



Online



Veiligheid





Inleiding

Deze presentatie gaat over de basis van online veiligheid.
Wat voor soorten cybercrime bestaan er? Maar ook: hoe gaan criminelen te werk? Welke scams worden er toegepast?
Hoe zorg jij dat je geen slachtoffer wordt van een online crimineel?

We geven ook wat voorbeelden van welke fraudevormen toegepast worden en waar je up-to-date kunt blijven over welke misdadtrucs er actief zijn. We praten ook over waarom het internet nu gratis is.
Aan het einde van de presentatie zijn er nog wat handige links te vinden.



Cybercrime: wat is het?

Cybercrime is iedere vorm van criminaliteit waarbij het internet gebruikt wordt. Zo kun je denken aan digitale gijzeling. Dat is wanneer software op een computer terechtkomt waardoor de pc onbruikbaar wordt en er losgeld geëist wordt. Pas als dat betaald is, kan men weer bij de gegevens. Dit soort aanvallen wordt voornamelijk uitgevoerd op grotere instellingen zoals ziekenhuizen, scholen, gemeenten of grote bedrijven. Plekken waarvan criminelen weten dat ze er veel geld mee kunnen vangen.

Als een computer gegijzeld is, dreigen ze vaak met het lekken van gegevens of dat ze alles zullen vernietigen wat er op een netwerk staat. Het verwijderen van data kan veel problemen veroorzaken voor een bedrijf.

Cybercrime kan ook over kleinere dingen gaan. Denk dan aan een misleidende e-mail van iemand die zich voordoeft als de Belastingdienst. Ze vragen je om met spoed 200 euro over te maken. Je maakt alleen geen geld over naar de Belastingdienst, maar naar een persoonlijke rekening. Als je dit een keer gedaan hebt, proberen ze het vaak nog een keer met een hoger bedrag.



Cybercrime: wat is het?

Als iemands adresgegevens online worden gezet, wordt dat doxing genoemd. Ondanks dat het een klein vergrijp lijkt, is het toch illegaal en wordt het als een serieuze misdaad gezien. Adresgegevens worden vaker online gezet bij politieke verschillen op het internet als een vorm van sociale gerechtigheid.

Gegevens kunnen ook online gezet worden na een datalek. Denk dan aan de Odido-hack. Het is niet zo dat je gegevens overal meteen op het internet staan. Vaak worden deze gegevens voor een bedrag ergens op het internet verhandeld in lijsten. Zo kun je gegevens van honderd mensen misschien kopen voor 5 of 10 euro. Deze gegevens worden weer verhandeld aan mensen die phishingmails sturen of op zoek zijn naar Netflix-accounts.

De cybercrime is een hele industrie waar miljoenen in omgaan. In Nederland was in 2023 16% van de bevolking slachtoffer van een vorm van cybercrime. Slachtoffer worden van een online misdaad is iets wat zo kan gebeuren.



Een klein geschiedenis

Cybercrime is ook ergens begonnen. De eerste crimineel in de digitale wereld die wij kennen, was Allan Scherr. Als MIT-student wilde hij in het jaar 1962 meer tijd doorbrengen op de computer. Rond die tijd mocht iedereen maar vier uur per dag een schoolcomputer gebruiken. Hij verzong een manier om de wachtwoorden, die toen nog op ponskaarten stonden, te stelen.

Het eerste echte virus, de Creeper, was een computereperiment uit 1971. Het programma, geschreven door Bob Thomas, vermenigvuldigde zichzelf op computers die aangesloten waren op een netwerk. Het verspreidde zichzelf. Dit experiment was een voorloper van hoe klassieke virussen zich later zouden verspreiden.

Robert Morris is de eerste persoon in de geschiedenis die veroordeeld is voor het verspreiden van een virus: de Morris-worm. Hij creëerde een zelfreplicerend programma dat het netwerk van een universiteit overbelastte. Dit gebeurde in 1988.



Hackers

Bij het woord 'hackers' denken we vaak aan mensen die met kwade bedoelingen in andermans computers inbreken. Toch is dat beeld niet compleet: er bestaan verschillende soorten hackers. Sommigen gebruiken hun kennis juist om de grenzen van beveiliging te testen. Hoe goed is een systeem écht beveiligd, en op welke manieren kan die beveiliging verder worden verbeterd?

