Preventie Cybercrime

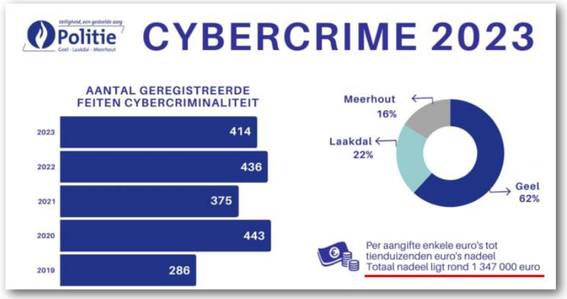
Veiligheid, een gedeelde zorg

Politie

Geel - Laakdal - Meerhout

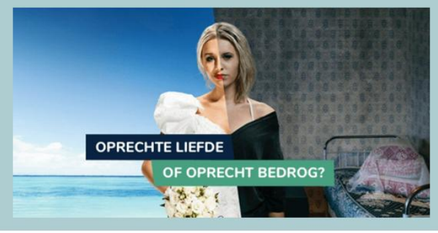
Overzicht

Cijfers politiezone GLM

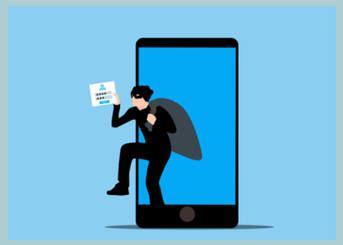


Phishing

Valse profielen / gestolen identiteit

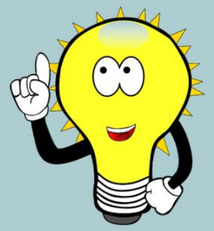


Social Media hacking



Scamming

Preventietips

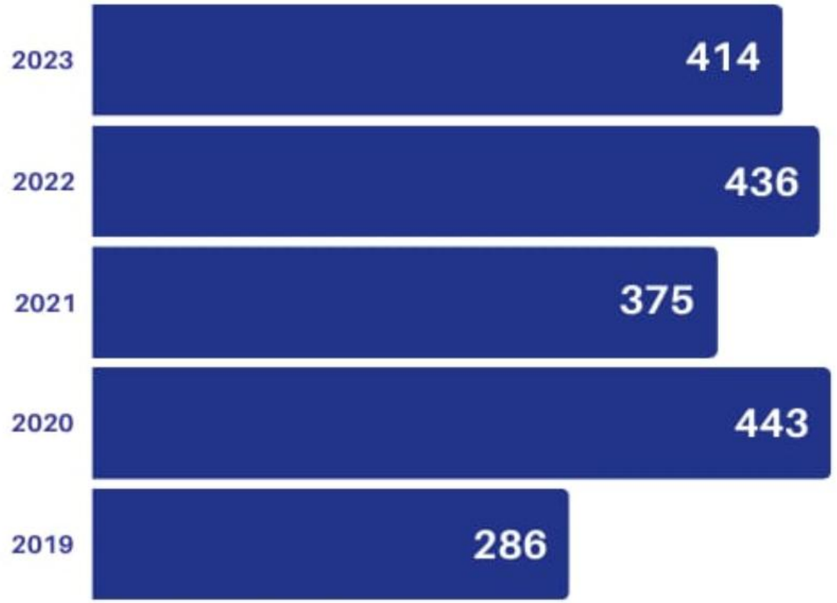


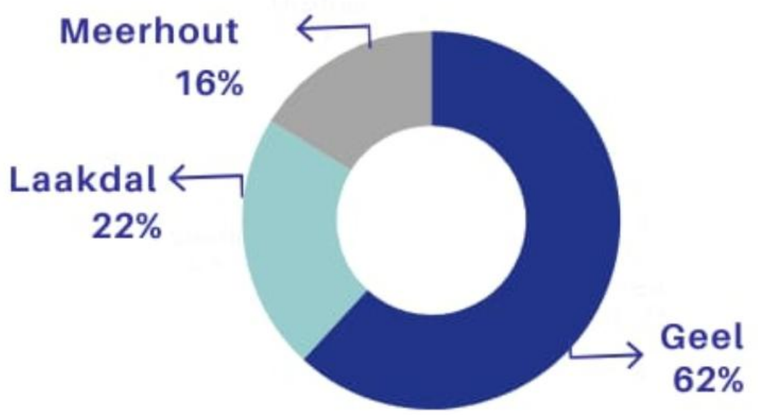
Cijfers politiezone GLM

Veiligheid, een gedeelde zorg
Politie
Geel - Laakdal - Meerhout

CYBERCRIME 2023

AANTAL GEREGISTREERDE FEITEN CYBERCRIMINALITEIT





Per aangifte enkele euro's tot tienduizenden euro's nadeel
Totaal nadeel ligt rond 1 347 000 euro

Cijfers politiezone GLM

Phishing

Phishing

- Phishing = *vissen* naar '**gegevens**' van slachtoffer
  - Wachtwoorden (sociale media, e-mail, …)
  - Contactgegevens (identiteit, persoonlijke informatie, …)
  - Bankgegevens (rekeningnummer, codes, …)

- Via **berichtjes** (e-mail, SMS, Whatsapp, Sociale media, …) of **telefoontjes**
  - naar heel **veel potentiële slachtoffers**
  - of **gericht** naar **1 of enkele personen**
    - Meestal na achterhalen persoonlijke gegevens

- Uiteindelijk doel = **GELD**!

Phishing

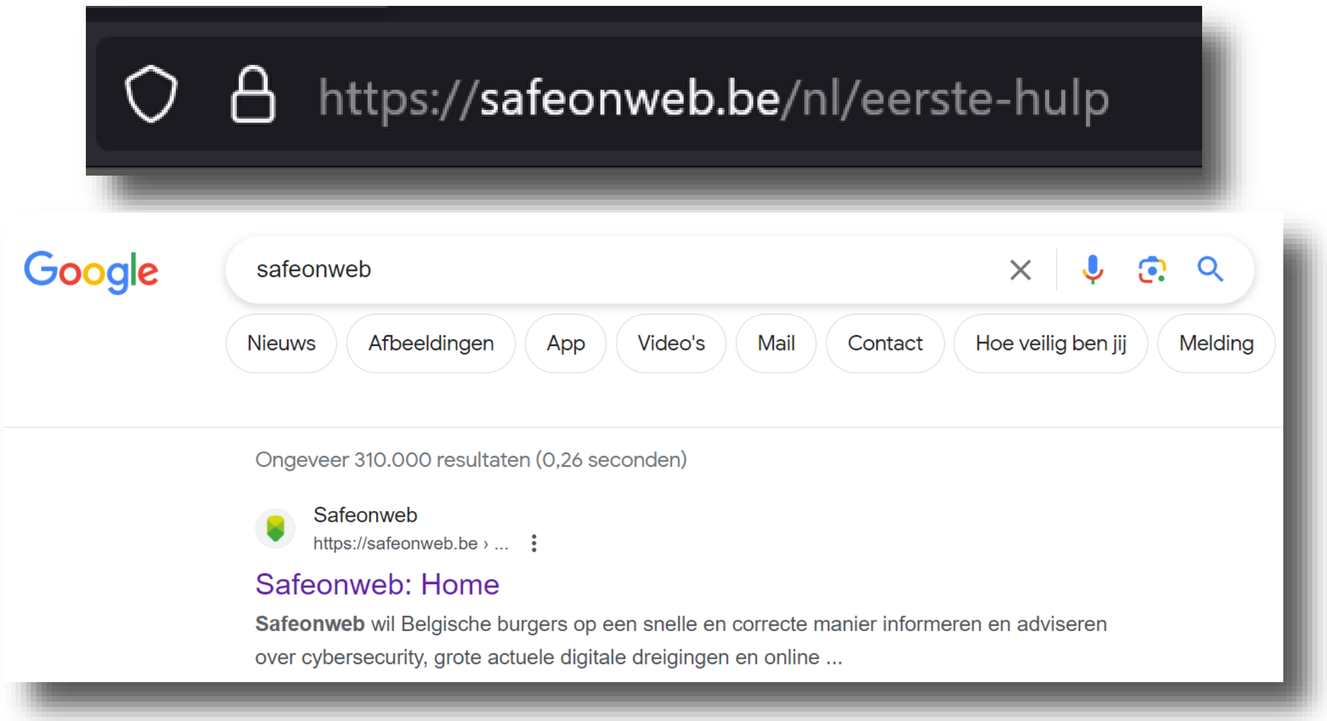
- **Kenmerken** van een phishing **bericht**
  - Het is **dringend** (je moet snel handelen)
  - Het bericht bevat een **link** of **QR code**

Klik hier!

- Wat zit er achter de **link**?
  - Een website die **persoonlijke informatie** vraagt
  - Een **nagemaakte website** waar je moet aanmelden
  - Een website die je een **App** wil laten installeren
  - …

Phishing – Links analyseren

- Ga op zoek naar de **domeinnaam** in een link!
  - **Controleer of de domeinnaam 'betrouwbaar' is**
    - Zoek eens met Google of Bing naar de website
  - Moderne browsers tonen de domeinnaam in het **vet**
    - Maar dan heb je al geklikt op de link ☺



Phishing – Links analyseren

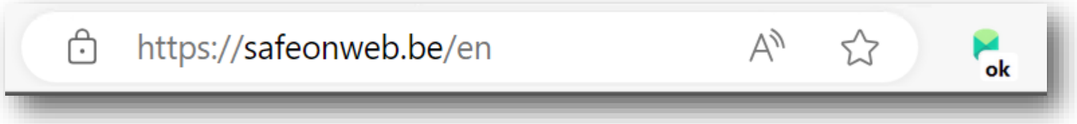
- Ga op zoek naar de **domeinnaam** in een link
  - Hoe je een domein zoekt wordt helder uitgelegd bij Safeonweb

https://surfenzonderzorgen.safeonweb.be

Phishing – Links analyseren

- Lange links kunnen ingekort worden met ***URL shorteners***
  - Bvb bit.ly, tiny.cc, shorturl.at, t.co
  - Controleer waar een korte link naar toe gaat via https://www.checkjelinkje.nl/

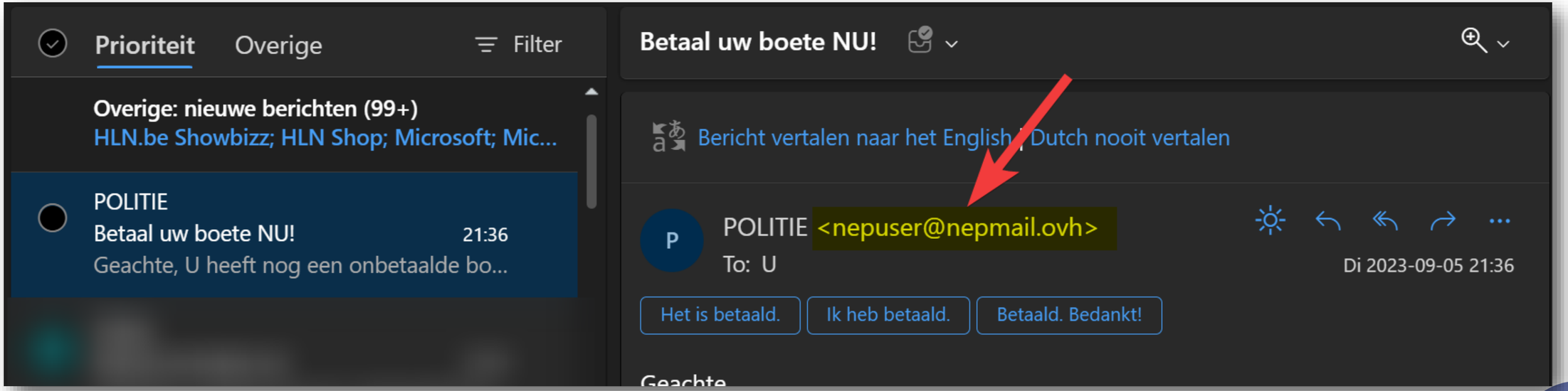
- **Hulpmiddelen** bij het analyseren van links
  - https://virustotal.com (kies voor URL controle)
  - https://www.scamadviser.com/
  - Safeonweb browser plug-in (chromium browsers)



Let op: je krijgt een **indicatie**, maar die is **niet altijd juist**!

