per ingang van 01 oktober 2022 zijn wij gestart met het uitgeven van digitale sleutels waarmee veilig gebruik kan worden gemaakt van de Liantis-diensten. Wegens onze nieuwe veiligheidsoverwegingen zijn al onze klanten verplicht hun meest recente contactgegevens bij te werken in ons klantensysteem. Wij attenderen u daarom nog eens erop om uw Liantis-sleutel aan te vragen. U hoeft tijdens deze procedure niet in te loggen. Wij vragen u enkel en alleen naar de actualiteit van uw gegevens.

U heeft tot 12 oktober 2022 om een aanvraag te doen voor uw digitale sleutel. Mocht u geen aanvraag hebben ingediend voor de gestelde datum dan zijn wij verplicht uw bedrijfsvorm als inactief te melden en heeft u geen recht meer op een Liantis-registratie. Start uw aanvraag nu via de onderstaande knop.

<https://t.co/1phqe61MPC>

**Aanvraag digitale sleutel**

Bij veel phishing-mails zijn de adressen (e-mail of web) vaak het enige herkenningspunt

di 19-1-2021 17:02

ING Bank N.V. <retail@ming.ing.nl>  
De beveiliging van uw ING-rekening is achterstallig

Aan Recipients

**ING**

Geachte klant,

We hebben onlangs een geavanceerde online beveiligingsoptie toegevoegd om uw ING Online bankieren beter te beveiligen, aangezien uw tevredenheid onze prioriteit is, moet u zich registreren in ons nieuwe verificatiesysteem.

Deze optie is verplicht.

Gebruik de onderstaande login om uw ING-online beveiliging bij te werken en te activeren, zodat u het hele jaar door onze service kunt blijven gebruiken.

**Inloggen**

Indien u deze stappen niet neemt, zullen wij om u te beschermen uw ING-rekening blokkeren en moet u een van onze kantoren bezoeken om uw identiteit te verifiëren.

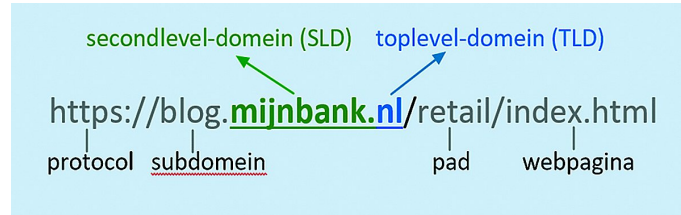
## Frauduleuze links

Wellicht het voornaamste kenmerk van phishing-mail zijn links naar frauduleuze webpagina's. Daarom is het belangrijk dat je nooit zomaar op een link in een mail klikt, maar eerst controleert waar zo'n link precies naar leidt! Op een pc of laptop doe je dit door met de muispijl boven een link te zweven. Linksonder of nabij de muiscursor verschijnt dan het bijbehorende webadres. Op een mobiel apparaat houd je de link ingedrukt tot er een venstertje met het webadres verschijnt.

Ga na of het webadres wel bij de vermeende afzender hoort, zoals je bank of een andere instelling. Let op voor *typo-squatting* (www.robabank.nl in plaats van www.rabobank.nl bijvoorbeeld) of voor andere sluwe aanpassingen als www.ing.nl-klanten.tk of www.login-ing.nl in plaats van www.ing.nl. Eigenlijk zijn alleen de twee 'domeinnamen' net voor de eerste enkele slash (/) van belang: bij https://login-ing.nl/ gaat het dan om login-ing.nl en bij www.ing.nl-klanten.tk/ om nl-klanten.tk en in beide geval-

len gaat het dus niet om (de bonafide domeinnaam) ing.nl.

Veel gebruikers begaan ook de vergissing een adres als betrouwbaar te zien wanneer dit met https:// in plaats van http:// begint. Dit betekent alleen dat het webverkeer met die site is versleuteld, het betekent niet (noodzakelijk) dat het om een bonafide site gaat!



Webadres checken? In dit voorbeeld draait het eigenlijk alleen om mijnbank.nl

## Sherlock

Heb je ook maar het geringste vermoeden dat de link niet naar een betrouwbare site verwijst, klik er dan nooit op! Eventueel kun je via een zogeheten whois-verzoek proberen na te gaan wie achter de registratie van de bijbehorende domeinnaam schuilt. Voor domeinnamen met .nl kan dit op [www.sidn.nl/whois](http://www.sidn.nl/whois) (tik hier bijvoorbeeld mijnbank.nl in). Voor andere, zoals .com, kan dit onder meer op [https://who.is](http://https://who.is)

Oplichters maken dikwijls ook gebruik van een zogeheten 'verkorte url' zodat het achterliggende webadres onzichtbaar kan blijven.

Zo'n url kan er bijvoorbeeld uitzien als: <https://t.co/1abc2def34>, <https://tiny.cc/mijnbank> of <https://bit.ly/1aBcD2e>.

Om te weten waar zo'n url daadwerkelijk naartoe leidt, kun je deze veilig intikken bij sites als <https://unshorten.it> of <https://checkjelinkje.nl>.

**Unshorten.It!**

<https://t.co/1phqe61MPC> Unshorten.It!