Hacken kan ook een vorm van protest zijn, zoals het bewust belasten van een netwerk om een mening te laten horen. Vaak zijn het mensen die ervan houden complexe problemen op te lossen. Denk maar aan een hackathon, waarbij groepen samenkomen om naar een bepaald vraagstuk te kijken.

Soms proberen hackers ook informatie naar buiten te brengen die overheden geheimhouden; websites als WikiLeaks hebben hierin een grote rol gespeeld. De term 'hacker' is dus eigenlijk een verzamelnaam die voor veel verschillende doeleinden wordt gebruikt.



Wat kan jij tegenkomen?

Op het internet kunnen we van alles tegenkomen. Iets wat veel voorkomt, is investeringsfraude. Een onbekende of een vage kennis zegt dat je veel geld kunt verdienen als je investeert in bijvoorbeeld bitcoin of een andere vorm van cryptogeld. Het lijkt eerst of je echt winst maakt; je krijgt zelfs een klein bedrag teruggestort. Daarna wordt er om meer geld gevraagd, zodat je nog grotere winsten kunt maken. Zodra het om een groot bedrag gaat, verbreekt de contactpersoon alle verbindingen en ben je je geld kwijt.

Een andere veelvoorkomende vorm is de zogeheten werkfraude. Je wordt gebeld of geappt door iemand die vraagt of je in je vrije tijd wat bij wilt verdienen, bijvoorbeeld door reviews te schrijven voor een kledingwebsite. Na de eerste opdrachten krijg je daadwerkelijk betaald. Alleen moet dat geld vervolgens weer terug de webwinkel in worden gestort, zogenaamd om de producten daadwerkelijk aan te schaffen zodat je er "echte" reviews over kunt schrijven. De bedragen die je zelf moet voorschieten worden steeds groter, totdat je doorhebt dat er iets niet klopt. Je wordt dan vaak emotioneel onder druk gezet om nog meer geld te storten om je eerdere inleg veilig te stellen.



Wat kan jij tegenkomen?

Een andere vorm van fraude die we zien, is familiefraude. Je wordt door een vreemd nummer bericht dat je zoon, neef of iemand anders snel geld nodig heeft, omdat diegene vast zou zitten in het buitenland. Ze zeggen dat ze een nieuw nummer hebben, omdat ze net hun telefoon kwijt zijn geraakt of een ander vaag smoesje. Vaak is je familielid daadwerkelijk in het buitenland.

Met informatie die openbaar te vinden is op bijvoorbeeld Facebook, weten ze dat je familie zich in het buitenland begeeft. Ze voeren emotionele druk op je uit, zodat je snel handelt. Vaak onder het mom van een noodsituatie.

De 'Love Scam' is ook iets wat veelvoudig voorkomt. Je komt op internet in contact met iemand die ergens anders in de wereld woont, maar soms ook gewoon in Nederland. Deze persoon windt je eerst om zijn of haar vinger. Dan heeft deze persoon ineens een keer geld nodig, omdat haar oma naar het ziekenhuis moet, er geld nodig is om te reizen naar een ziek familie lid of er moeten essentiële medicijnen gekocht worden. Als je er diep in zit, heb je het idee dat de persoon waarmee jij praat echt in nood zit en geld van je nodig heeft. In werkelijkheid is het een scammer die neprelaties met verschillende mensen onderhoudt. Ze gebruiken het geld misschien om hun eigen verslavingen te onderhouden of hun gezin te onderhouden. Verderop in de presentatie vinden we de link naar de aflevering van BOOS, waarin met slachtoffers en daders gesproken wordt over dit onderwerp.



Hoe bescherm ik mijzelf?

De eerste stap: neem een goed wachtwoord! Wachtwoorden zoals 'Superman123', 'Kemper00', 'PSV!!' of 'admin' zijn niet erg sterk; mensen met slechte intenties kunnen deze simpelweg raden. Het is belangrijk dat je op verschillende plekken andere wachtwoorden gebruikt. Als kwaadwillenden op één plek inbreken, kunnen ze in ieder geval niet meteen bij al je andere gegevens. Wanneer je overal hetzelfde wachtwoord gebruikt en dit wordt gekraakt, kunnen ze overal binnen. Een slecht wachtwoord is als een sleutel onder de deurmat: iedereen kan zo naar binnen lopen. Zorg er dus voor dat je verschillende sleutels hebt voor verschillende sloten.