E-mail Phishing

- Een phishing **e-mail** herkennen
  - Kijk naar het **e-mail adres van de afzender**
  - Kijk naar de **link** in het bericht
  - Kijk naar de **inhoud** van het bericht
    - Spelfouten, manier van schrijven, …



E-mail Phishing

<u>Maar let op!</u>

- Ken je het e-mail adres van de afzender
  - **Een bekende afzender is niet automatisch veilig!**
    - Afzender kan zelf slachtoffer zijn van phishing

- Staat er https:// in de link
  - **Een link die begint met https:// is niet automatisch veilig!**
    - Controleer de volledige link

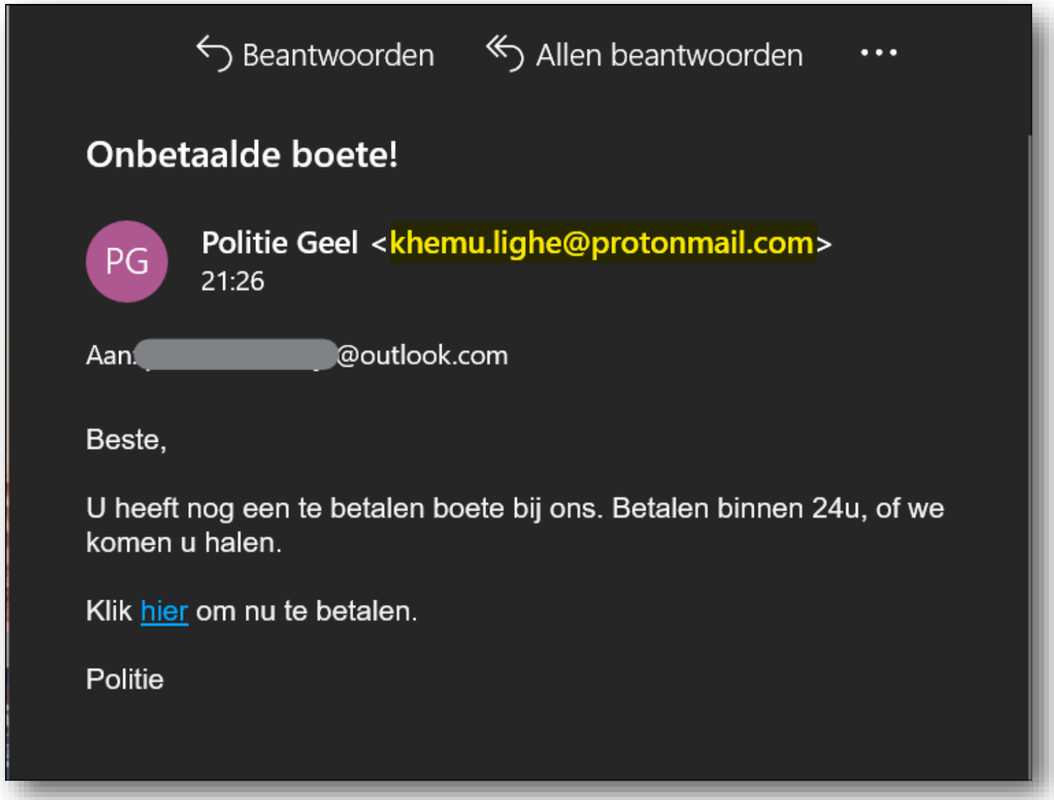
- Geen '*spelvauten*' maar perfecte tekst
  - **Vertaalprogramma's worden steeds beter**
    - Een vertaald bericht is soms beter geschreven dan een 'echt' bericht ☺

E-mail Phishing

E-mail op je smartphone

Geen e-mail adres van afzender!

E-mail op je computer



E-mail adres afzender zichtbaar!

Smishing (SMS phishing)

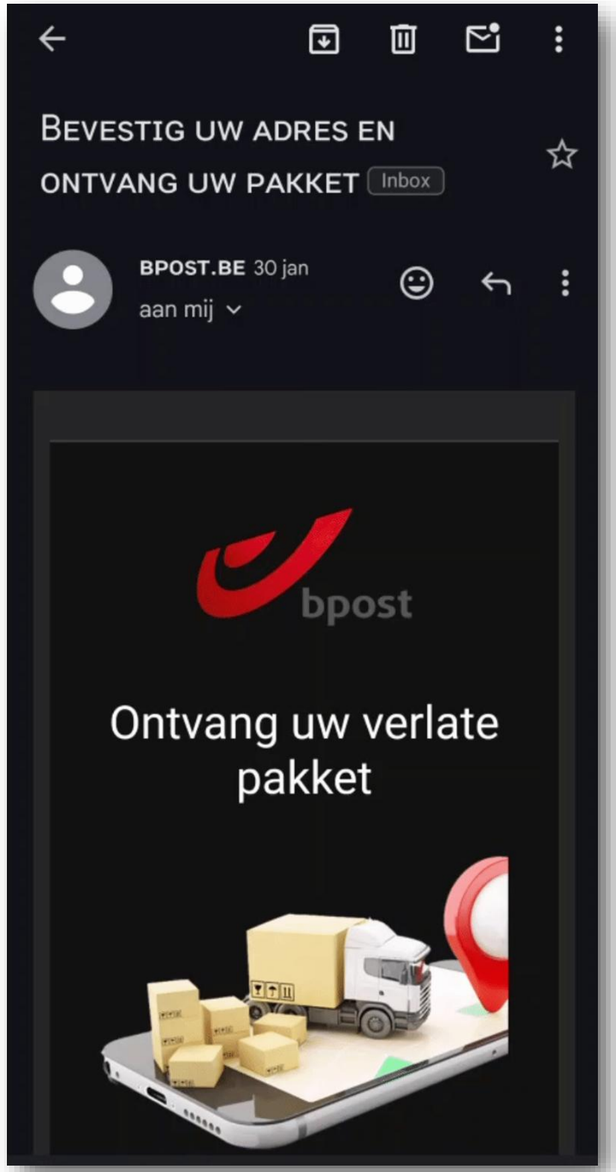
Een Smishing bericht herkennen

- Kijk naar het **GSM-nummer**
  - **Buitenlands** nummer?
  - **Bekend** nummer?
  - **Verkort** nummer?

- Controleer de **volledige link**!
  - Link kan niet verborgen worden

Phishing links

- Link/e-mail adres op **smartphone**
  - Lang **drukken** (niet tikken!)



Phishing via briefpost!

- **Factuur** phishing
  - Echte factuur onderscheppen
  - Rekeningnummer aanpassen
  - Telefoonnummer aanpassen

Slachtoffer schrijft geld over naar verkeerde rekening!

Vishing (Voice phishing)

- Telefonische phishing
  - **Valse bankmedewerker**
    - *“Er is een probleem met uw rekening”*
    - Vertrouwen wekken
      - Met persoonlijke gegevens die ze hebben buitgemaakt
    - Geld overschrijven naar een “**veilige rekening**”

- Preventietip
  - Bel zelf terug naar de bank!

Chantal uit Weelde ziet 100.000 euro verdwijnen door spoofing: "Ik werd gebeld met het nummer van mijn bank"

Chantal Janssens uit Weelde (Ravels) was in enkele uren 100.000 euro kwijt, toen ze het slachtoffer werd van spoofing, een vorm van oplichting waarbij de dader een valse identiteit aanneemt. Ze had telefoon gekregen van haar bank - het nummer klopte - en kreeg te horen dat internetcriminelen probeerden in te loggen op haar rekeningen. Daarop werd haar aangeraden om haar spaargeld over te schrijven naar een andere rekening. Dat was die van de oplichters. Ze wil nu iedereen waarschuwen.

Radio 2, An Verstuyft
ma 10 okt 08:30

Vishing (Voice phishing)

- Telefonische phishing
  - **Bankkaart fraude**
    - Doelgroep: vooral **senioren**
    - *“Er is een probleem met uw bankkaart, we komen uw bankkaart ophalen en vernietigen”*
    - **Vertrouwen wekken**
    - Criminelen komen **ter plaatse**!
      - Bankkaart en pincode ontfutselen

- Preventietip
  - Je bank komt niet langs bij jou!
  - Wees waakzaam voor babbeltrucs (Ook aan de deur. Bv valse politieagenten)

François (89) verloor 8.000 euro door bankkaartfraude, en hij is niet de enige: “Verblind door geld worden senioren opgelicht”

TURNHOUT - **Drie jonge Nederlanders stonden woensdag in Turnhout terecht voor bankkaartfraude bij enkele tachtigers uit Turnhout. Ze riskeren celstraffen van een jaar tot 37 maanden. Een van de slachtoffers is François Vissers (89) uit Turnhout, bij wie de daders begin maart erin slaagden om 8.000 euro af te halen. “Ik wil vooral mijn geld terug”, zei de tachtiger op de rechtbank.**

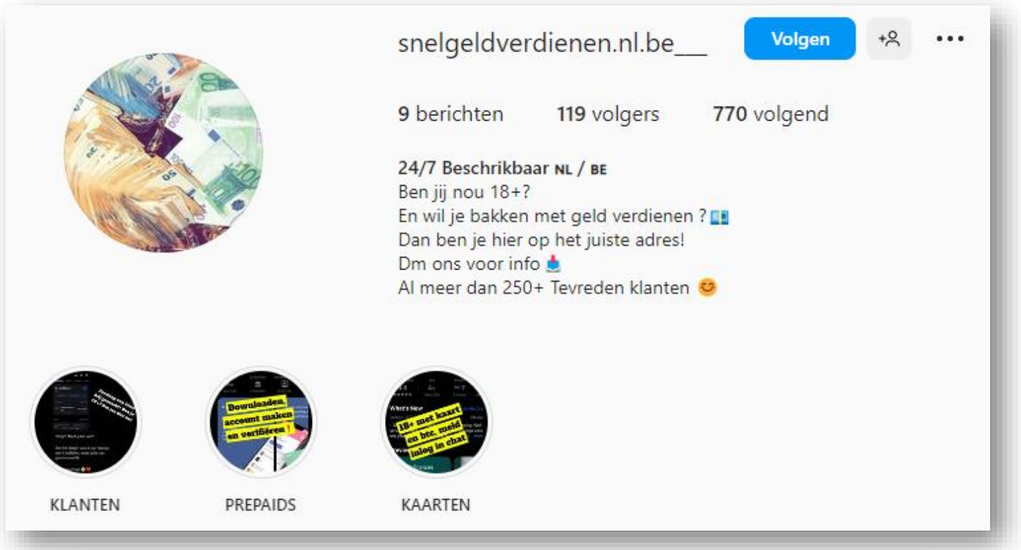
Phishing – Wat met het geld?