Not got a short URL to try? Here's one: <http://bit.ly/GVBJJS>

This website does not have a title available.

Destination URL:  
<https://web8873.web07.bero-webspace.de/38237Hsdusfd72sGsB>

Description:  
This site does not have a description available.

Safety Ratings (Provided by Web of Trust):  
Trustworthiness: Not enough ratings  
Child Safety: Not enough ratings

Blacklists:  
hpHosts - Service Unavailable

View Web of Trust Scorecard

Go to <https://web8873.web07.bero-webspace.de/38237Hsdusf...>

Diensten als Unshorten.it vertellen je waar een verkorte url naartoe leidt

## Do's en don't's

Nooit zomaar op links in (verdachte) e-mails of sms'en klikken, is dus essentieel, maar er zijn nog wel zaken waarop je

dient te letten. Zo is het een goed idee om in je browser zelf favorieten aan te maken die naar sites verwijzen van bijvoorbeeld je bank en andere instanties.

*Gebruik altijd deze favorieten in plaats van op een link te klikken.*

Open ook nooit zomaar bijlagen van onbekende e-mails en al zeker niet wanneer die bestandsextensies hebben als zip, exe, js, lnk, wsf, scr of jar. Immers, deze bestandstypes kunnen malafide code bevatten.

Ben je er niet zeker van of het om een phishing-mail gaat, dan kun je ook nog even checken op sites als:

<https://opgelicht.avrotros.nl/alerts> en [www.fraudehelpdesk.nl/actueel/valse-emails](http://www.fraudehelpdesk.nl/actueel/valse-emails) of het betreffende bericht als phishing-mail is vlagd. Bel ook geen telefoonnummers op die in de mail staan vermeld.

Bij twijfel bel je eventueel zelf de betreffende bank of instelling op. Dit nummer vind je zeker op de officiële website. Uiteraard houd je ook Windows, je applicaties en je antivirusprogramma mooi up-to-date.

Heb je wachtwoorden ingevuld, wijzig deze dan zo snel mogelijk, ook op andere sites waar je hetzelfde wachtwoord gebruikt. Je kunt ook altijd nakijken of je e-mailadres of telefoonnummer zich in een database bevond die inmiddels is gehackt. Je hoeft dit maar in te vullen op: <https://haveibeenpwned.com>

Heb je informatie over je creditcard prijsgegeven, neem dan meteen contact op met je creditcardmaatschappij om je kaart te blokkeren. Je kunt hiervoor ook terecht op: [www.creditcard.nl/faq/creditcard-blokkeren](http://www.creditcard.nl/faq/creditcard-blokkeren) of op <https://cardstop.be/nl/home/ik-wil-blokkeren.html>

Het is ook verstandig je bank op de hoogte te brengen. Ontvangen phishing-mails kun je, zoals aangegeven, eventueel uploaden naar sites als [www.fraudehelpdesk.nl](http://www.fraudehelpdesk.nl) maar wanneer je daadwerkelijk bent opgelicht tijdens een transactie, meld dit dan ook bij: [www.politie.nl/informatie/slachtoffer-van-internet-oplichting-doe-aangifte.html](http://www.politie.nl/informatie/slachtoffer-van-internet-oplichting-doe-aangifte.html)

In België kan dit bij <https://meldpunt.belgie.be> of rechtstreeks op: <https://meldpunt.belgie.be/meldpunt/nl/vragen/1> als het om phishing gaat.

The screenshot shows the 'Actuele valse e-mails' section of the Fraudehelpdesk.nl website. It features a search bar and a list of recent phishing emails. Each entry includes the sender's name (e.g., KVK, FedEx, ICS), the date (19 okt 2022), and a brief description of the email's content. For example, one entry from KVK mentions a change in the trade register, while another from ICS mentions a security alert.

Hier kun je recente phishing-mails opzoeken en ook zelf melden

## Wat nu?

Ondanks je voorzorgsmaatregelen en een flinke dosis gezond verstand ben je er toch ingetuind en heb je bijvoorbeeld op een foute link in een phishing-mail geklikt. Dit hoeft nog geen ramp te zijn, zolang je geen e-mailadres, wachtwoorden of kredietkaartgegevens op die (malafide) site hebt ingevuld.

Heb je toch een e-mailadres of persoonlijke gegevens als je naam of adres ingevuld, dan kun je wellicht meer spam verwachten, of de oplichters gebruiken die informatie om jou of je kennissen gerichter te kunnen benaderen (via *spoofing* of *spear phishing*). Heb je je mobiele nummer ingevuld, check dan even bij [www.payinfo.nl](http://www.payinfo.nl) en meld je af voor ongewenste betaaldiensten.

The screenshot shows the 'have i been pwned?' website. The main heading is ';-) have i been pwned?' with a subtext 'Check if your email or phone is in a data breach'. There is a search input field with a 'pwned?' button. Below this, a section titled 'Oh no — pwned!' states 'Pwned in 13 data breaches and found 2 pastes (subscribe to search sensitive breaches)'. It then lists '3 Steps to better security': 1. Use 1Password for strong passwords, 2. Enable 2-factor authentication, and 3. Subscribe to notifications and change passwords.

Ga regelmatig na of je e-mailadres in een gelekte databank voorkomt