Als je moeite hebt om wachtwoorden te onthouden, is de automatische wachtwoordopslag van je browser een prima plek om ze op te slaan. Je hoeft hiervoor geen extra programma's in gebruik te nemen; deze systemen zijn van zichzelf vaak al heel goed beveiligd.



Hoe bescherm ik mijzelf?

Het gaat niet alleen om het hebben van een sterk wachtwoord; je moet ook oplettend zijn met wie je praat. Is de persoon of instelling met wie je contact hebt wel echt wie je denkt dat het is? Mocht je een bericht krijgen van een vriend of familielid die snel geld nodig heeft omdat diegene ergens vastzit, bel dan niet het nummer terug waarmee je het bericht hebt ontvangen. Bel de persoon op via de contactgegevens die je al van hen hebt.

Dit is belangrijk omdat deepfake-technieken steeds vaker worden toegepast. Dit zijn technologieën waarmee mensen gezichten of stemmen kunnen kopiëren. Let daarom goed op of de persoon met wie je in contact staat een afwijkend spraakpatroon heeft. De technologie is vaak nog niet zo goed dat het echt menselijk klinkt. Vaak kan het ook nog niet live, maar gebeurt het via spraakopnamen of video's.



Hoe bescherm ik mijzelf?

Iets wat we niet kunnen vergeten is phishing. Dit zijn e-mails die nep zijn. Mensen doen zich voor als bedrijven, veelal de Belastingdienst, Justitie, Rijkswaterstaat, telecombedrijven of banken. Vaak vragen ze ineens geld voor een boete, abonnement of iets anders. Dit moet vaak snel afgehandeld worden, omdat je anders het risico loopt dat je boete veel hoger wordt.

Deze mails worden verstuurd vanuit het buitenland en zijn vaak geschreven in gebrekkig Nederlands. Vaak kloppen namen of logo's niet, of vermelden ze je naam niet eens. Echter, met de komst van nieuwe technologieën zoals AI kunnen teksten beter vertaald worden en lijken de mails steeds realistischer. De beste manier waaraan je een phishingmail kunt herkennen, is het e-mailadres.



Hoe bescherm ik mijzelf?

Let op de e-mailadressen; phishing-mails zijn vaak te herkennen aan hun rare email adressen. Zoals:

- DHL12984NO)348REpLY@Gmail.com,
- Cjib-niet-beantwoorden-administratieve-referentie.17F45E95-E8D1-2AD8-D3619F47B6083586@chamsswitch.com

Dit soort e-mails staan vaak in je spambox. Ze spelen in op haast; vaak staan er hoge boetes in of vragen ze je om snel een besteld pakketje te betalen.

Als iets of iemand online je onderdruk zet is het bijna altijd nep.

Vetrouw je iets niet, bel de desbetreffende instantie op met het nummer wat op de officiële website staat. Niet het nummer wat in de email staat.



Extra tips!

Brieven van de Belastingdienst bevatten nooit links naar websites. De Belastingdienst stuurt alleen berichten naar je persoonlijke inbox op Mijn Belastingdienst (belastingdienst.nl).

Vertrouw je een bericht of e-mail niet? Bel het desbetreffende bedrijf of de instelling op en controleer of het bericht wel echt van hen afkomstig is.

Houd ook in je achterhoofd: Bill Gates of een Nigeriaanse prins heeft nooit geld voor jou klaarliggen. Je hebt een grotere kans de loterij te winnen dan zomaar geld te krijgen van een vreemde op het internet.

Controleer daarom altijd het e-mailadres. E-mails van grote bedrijven zijn makkelijk te controleren; scammers gebruiken vaak vage e-mailadressen of adressen die net niet op de echte lijken.



Je bent er ingetrapt!

Het is niet erg; iedereen trapt er weleens in. Als ze je bankgegevens hebben, bel dan eerst de bank op, zodat zij eventuele fraudeurs kunnen blokkeren. Als je persoonlijk bent opgelicht, doe dan aangifte, zodat de politie op de hoogte is van de actieve fraudeurs.