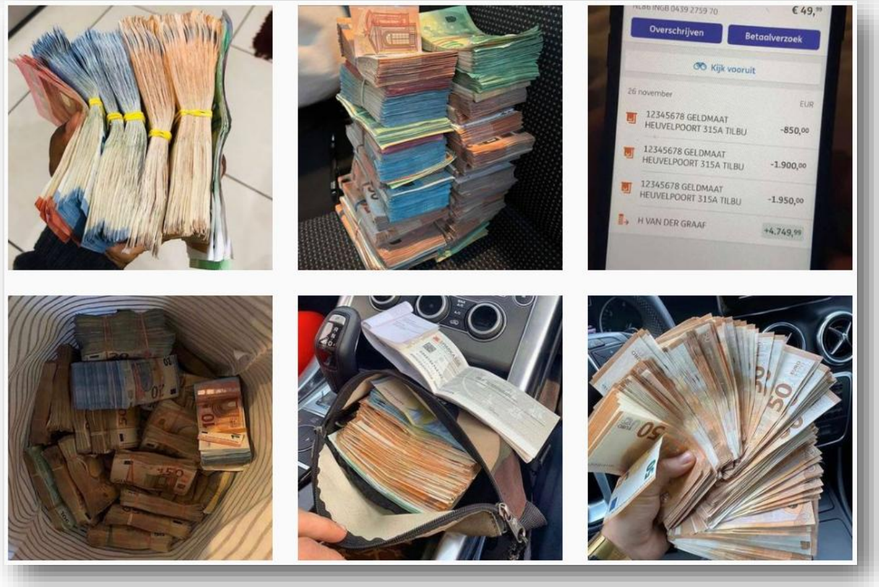
- Wat doen criminelen met het geld?
  - Online **aankopen** (materiaal, Bitcoin, …)
    - Recuperatie is zeer moeilijk
  - Overzetten naar **buitenlandse rekening**
    - Recuperatie is zeer moeilijk
  - Overzetten naar **Belgische rekening**
    - Via **geldezels**
    - Is door politie te traceren

- Tip
  - Doe **zo snel mogelijk** aangifte
    - Ook voor kleinere bedragen

Phishing – Geldezels

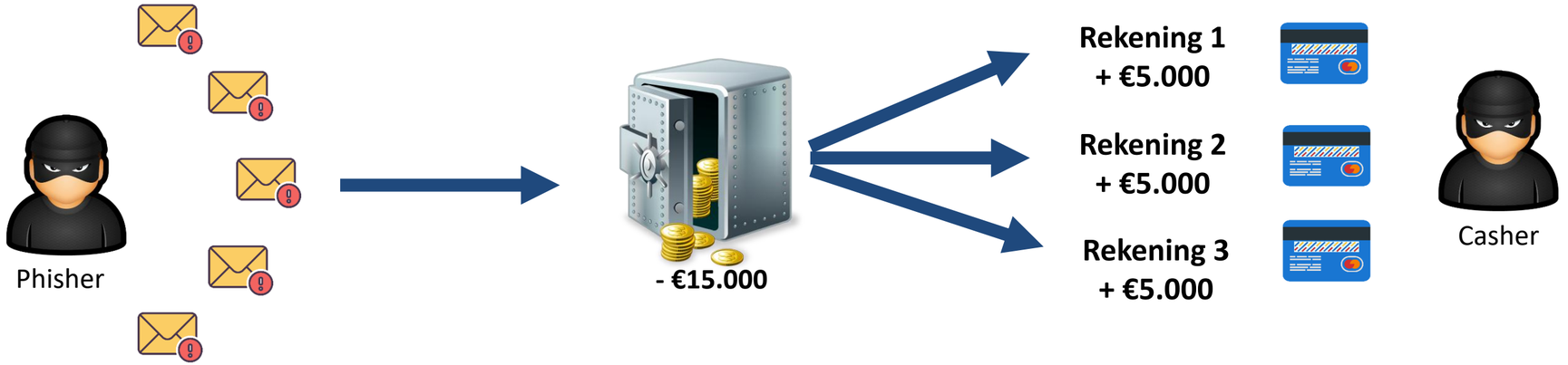
- Geldezel = tussenpersoon
  - Doelgroep: **jongeren**
  - Geronseld via **Social Media**
  - Krijgt een **beloning**
    - Uitlenen van **bankrekening en –kaart**
  - Pleegt zelf een **strafbaar feit**!
    - Pakkans = 100%
    - Veroordeling + strafblad
    - Zwarte lijst bij de bank





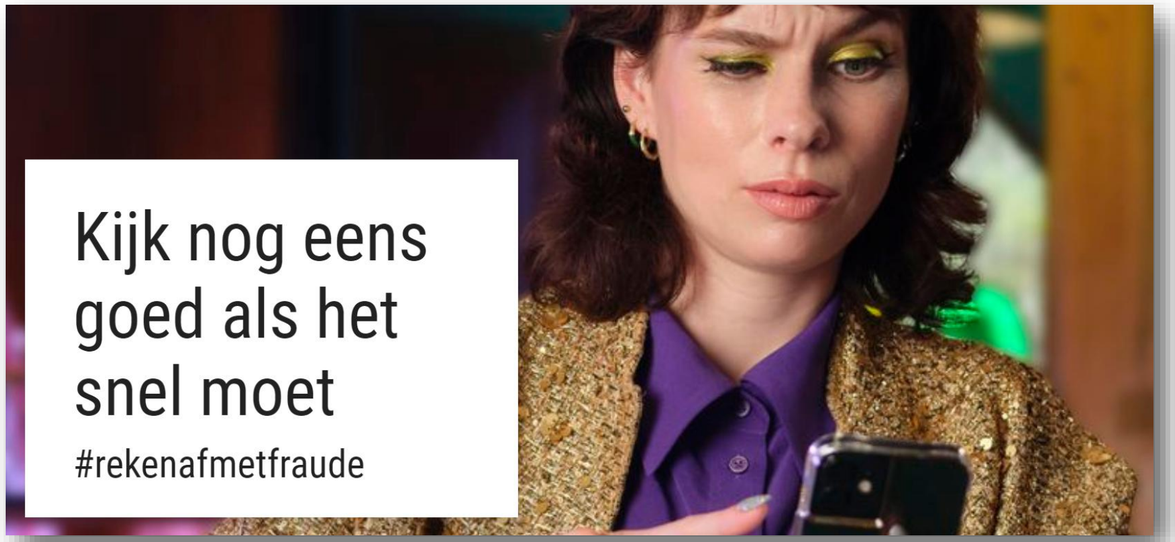
https://moremoney.be

Phishing – Geldezels



Phishing – Preventietips!

- Wees alert voor links in berichten. Klik niet zonder na te denken!
  - **Controleer de link**. Is het domein verdacht => niet klikken!
- Een bericht van je bank, sociale media, …
  - Ga steeds **via een vertrouwde manier** naar de website
    - Zet belangrijke websites bij je **favorieten**
    - **Zoek de website** via google/bing/…
- Ken je de **afzender**?
  - Kijk naar het **e-mail adres**!!!
- **Verwacht** je het bericht?
- Is het **dringend**?
  - Niet meteen reageren, eerst nadenken!



Phishing – Preventietips!

- Gebruik **complexe wachtwoorden**
  - Lange wachtwoorden kunnen moeilijker ‘geraden’ worden
- Gebruik **nooit hetzelfde wachtwoord** voor verschillende toepassingen
  - Geldt ook voor je **PIN codes**!
  - Gebruik een **wachtwoordkluis** of een wachtwoordboekje als geheugensteun
- Kies indien mogelijk voor **tweestapsverificatie**
  - Extra bevestiging bij het aanmelden
- Installeer steeds officiële **software updates** voor je systemen
  - Zo maak je je systemen minder kwetsbaar
- Installeer een **antivirusprogramma**
  - Minder kans dat gegevens gestolen worden via een virus

Vishing – Preventietips!

- **Vertrouw niet op een telefoonnummer**
  - Een telefoonnummer op je scherm kan vervalst zijn (spoofing)

- **Bel zelf terug** naar de contactpersoon (bank, …) bij twijfel
  - Als je zelf belt kom je op de juiste plaats terecht!

- **Geef nooit codes** of andere persoonlijke informatie aan de telefoon
  - Een code van een kaartlezer doorgeven is hetzelfde als de pincode van je bankkaart doorgeven!

Phishing – Berichten rapporteren!

- Stuur verdachte berichten naar verdacht@safeonweb.be
  - **E-mail** berichten => doorsturen
  - **SMS** berichten => **schermafbeelding** doorsturen
  - Automatische analyse, je krijgt **geen terugkoppeling**!
  - Slechte links worden **(inter)nationaal geblokkeerd**

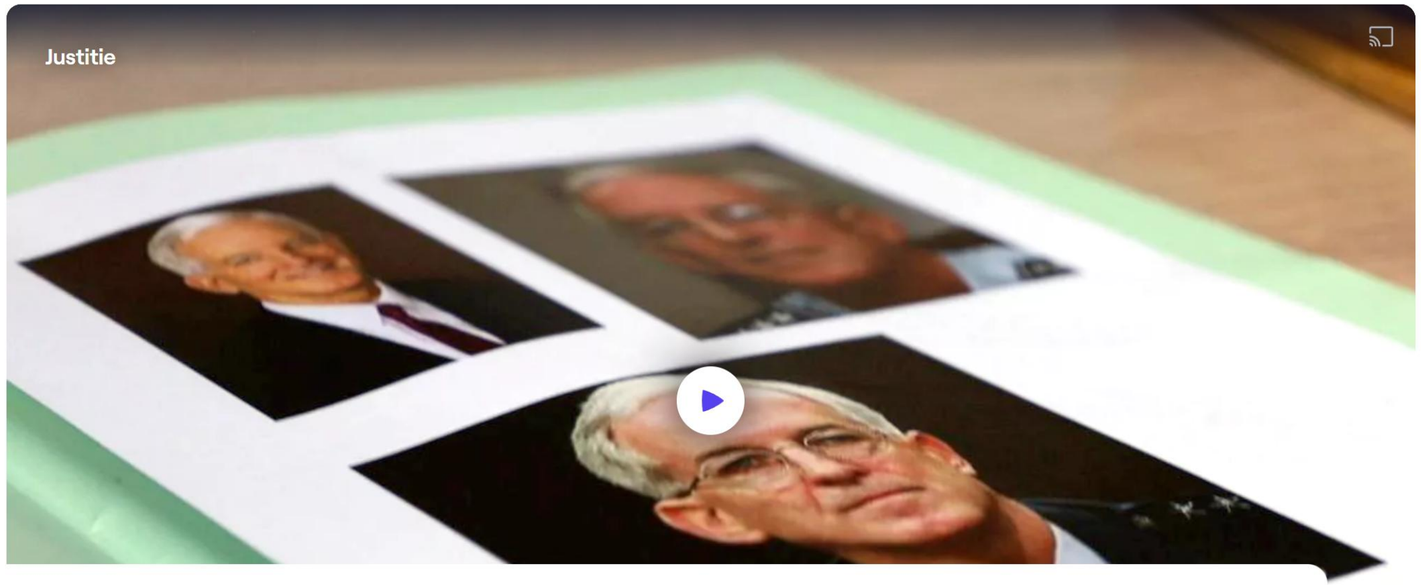
Valse profielen / gestolen identiteit

Vriendschapsfraude

- Vals account op sociale media / dating app
  - **Aantrekkelijke** personen
  - Vrienden aantrekken
    - Slachtoffer **bewust kiezen**
  - **Vertrouwensrelatie opbouwen**
    - Kan maanden duren
  - **Vertrouwen** misbruiken
    - *“Ik heb geld nodig!”*

[Getuigenis vriendschapsfraude]

Vriendschapsfraude



Dit zijn de slachtoffers van vriendschapsfraude: Katelijne schreef 40.000 euro over naar haar "Amerikaanse generaal"

Wie zit er achter die 2.000 meldingen van vriendschapsfraude? Zo'n drie jaar geleden kreeg Katelijne* een vriendschapsverzoek van een - zogezegde - Amerikaanse generaal. Ze raken aan de praat. Maandenlang voeren ze gesprekken. En dan begint hij geld te vragen. Veel geld.