Schaam je niet en vertel het aan vrienden en familie, zodat zij ook bewust zijn van de fraudetrucs die rondgaan. Een website zoals [Fraudehelpdesk.nl](https://www.fraudehelpdesk.nl) kan je helpen met het zoeken naar welke fraudetrucs op dit moment actief gebruikt worden. De website helpt ook als je slachtoffer geworden bent van fraude.



Cookies

Wat zijn cookies nu eigenlijk? Het zijn kleine tekstbestanden met gegevens die door een website worden opgeslagen op je computer. Er kan van alles in staan: informatie over je geslacht, e-mailadres, IP-adres of locatie. Deze informatie is geld waard en wordt vaak doorverkocht aan andere partijen.

Met deze data kunnen bedrijven gerichtere, persoonsgebonden reclames aanbieden. Zo weten ze precies wanneer jij op zoek bent naar een nieuwe koelkast of wat je vanavond wilt eten.

Toch hebben ze ook een praktisch nut: een cookie laat een digitaal 'kruimelpad' achter, waardoor een website je herkent en de volgende keer sneller laadt. Gelukkig heb je zelf de controle: cookies zijn altijd eenvoudig te verwijderen via je browserinstellingen.



Waarom is het internet gratis?

Cookies zijn de reden dat veel diensten op het internet gratis lijken: jouw data is namelijk geld waard! Bedrijven betalen flink wat geld om jou de juiste reclames te tonen, in de hoop dat je iets bij hen koopt. Ook je e-mailadres is waardevol; daarom wil bijna iedere website dit hebben. Ze gebruiken het om reclame naar je mailbox te sturen, zodat je sneller tot een aankoop overgaat.

Uiteindelijk maken Facebook en andere sociale media winst op jou door de gegevens die jij openbaar maakt, door te verkopen. Op het internet ben jij vaak het product. Hoe langer je een app gebruikt, hoe winstgevender je voor hen bent. Ga daarom verstandig om met de gegevens die je op het internet achterlaat.



De overheid

Voor de EU staat erom bekend sterke wetten te maken die de online veiligheid voor de Europese burger hoog in het vaandel hebben. In Europa moeten techbedrijven zich houden aan strenge regels voor hun algoritmes en het modereren van content. Deze regelgeving staat echter regelmatig op gespannen voet met landen als China en de Verenigde Staten, waar veel van deze grote techbedrijven zijn gevestigd en opereren.

Criminaliteit handhaven blijft lastig, ook omdat veel phishingpraktijken vanuit het buitenland worden aangestuurd. De arm van de EU kan geen mensen oppakken die gevestigd zijn in andere delen van de wereld. Omdat de digitale wereld geen grenzen heeft, maar de wetgeving wel, is internationale samenwerking lastig. Uiteindelijk ben je hierdoor als gebruiker vaak zelf de belangrijkste schakel in je eigen online veiligheid.



Interessante links

Website om op te zoeken of je data ergens gelekt is:

<https://haveibeenpwned.com/>

Fraudehelpdesk:

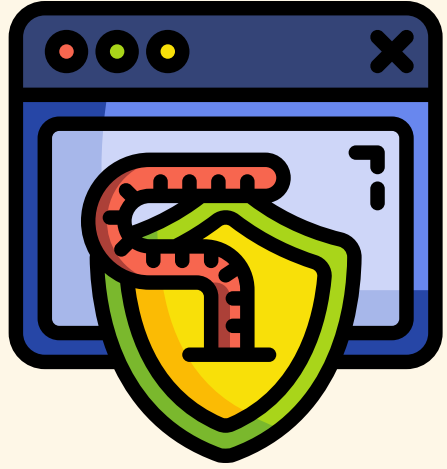
<https://www.fraudehelpdesk.nl/>

Aflevering boos, hoe gaat een fraude eraan toe:

<https://youtu.be/C400qDSboMg?si=ZTiUbAhfbmh06fJ>

In de volgende slides vind je voorbeelden van hoe eventuele phishingberichten eruit kunnen zien. Wil je weten welke fraudetrucs er op dit moment in omloop zijn?

Dan kun je de website van de Fraudehelpdesk raadplegen.



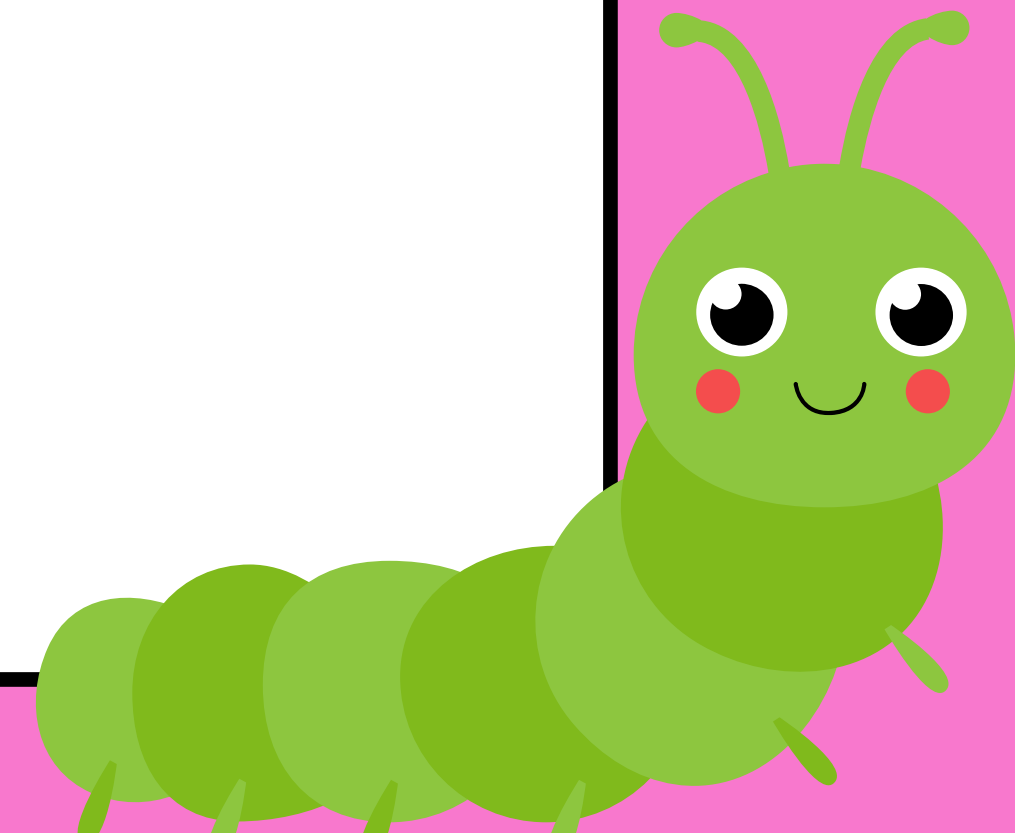
De klassieke fraude truc

Dear Sir,

I am prince [redacted] from Nigeria. Your help would be very appreciated. I want to transfer all of my fortune outside of Nigeria due to a frozen account, If you could be so kind and transfer small sum of 3 500 USD to my account, I would be able to unfreeze my account and transfer my money outside of Nigeria. To repay your kindness, I will send 1 000 000 USD to your account.

Please contact me to proceed

Prince [redacted]





Belastingdienst Fraude



Belastingdienst

Geachte heer/mevrouw,

Wegens de nieuwe belastingregels voor cryptovaluta die vanaf 2025 van kracht zijn, hebben wij u onlangs verzocht een verplicht formulier in te vullen met betrekking tot uw crypto-activa. We verzoeken u vriendelijk om het formulier vóór 10 maart 2025 in te dienen. Als u dit niet op tijd doet, loopt u het risico op een boete.

Let op: Als u geen cryptovaluta bezit, vragen wij u om het formulier niet in te dienen. Het onterecht indienen van het formulier kan resulteren in de verwerking van onjuiste gegevens.

[Formulier inleveren](#)

U bent verplicht om uw gegevens eerlijk en nauwkeurig in te vullen. Volgens het Europese Know Your Customer (OIC) beleid zijn wij verplicht om uw informatie te verifiëren bij de aangeboden aanbieder die u heeft opgegeven.

Met vriendelijke groet,
MijnOverheid

Dit is een automatisch gegenereerd bericht. Een reactie op dit bericht zal niet worden gelezen of beantwoord.