Nagemaakte profielen

- Nagemaakte accounts op sociale media
  - **Persoonlijke informatie** van vrienden verzamelen
    - Vb om gerichte phishing mails te sturen
  - **Geld aftroggelen**
    - Vb Fans van bekend persoon
  - **Reputatie schaden**
    - Foute uitspraken doen

Nagemaakte profielen

vrt nws

Hoofdpunten Regio Kijk Luister Meest recent Zoek

Metejoor waarschuwt fans voor oplichters op sociale media: "Sommigen betaalden al honderden euro's"

Zanger Metejoor wil zijn fans waarschuwen voor oplichters, die zich voordoen als de zanger en die daarna geld aftroggelen. Dat staat in Dag Allemaal en bevestigt Joris van Rossem, zoals Metejoor echt heet, aan onze redactie. De zanger krijgt geregeld meldingen van fans die zeggen dat er een vals account van Metejoor op Facebook of Instagram is opgedoken. Sommige fans hebben ook al geld betaald aan de oplichters.

Top Nieuwste Personen Media Lijsten

Metejoor
@Metejoor921651
Volgen

Metejoor Joris
@MetejoorJ49560
Volgen
Artist DIT IS MIJN ENIGE PRIVÉ-ACCOUNT ALLEEN VOOR FAMILIE EN FANS 👍👍

metejoor
@Metejoor90
Volgen

MeteJoor
@MeteJ94319
Volgen

Metejoor
@Metejoor7
Volgen

Mete Joor
@metejoor285
Volgen

metejoor
@metejoor4
Volgen

Valse profielen

vrt nws

Hoofdpunten Regio Kijk Luister Meest recent Zoek

AFP or licensors

"Eveline" lokte veel meer mannen dan enkel BV's: "Eerst gesprek over koetjes en kalfjes, al snel wou hij naaktfoto's"

De 27-jarige Gentenaar die verdacht wordt van de verspreiding van naakt- en seksvideo's van drie bekende Vlamingen, was niet aan z'n proefstuk toe. Via valse profielen op sociale media benaderde de verdachte in het verleden al verschillende andere mannen, zowel homo's als hetero's, om van hen naaktbeelden te verzamelen. Sommigen trokken zelfs naar de politie. VRT NWS sprak met enkele mannen die door hem zijn benaderd. "Maar er zijn er meer. Veel meer."

Valse profielen – Preventietips

- Preventietips
  - **Aanvaard niet zomaar alle vriendschapsverzoeken**
  - **Controleer het profiel** van je ‘vriend’
    - Is het profiel ‘*te mooi om waar te zijn*’?
    - Vind je de foto’s ook nog ergens anders?
  - Wees alert voor **zielige verhalen**
    - Inspelen op **emotie** werkt!
    - Geen hulp van familie of vrienden?
  - **Deel niet alles**
    - Geef geen persoonlijke informatie aan een ‘vreemde’ die je nooit hebt ontmoet!
  - **<u>Geef nooit geld</u>** aan iemand die je kent via internet

Identiteitsfraude

- Misbruik van je **identiteitskaart**
  - Kopie voor- en achterkant kaart
  - **Afsluiten contracten/abonnementen**

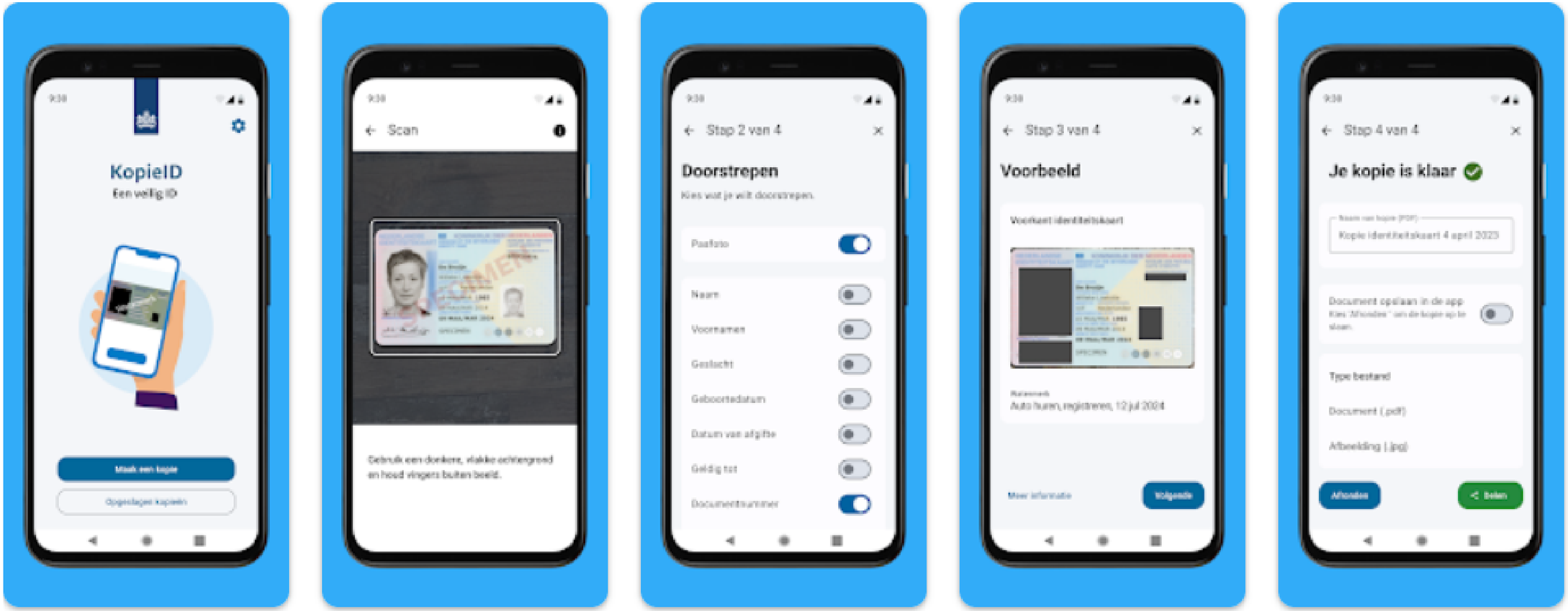
- Hoe word je in de val gelokt
  - Phishing
  - Valse vacatures
  - Tweedehands verkoopwebsites

Expert waarschuwt nadat burgemeester nieuwe identiteitskaart toont: “Dit kan jaren miserie opleveren. Wie je identiteitskaart heeft, heeft alles”

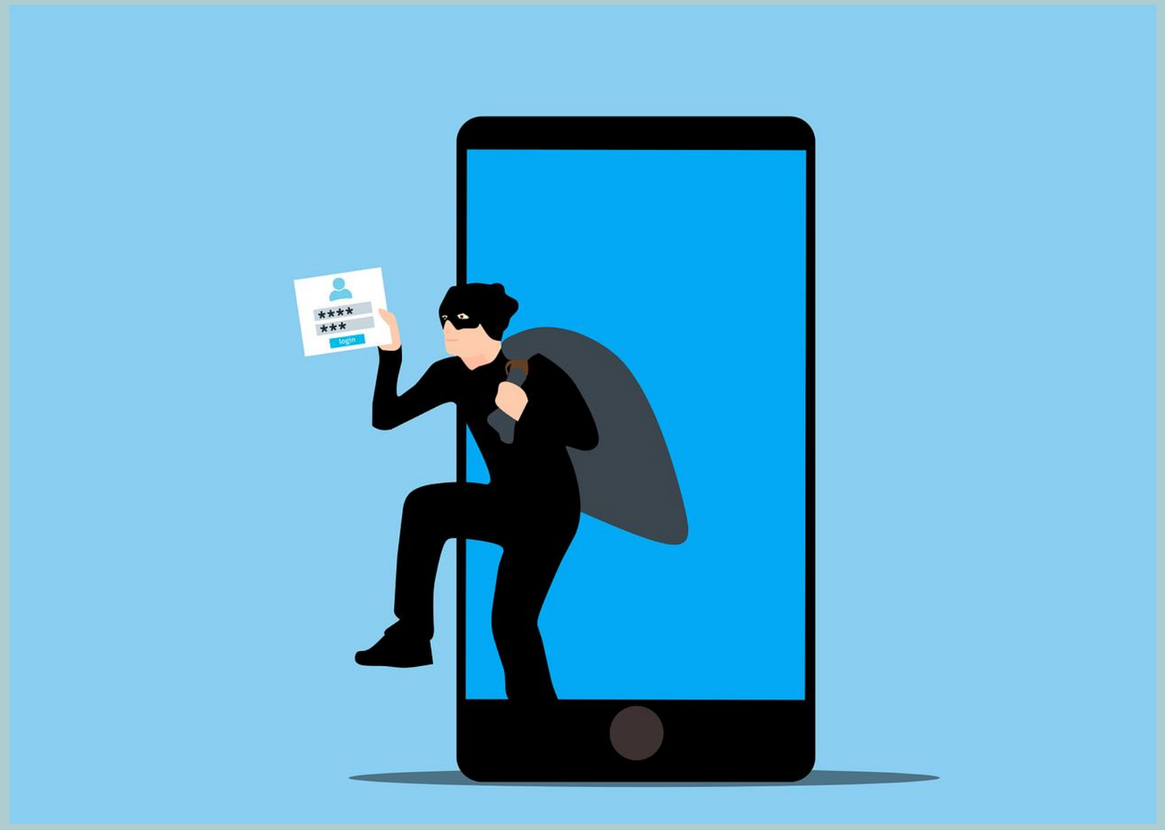
Identiteitsfraude - Preventietips

- Geef nooit je identiteitsgegevens zomaar in op websites
  - Enkel op officiële websites (overheid, bank, ziekenhuis, …)
  - Maak gebruik van **itsme** waar mogelijk!
- Stuur **nooit foto's van je identiteitskaart**
- Indien kopie toch vereist
  - Maak **gegevens onzichtbaar**
  - Zet op de kopie waarvoor deze dient
- Laat je identiteitskaart nooit ergens achter

KopieID - app

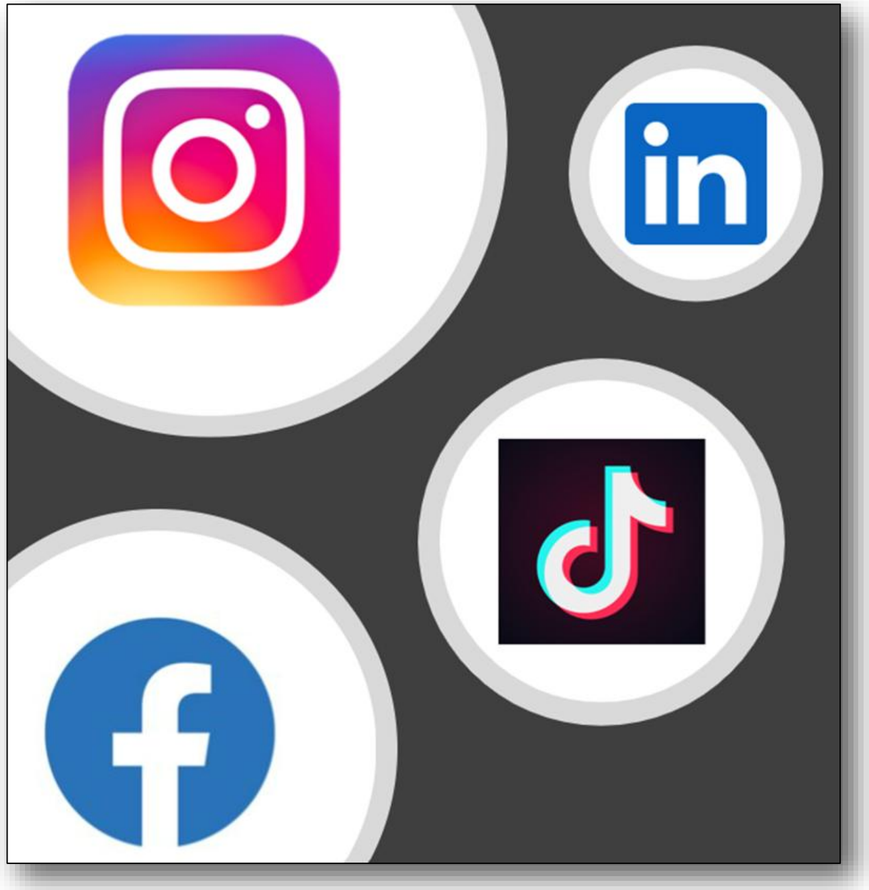

KopieID
Een veilig ID
Maak een kopie
Opgeslagen kopieën
Scan
Gebruik een donkere, vlakke achtergrond en houd vingers buiten beeld.
Stap 2 van 4
Doorstrepen
Kies wat je wilt doorstrepen.
Pasfoto
Naam
Voornamen
Geslacht
Geboortedatum
Datum van afgifte
Geldig tot
Documentnummer
Stap 3 van 4
Voorbeeld
Voorkant identiteitskaart
Auto huren, registreren, 12 jul 2024
Meer informatie
Volgende
Stap 4 van 4
Je kopie is klaar
Kopie identiteitskaart 4 april 2023
Document opslaan in de app
Type bestand
Document (.pdf)
Afbeelding (.jpg)
Afronden
Delen

Social Media hacking



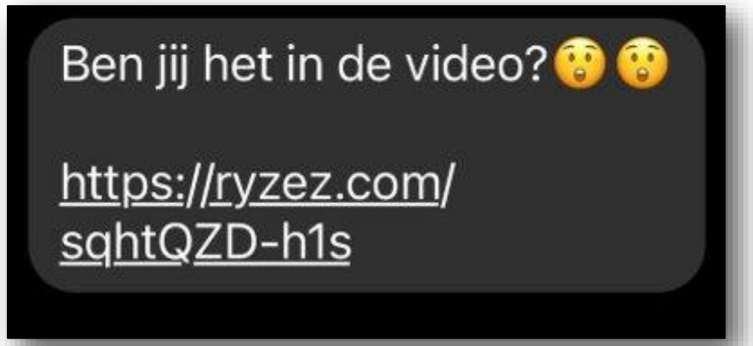
Social Media hacking

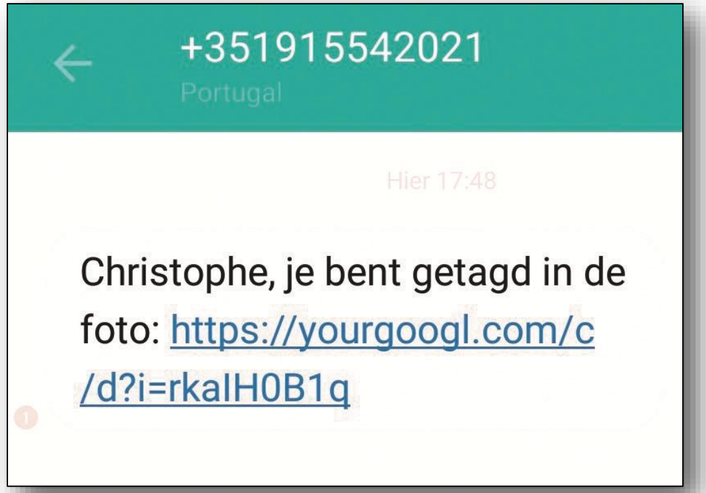
- Doel
  - Toegang krijgen tot **je account**
    - Beveiliging aanpassen (jou buitensluiten)
    - Berichten plaatsen in jouw naam
    - Reviews plaatsen in jouw naam
  - Toegang tot **je gegevens**
    - Persoonlijke informatie
    - Vriendenlijst
    - Phishing/scamming



Social Media hacking

- Hoe
  - Phishing => ***clickbait*** met een link!
    - Inspelen op je **emotie**
      - *“Ben jij het in deze video?”*
      - *“Wat heb ik nu over jou gevonden?”*
    - Je wordt getagd
      - Vb artikel om goedkoop schoenen te kopen
    - Een BV heeft je een vriendschapsverzoek gestuurd
  - Via de link proberen ze je logingegevens te stelen





Social Media hacking

- **Hulpvraagfraude**
  - Vriend of familie **in nood**
  - Dringend **geld nodig**
  - Via social media, e-mail of SMS
    - Gehackte accounts
    - Gekopieerde accounts
    - Nagemaakte accounts
    - …

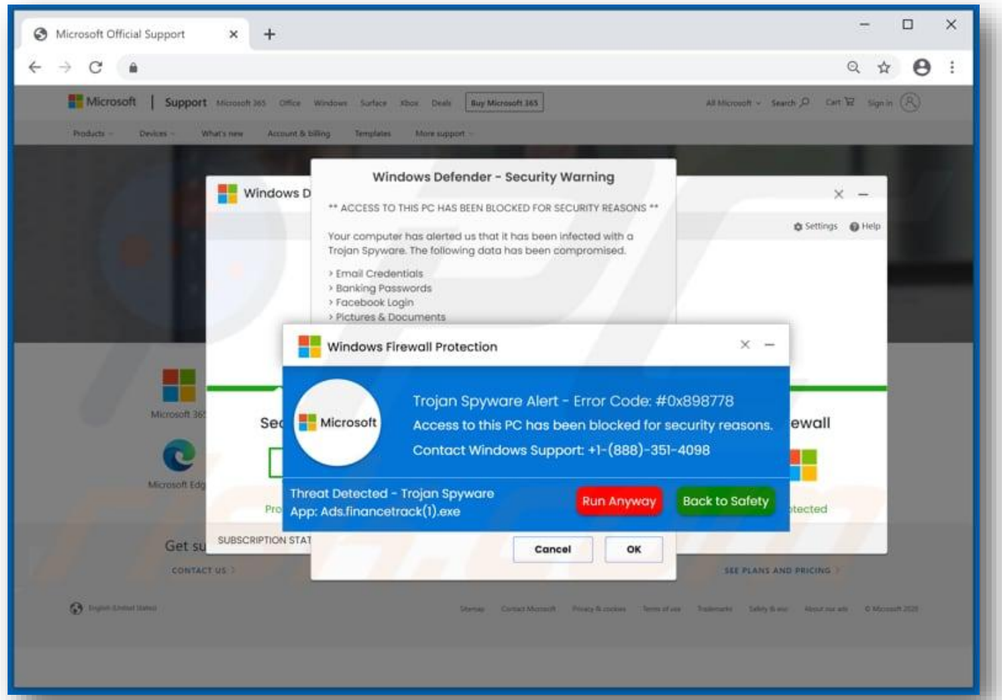
Social Media hacking

- Preventietips
  - **Twijfel** je over een bericht van een vriend?
    - Contacteer je vriend via een **ander medium**
      - Telefoon, SMS, fysiek, …
  - **Whatsapp** hulpvraag zoon/dochter
    - Bel eens naar het nieuwe nummer => er zal niet opgenomen worden
    - Bel eens naar het oude nummer => er zal waarschijnlijk wel opgenomen worden
  - Is je account **gehackt**?
    - Waarschuw je contactpersonen
      - Via een vriend, nieuw profiel, ander platform, …
    - Waarschuw het Social Media platform
      - Misschien kan je je account nog redden

Scamming

Helpdesk fraude

- Contact door Microsoft/Apple/bank/…
  - Er is een problem met je **PC of Mac**!?
    - Je wordt zelf gebeld
    - Je krijgt een pop-up met een waarschuwing
      - Er staat een nummer dat je kan bellen
  - Er is een probleem met je **bankrekening**
    - De helpdesk van de bank lost het wel op
  - Er wordt gevraagd om **software te installeren**
    - Je toestel wordt **overgenomen vanop afstand**
      - Installatie AnyDesk, TeamViewer, …
    - Kan uren duren



Bron: pcrisk.nl

Ga je hierop in, dan heeft de hacker volledige controle over je toestel!