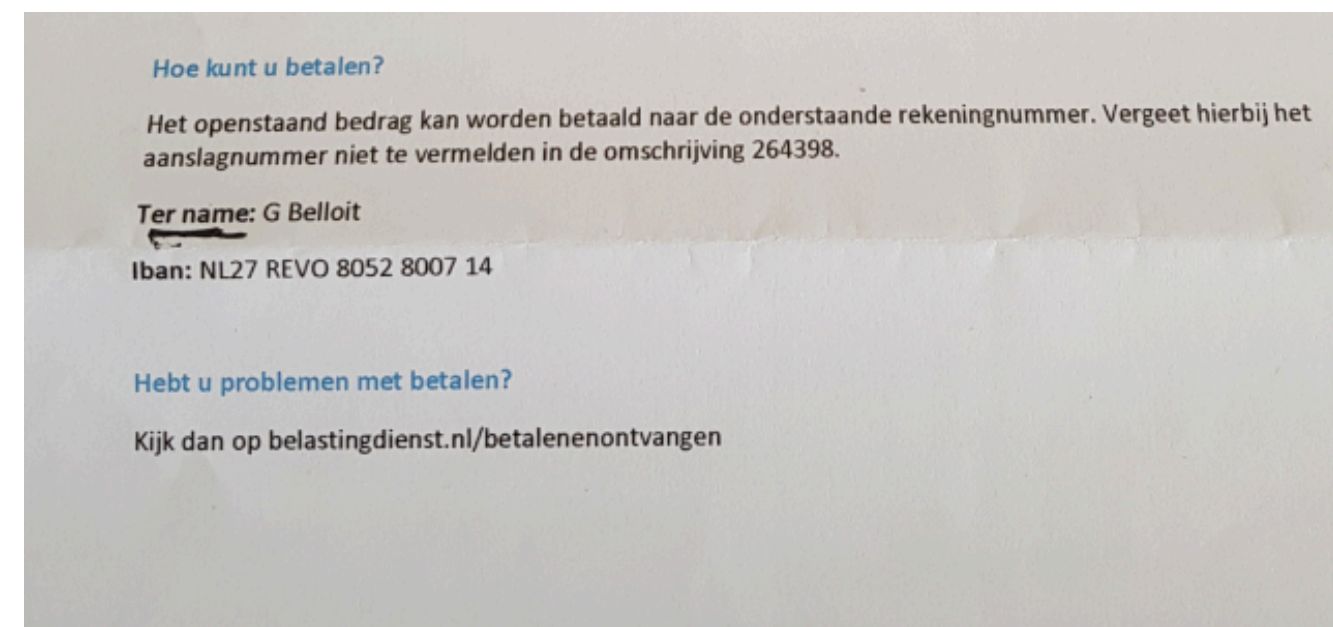
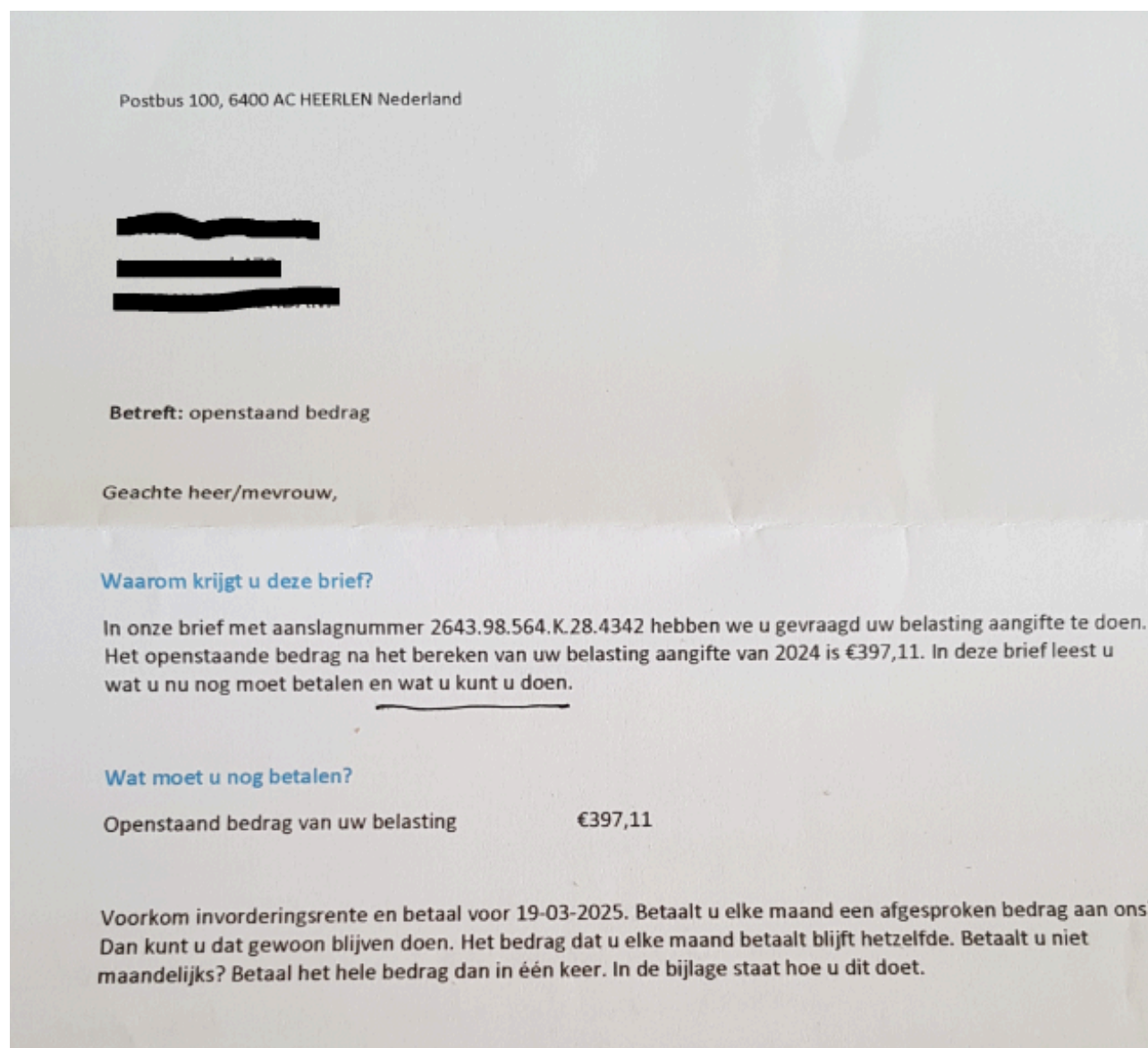
Sms fraude