Helpdesk fraude

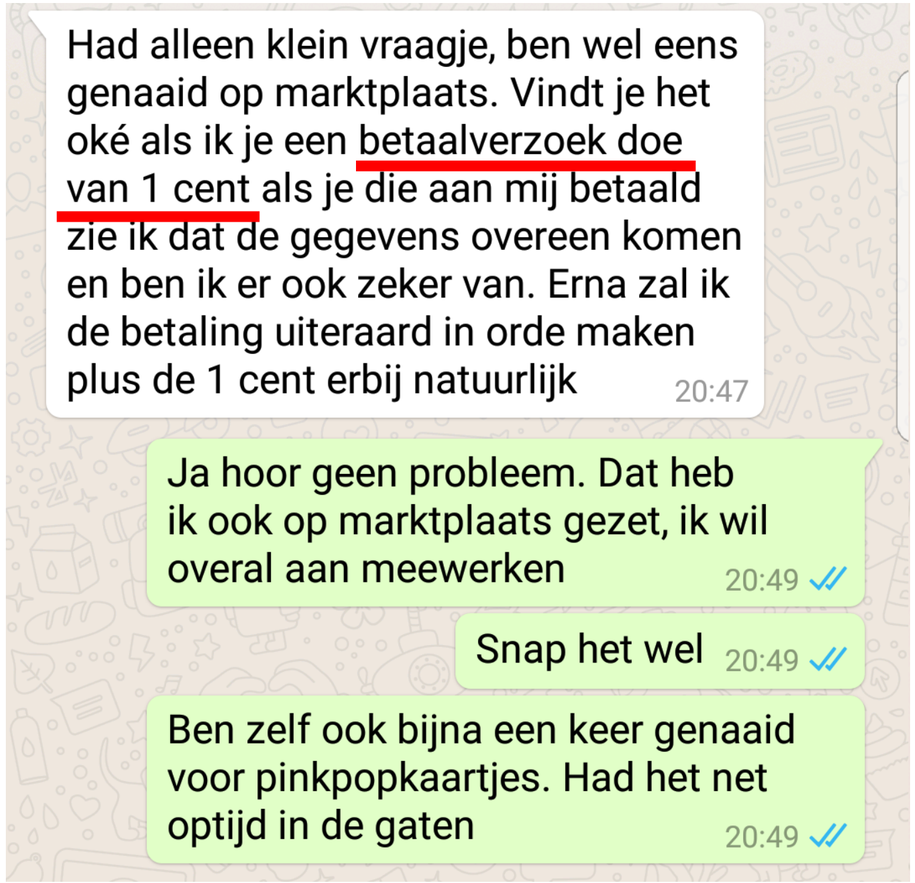
- Preventietips
  - Microsoft of Apple zal je nooit zelf bellen!
  - Word je gebeld door je bank, **bel dan zelf terug**!
  - **Installeer nooit software** op aanraden van een telefonische helpdesk
  - Laat je scherm nooit overnemen vanop afstand
    - Ze krijgen volledige controle over je toestel
    - Ze kunnen opgeslagen wachtwoorden uitlezen
    - Ze kunnen je zelf buitensluiten uit je eigen computer
    - Ze kunnen een programma installeren dat alles logt wat je doet op het toestel
  - Heb je **toch toegang gegeven** tot je computer?
    - **Verbreek de internetverbinding**
    - **Laat je toestel nakijken** door een professional

Verkoop scamming

- Oplichting via 2de hands platform
  - Eerste actie: Koper wil je **contacteren buiten het platform** (Whatsapp, …)
    - Bescherming platform valt dan weg!
  - Methode 1: Koper wil eerst **controleren of verkoper te vertrouwen** is
    - Verkoper moet eerst zelf 1 cent betalen
    - Verkoper krijgt een (phishing!) link om te betalen
      - Rekening wordt geplunderd!

Verkoop scamming

- Voorbeeld methode 1: de valse overschrijving



Verkoop scamming

– Methode 2: **een (nep) koeriersdienst** inschakelen (DHL, DPD, …)
  - Koper heeft het veel te druk
  - Koeriersdienst komt pakje afhalen
  - Koeriersdienst zal je betalen
  - Je krijgt een (phishing) link naar de koeriersdienst
    – Je moet een **account aanmaken**
    – Je moet **eerst zelf een overschrijving** doen!

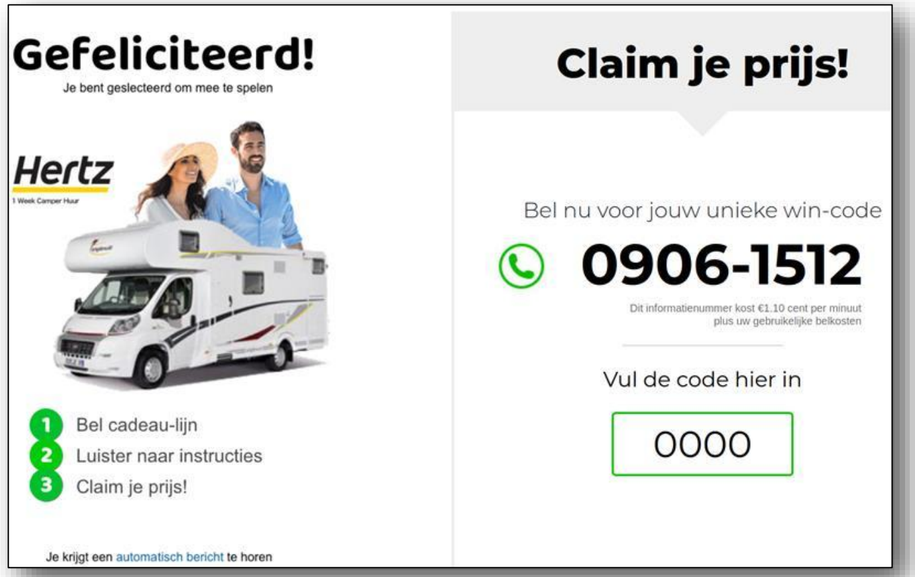
Verkoop scamming

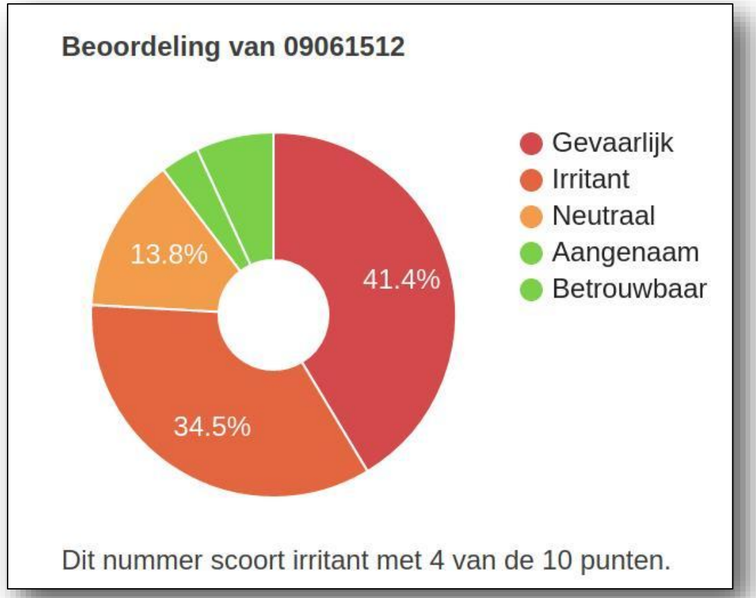
- Preventietips
  - Alle communicatie **via het verkoopsplatform**
    - Schakel niet over naar Whatsapp, …
    - Je bent enkel beschermd binnen het platform
  - Aanvaard **enkel bankoverschrijving of cash**
    - Controleer of je het geld ontvangen hebt
  - **Te mooi om waar te zijn**…?

Getuigenis verkoop Scam

Social Media scamming

- **Wedstrijden** met dure prijzen
  - *“Klik hier om te winnen!”*
    - Vragenlijst invullen (persoonlijke gegevens!)
    - Contactgegevens achterlaten
    - Dure betaalnummers





Social Media scamming

- Dure spullen aangeboden tegen spotprijzen
  - *“Te mooi om waar te zijn?”*
  - Je tekent in op een duur **abonnement**!

Een eerdere versie van het ‘Millennium Falcon’-ruimteschip.

Normaal meer dan 800 euro, nu voor “slechts 2,99 euro”: misleidende LEGO-advertentie doet de ronde op sociale media

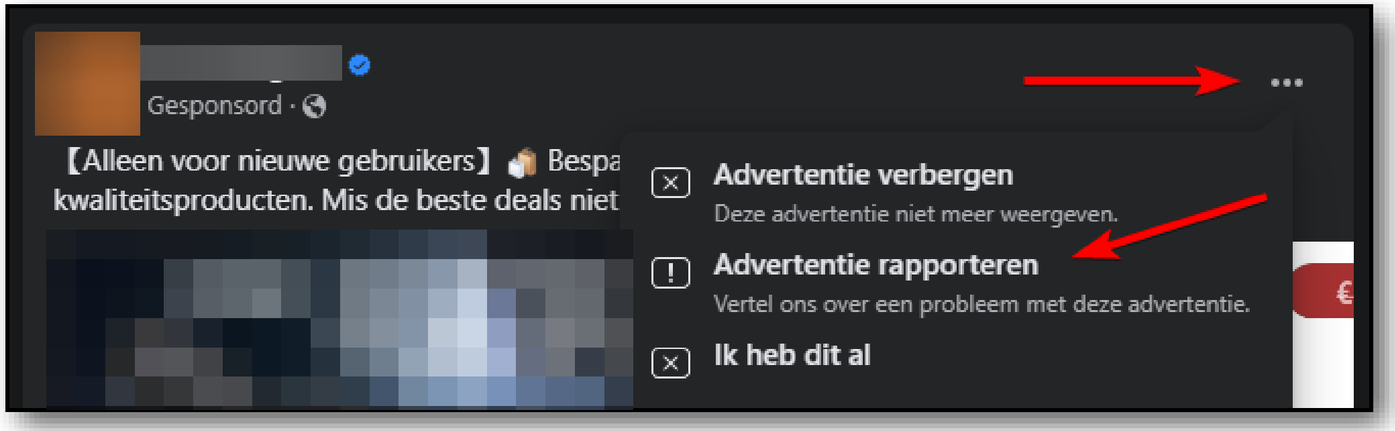
In verschillende LEGO-fangroepen op sociale media doet een post de ronde dat de populaire ‘Millennium Falcon’-set, die normaal meer dan 800 euro kost, nu verkrijgbaar is voor slechts 2,99 euro. De uitverkoop zou deel uitmaken van een bredere campagne rond het ‘Star Wars’-gamma van LEGO. Maar de FOD Economie waarschuwt dat het een abonnementsvalkuil zou zijn. Als je op de link klikt om het pakket te bestellen, eindig je met een duur abonnement.

Social Media scamming

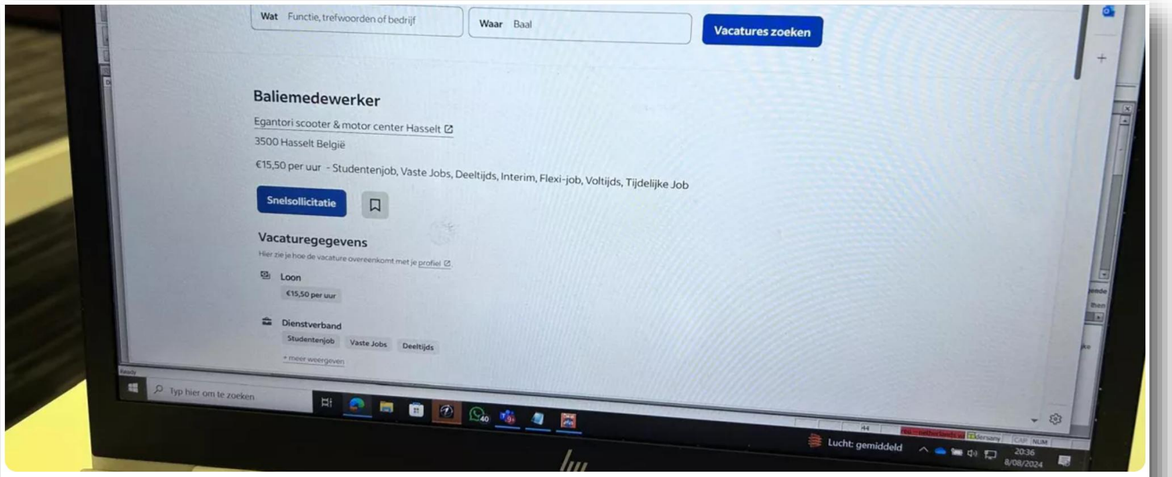
- **Beleggingsfraude**
  - Hoe word je gelokt?
    - Advertentie op Social Media
      - Met bekende personen
    - Telefonisch contact
    - Snel/veel geld verdienen!
  - Werkwijze
    - Eerst klein bedrag inleggen
    - Valse App/Website toont winst!
    - Grotere bedragen inleggen
    - Contact wordt verbroken…
  - Vaak 2 keer slachtoffer => criminelen ‘helpen’ je geld recupereren

Social Media scamming

- Preventietips
  - Als het **te mooi is om waar te zijn**, dan is het dat ook! Trap niet in de val!
  - Veel **persoonlijke informatie** vragen = verdacht
    - Let op met het doorgeven van bankrekeningnummers, telefoonnummers, …
  - **Lees steeds de kleine lettertjes**!
    - Krijg je wel wat beloofd wordt?
  - **Rapporteer** valse berichten op het platform!



Job scamming



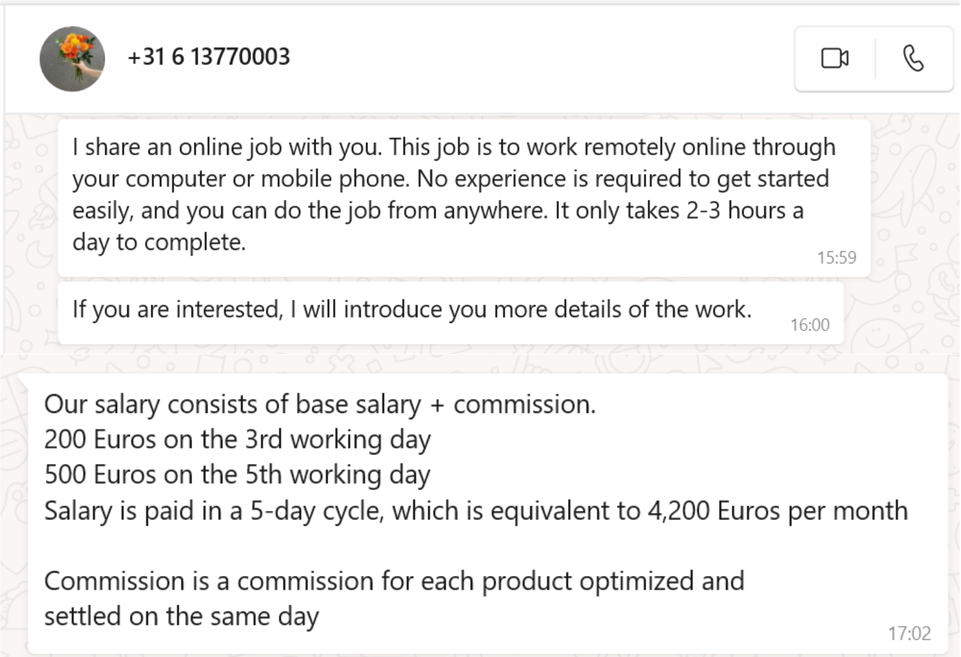
De vacature ziet er echt uit, maar ze is dus vals.
Foto: VRT NWS

Politie waarschuwt voor valse vacature van Hasselts bedrijf op website Indeed: "Het ziet er heel echt uit"

De politie in Hasselt waarschuwt voor een valse vacature van het bedrijf Scooter Center Hasselt op de website Indeed. Oplichters zouden een vacature voor baliemedewerker op de website hebben gezet om bij mogelijke kandidaten geld of identiteitsgegevens te ontfutselen. "Als je moet betalen bij een vacature, kan je ervan uitgaan dat het nep is", zegt Dorien Baens van Politiezone Regio Hoofdstad.

Wat is thuiswerk-oplichting?

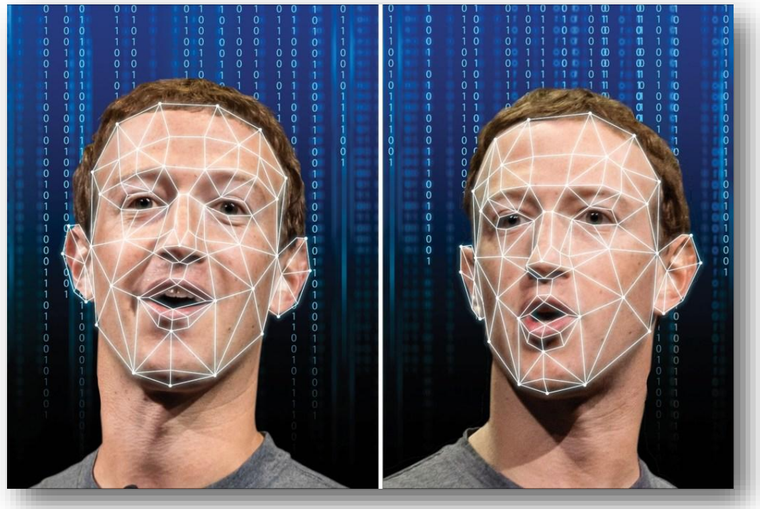
Thuiswerk-oplichting is een vorm van oplichting waarbij werkzoekenden worden gelokt die alleen op zoek zijn naar een baan die ze op afstand kunnen doen. Meestal bieden deze vacatures geweldige salarissen en compensatie om werkzoekenden te verleiden en ze er gemakkelijk in trappen. Het belangrijkste doel van thuiswerk-oplichting is om de persoonlijk identificeerbare gegevens (PII) van een werkzoekende te stelen of te zorgen dat de werkzoekende geld overmaakt naar de oplichter. Als een oplichter erin slaagt om een werkzoekende te misleiden, is de werkzoekende kwetsbaar voor financieel verlies en wordt hun identiteit gestolen.



Artificiële Intelligentie

- Krachtige tools
  - **Afbeeldingen** genereren
  - **Video's** genereren
    - Deepfake => persoon nabootsen
  - **Audio** genereren
    - Klonen van stemmen
      - Slechts enkele seconden nodig

- **Moeilijk te detecteren**
  - Wat kan je nog vertrouwen?



Artificiële Intelligentie

- AI is in opmars bij oplichters!
  - Stem van zoon/dochter **klonen**
  - **Blijf kalm** bij verdachte situaties
  - **Contacteer persoon zelf**!

- Preventietips
  - Let op wat je publiek deelt!
  - **Scherm je Sociale Media profielen af!**

Marion werd opgelicht met stem van zoon: 'Hij liep net op tijd de woonkamer binnen'

Door Karlijn Houterman
23 mei 2023 13:56 • Aangepast 23 mei 2023 17:43

rtl nieuws

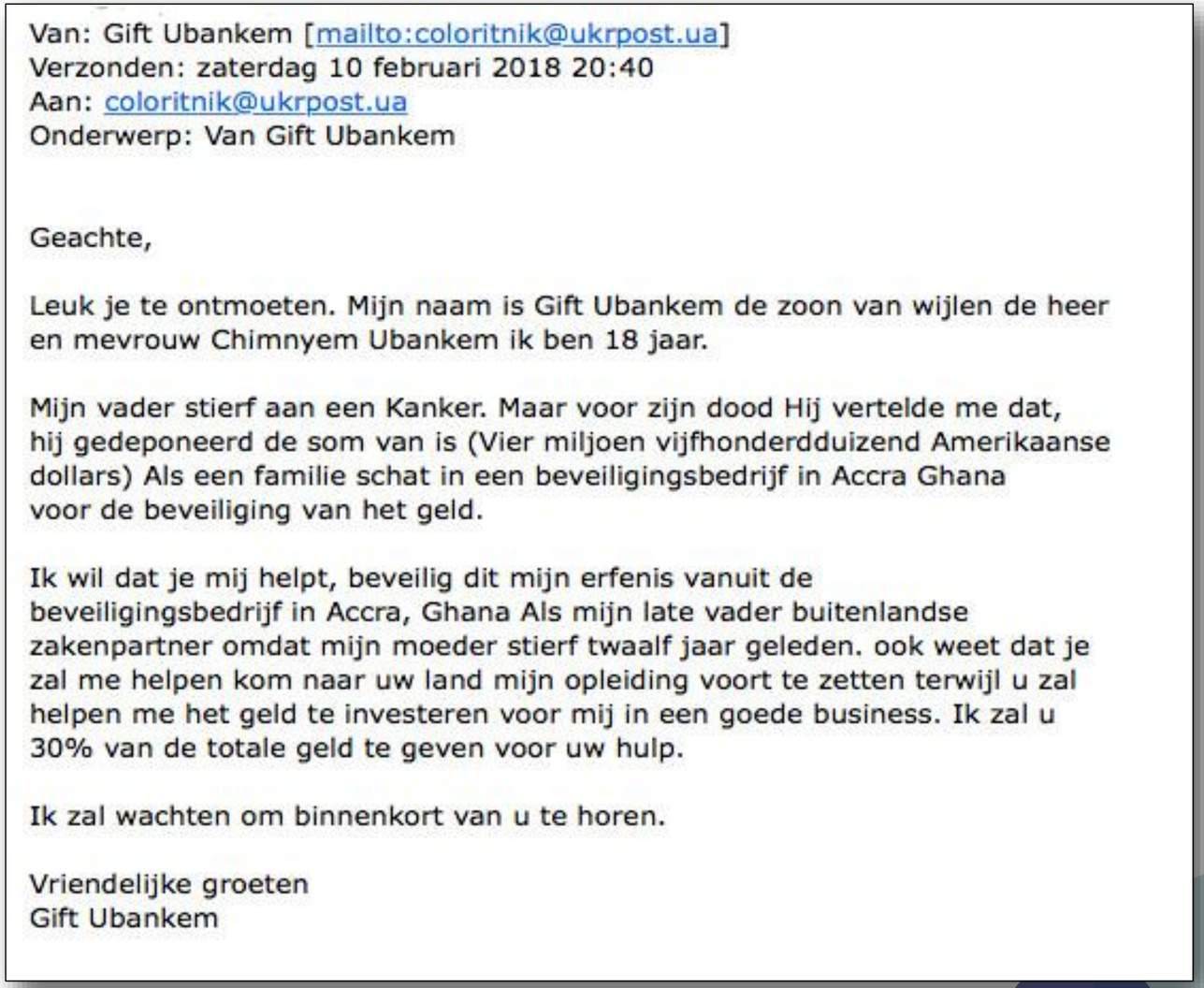
Nieuwsblad

Moeder hoort "ontvoerde dochter" om hulp schreeuwen aan telefoon en slaat in paniek, tot haar man de leugen kan doorprikken

Jennifer DeStefano. — © Facebook

Erfenisfraude

- Recht op erfenis in buitenland
  - Vaak gemeld door advocaat of bankier
  - Ze gebruiken realistisch ogende certificaten
- Maar … eerst een voorschot betalen!
- Soms ook per briefpost!