[BELASTINGDIENST]: Uw openstaande schuld van €413,28 euro met kenmerk: [33924738](#) is ondanks meerdere herinneringen nog niet voldaan. Op 7 Maart 2024 zal de gerechtsdeurwaarder overgaan tot conservatoir beslag. Betaal nu direct via iDeal: <https://tikkie.me/pay/phf612uaeqb5rhaddt9p>



Brievenpost fraude





Tot slot

Het is belangrijk om alert te blijven wanneer je online met anderen communiceert. Het is niet per definitie verkeerd om met vreemden te praten, zolang je maar waakzaam blijft. Fraudeurs proberen misbruik te maken van een zwak moment of een kort gebrek aan concentratie. Slachtoffer worden van oplichting kan iedereen overkomen en is vaak zo gebeurd. Wees daarom extra alert op verdachte e-mails, vreemde telefoonnummers en mensen die je proberen te verleiden. Onthoud goed: als iets te mooi lijkt om waar te zijn, dan is dat meestal ook zo.

We hopen dat de wetgeving in de toekomst krachtig genoeg wordt om ook daders van buiten Europa aan te pakken. Sterke wetten zijn essentieel voor onze bescherming, maar helaas loopt de wetgeving soms achter op de nieuwste technieken van cybercriminelen. Het blijft een voortdurend kat-en-muisspel.

Vergeet daarnaast niet dat veel diensten op het internet niet zonder reden gratis zijn: jouw data is geld waard. Vrijwel elk platform verdient aan de informatie die jij achterlaat. In die zin ben je vaak geen gebruiker, maar het product.



Partners

TechClub is een project van Baltan Laboratories
in samenwerking met:

Buurthuis Rochus, Filmhuis Natlab, Bibliotheek Eindhoven, Bibliotheek Best, Bibliotheek Waalre en Bibliotheek Son en Breugel.

TechClub is tot stand gekomen met financiële steun van Provincie Noord-Brabant.

Provincie Noord-Brabant



BALTAN LABORATORIES