Van: Gift Ubankem [mailto:coloritnik@ukrpost.ua]
Verzonden: zaterdag 10 februari 2018 20:40
Aan: coloritnik@ukrpost.ua
Onderwerp: Van Gift Ubankem

Geachte,

Leuk je te ontmoeten. Mijn naam is Gift Ubankem de zoon van wijlen de heer en mevrouw Chimnyem Ubankem ik ben 18 jaar.

Mijn vader stierf aan een Kanker. Maar voor zijn dood Hij vertelde me dat, hij gedeponeerd de som van is (Vier miljoen vijfhonderdduizend Amerikaanse dollars) Als een familie schat in een beveiligingsbedrijf in Accra Ghana voor de beveiliging van het geld.

Ik wil dat je mij helpt, beveilig dit mijn erfenis vanuit de beveiligingsbedrijf in Accra, Ghana Als mijn late vader buitenlandse zakenpartner omdat mijn moeder stierf twaalf jaar geleden. ook weet dat je zal me helpen kom naar uw land mijn opleiding voort te zetten terwijl u zal helpen me het geld te investeren voor mij in een goede business. Ik zal u 30% van de totale geld te geven voor uw hulp.

Ik zal wachten om binnenkort van u te horen.

Vriendelijke groeten
Gift Ubankem

Sextortion

----Oorspronkelijk bericht-----
Van:
Verzonden: woensdag 6 februari 2019 19:48
Aan:
Onderwerp: Zorg ervoor dit bericht te lezen! Uw persoonlijke gegevens worden bedreigd!

Hallo!

Zoals je misschien hebt gemerkt, heb ik je een e-mail van je account gestuurd.
Dit betekent dat ik volledige toegang tot uw account heb.

Ik hou je nu al een paar maanden in de gaten.
Het is een feit dat je bent geinfecteerd met malware via een site voor volwassenen die je hebt bezocht.

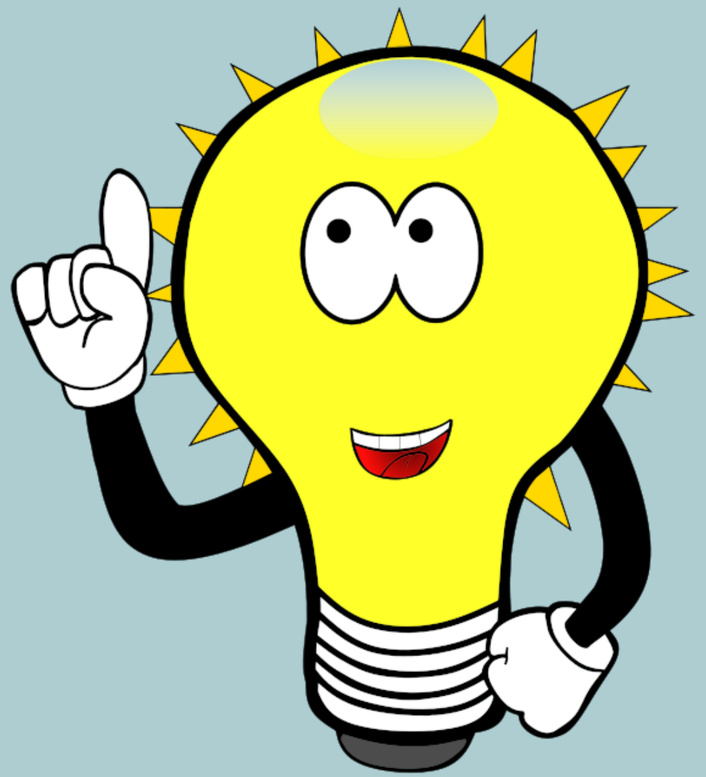
Als je hier niet bekend mee bent, zal ik het uitleggen.
Trojan Virus geeft me volledige toegang tot en controle over een computer of ander apparaat.
Dit betekent dat ik alles op je scherm kan zien, de camera en microfoon kan inschakelen, maar je verdenkt het niet.

Ik heb ook toegang tot al uw contacten en al uw correspondentie.

Waarom heeft uw antivirus geen malware gedetecteerd?
Antwoord: Mijn malware gebruikt de driver, ik update zijn signatures elke 4 uur zodat uw antivirus stil is.

Ik heb een video gemaakt die laat zien hoe jij bevredigt jezelf stelt in de linkerhelft van het scherm (je begrijpt zeker wat ik bedoel ...), en in de rechterhelft zie je de video die je hebt bekeken.
Met een muisklik kan ik deze video verzenden naar al uw e-mails en contacten op sociale netwerken.
Ik kan ook de toegang posten tot al uw e-mailcorrespondentie en messengers die u gebruikt.

Preventietips



10 preventietips

1. Gebruik een sterk wachtwoord!
2. Kies voor tweestapsverificatie (2FA, MFA)
3. Installeer steeds de officiële software-updates
4. Installeer een antivirus programma op al je toestellen
5. Open geen verdachte bestanden of berichten
6. Installeer enkel Apps uit de officiële applicatiewinkels (App Store)
7. Controleer het adres van websites op onregelmatigheden
8. Verbreek het contact met ongevraagde helpdeskmedewerkers
9. Stel je privacyinstellingen zo hoog mogelijk in op sociale media
10. Maak verbinding met vertrouwde wifinetwerken

Wat als het toch fout gaat?

- Weet dat je **niet het enige slachtoffer** bent! **Voel je niet beschaamd!**
- **Doe zo snel mogelijk aangifte bij de politie**
  - Verzamel zo veel mogelijk **bewijsmateriaal** + **datum/tijdstip** van de feiten
- **Verander je wachtwoorden** indien nodig

- Zijn ze aan je **bankrekening** geraakt?
  - Laat je **kaarten blokkeren** via Cardstop
  - Laat je **financiële Apps blokkeren** bij de bank
    - Bank is 24/7 bereikbaar voor melden fraude!
    - Noteer het nummer van je bank voor noodgevallen

https://www.cardstop.be/nl/home/ik-wil-blokkeren/Blokkeer-via-uitgever.html

Een waarheid als een koe…

Nuttige website

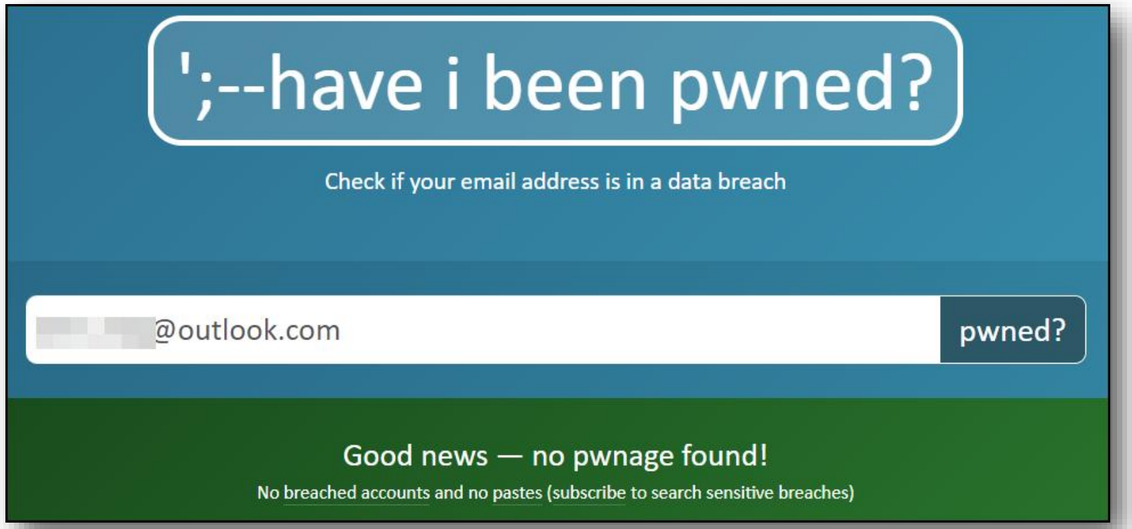
https://safeonweb.be

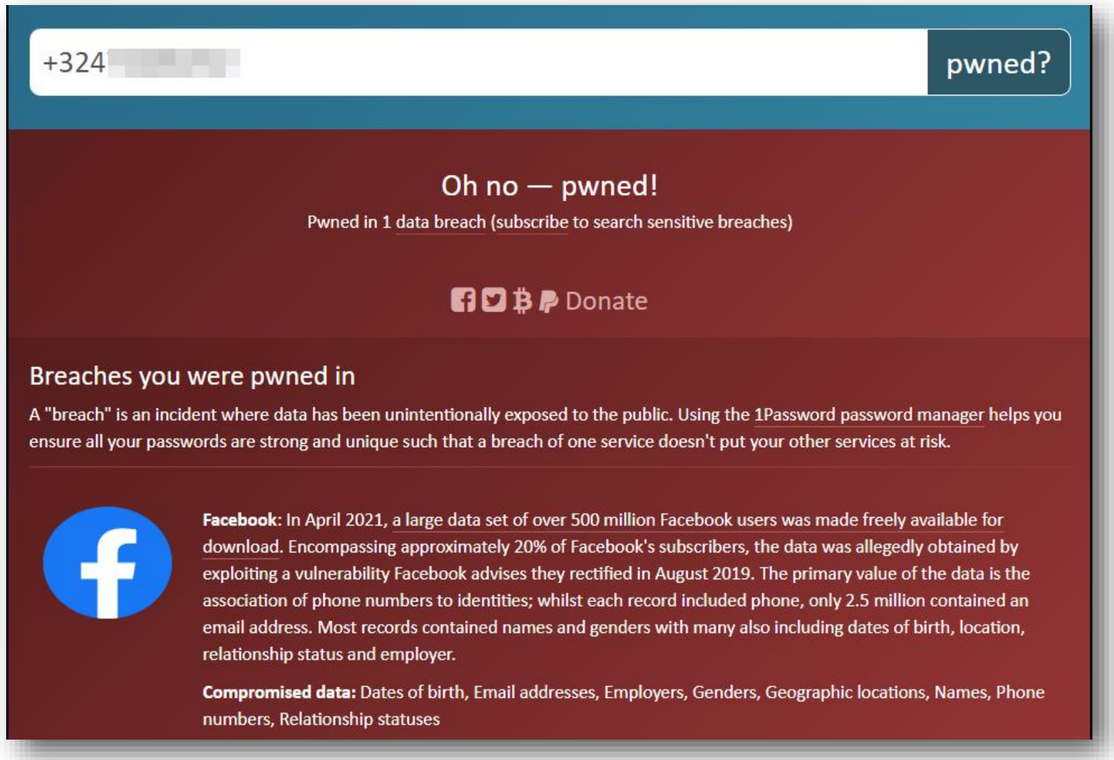
- Kijk voor tips, actuele dreigingen, en veel meer op Safeonweb!

Nuttige website

https://haveibeenpwned.com/

- Welke gegevens zijn van jou ooit gelekt?
  - Zoeken op e-mail adres, telefoonnummer, wachtwoord





Bedankt!

En denk erom: als het te mooi is om waar te zijn...!

www.pzglm.be

Veiligheid, een gedeelde zorg

Politie

Geel - Laakdal - Meerhout