Infoavond cybercriminaliteit (20/02/24)

Commissaris Heytens Lies
Recherche PZ Regio Tielt

Cijfers

PZ Regio Tielt

Financieel nadeel in PZ Regio Tielt:

- 2021: 1.054.499,76 euro – 332 feiten
- 2022: 1.276.565,69 euro – 315 feiten
- 2023: 1.553.120 euro – 281 feiten

Dark number? Onderschatting van de realiteit.

TIP! Aangifte doen is belangrijk!

HLN TECH ABONNEREN

verdienen. © Kenneth Dee

HLN ONDERZOEK. "Ze zijn erin geslaagd niet enkel mijn eigen portefeuille te plunderen": WhatsApp-fraudeurs stelen bij Eva 110.000 euro en wij proberen ze te pakken

Een maand, zo lang hebben cybercriminelen nodig om Eva* een pak geld te kosten. Het begint met een bericht over een jobaanbieding, het eindigt met lege bankrekeningen en heel wat miserie. Dit is het verhaal van een slachtoffer van de WhatsApp-jobfraude, waarvoor Eva via haar getuigenis iedereen wil waarschuwen. Maar we sporen ook de daders op, tot in de Verenigde Arabische Emiraten.

Kenneth Dee 16-02-24, 16:10

Nieuwsblad · 3d

De beelden zijn nep, de impact immens: nieuwe vorm van seksueel geweld in opmars

Deepnudes ofte valse naaktbeelden gemaakt met AI. Ruim 12 procent van de ...

Na het **datalek bij Limburg.net** duikt in **politiezone Carma** een nieuwe vorm van **phishing** op. Mensen worden opgebeld met de melding dat ze het slachtoffer zijn geworden van phishing en er al geld van de rekening is gehaald. Nadat ze de nodige informatie hebben gekregen, roven ze de rekening leeg. De oplichters doen zich voor als medewerkers van **Stop**. Ze bellen hun slachtoffers om te melden dat de

Inhoud

PZ Regio Tielt

- **Wat niet?**
  - Cursus Cybercrime
  - Hackingtools, onderzoekstechnieken
- **Wat wel?**
  - Soorten oplichting / cybercrime (selectie!)
  - Gevaren
  - Voorbeelden
  - Tips om te voorkomen dat u slachtoffer wordt
  - Bewustmaking

Het internet

PZ Regio Tielt

Positief verhaal!

- Krant lezen
- Opzoekingen doen
- Bankieren
- Aankopen en verkopen van goederen
- E-mails, sms-en, chat…
- Whatsapp
- Skypen, facetime, videobellen…
- Sociale media (Facebook, Twitter, …)
- …

Maar…

Begrip

PZ Regio Tielt

- **Cybercrime of cybercriminaliteit** = verzamelnaam voor alle vormen van criminaliteit op of via het internet:

  Hacking, Illegaal downloaden, Cyberpesten, Misbruik van bankkaarten, Aanzetten tot terrorisme, Witwassen van geld, aanvallen op systemen voor geautomatiseerde gegevensverwerking, het versturen van virussen, oplichting…

- Anonimiteit internet (nulletjes/eentjes; IP-adressen,…)
- **Iedereen** kan SO worden (kwetsbaar, onoplettend, goedgelovig, …)
- **Strafbaar** maar schade herstellen is moeilijk en opsporen verdachten niet eenvoudig en tijdrovend;

Soorten oplichting

PZ Regio Tielt

1. Internetbankieren- mobiel bankieren
2. Sociale media
3. Zoekertjes
4. Te mooi om waar te zijn
5. Phishing
6. Beleggingsfraude

Soorten oplichting

PZ Regio Tielt

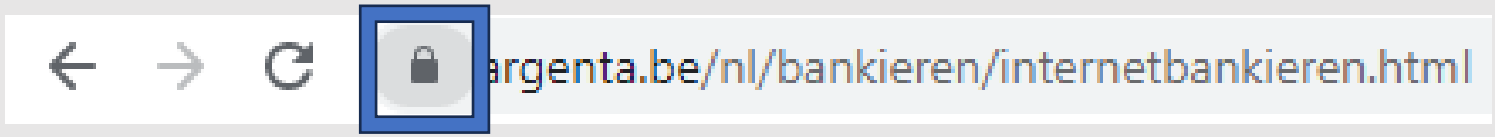
1. **Internetbankieren- mobiel bankieren**
2. Sociale media
3. Zoekertjes
4. Te mooi om waar te zijn
5. Phishing
6. Beleggingsfraude

SOORTEN OPLICHTING / Internetbankieren – mobiel bankieren

Gevaar: Veilige site voor internetbankieren?

1. Officiële website?
   - www.safeonweb.be/tips
     - Het domein is 'safeonweb'
   - www.safeonweb.tips.be/safeonweb
     - Het domein is 'tips' → je wordt naar een andere website geleid!

2, In de adresbalk staat het icoon van een **slotje**. → veilig?



3, http**s://** → veilig?

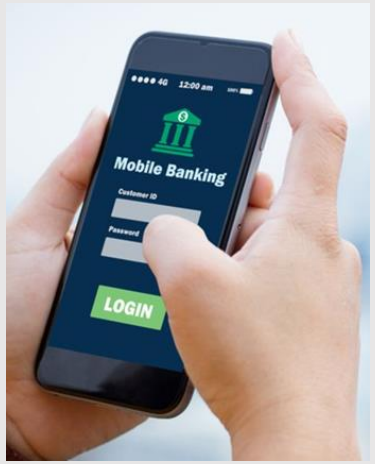
4. Sla de echte website op in je favorieten of typ het adres manueel in

SOORTEN OPLICHTING / Internetbankieren – mobiel bankieren

Beiden zijn even veilig bij correct gebruik!

10 GEBODEN

1. Gebruik officiële apps!
2. Updates!
3. Gebruik beveiligingsinstellingen bank-apps!
4. Beveilig je smartphone!
   - pincode, patroon of biometrische
   - antivirussoftware
5. Géén openbare netwerken!
6. Controleer transacties regelmatig!
7. Alertheid voor phishing!
8. Log uit na gebruik!
9. Gebruik sterke wachtwoorden!
10. Meld verlies of diefstal!



Soorten oplichting

PZ Regio Tielt

1. Internetbankieren
2. **Sociale media**
3. Zoekertjes
4. Te mooi om waar te zijn
5. Phishing
6. Beleggingsfraude

SOORTEN OPLICHTING / Sociale media

Begrip

Whatsapp (meta), Facebook (meta) , X, Instagram, Youtube, LinkedIn,
Google+, Pinterest, Snapchat, Instagram, Tiktok, Youtube, Playstation, games…

Voorbeeld

U krijgt op sociale media een vriendschapsverzoek van een vriend van een vriend. U bent zelf niet echt bevriend met deze persoon. Wat doet u?

- Ik accepteer. Ik weet wie het is, ook al ken ik deze persoon niet echt goed maar het is een goede vriend van mijn vriend dus het kan geen kwaad.

- Ik negeer. Ik vind het niet nodig om met iedereen vrienden te zijn. Ook niet online.

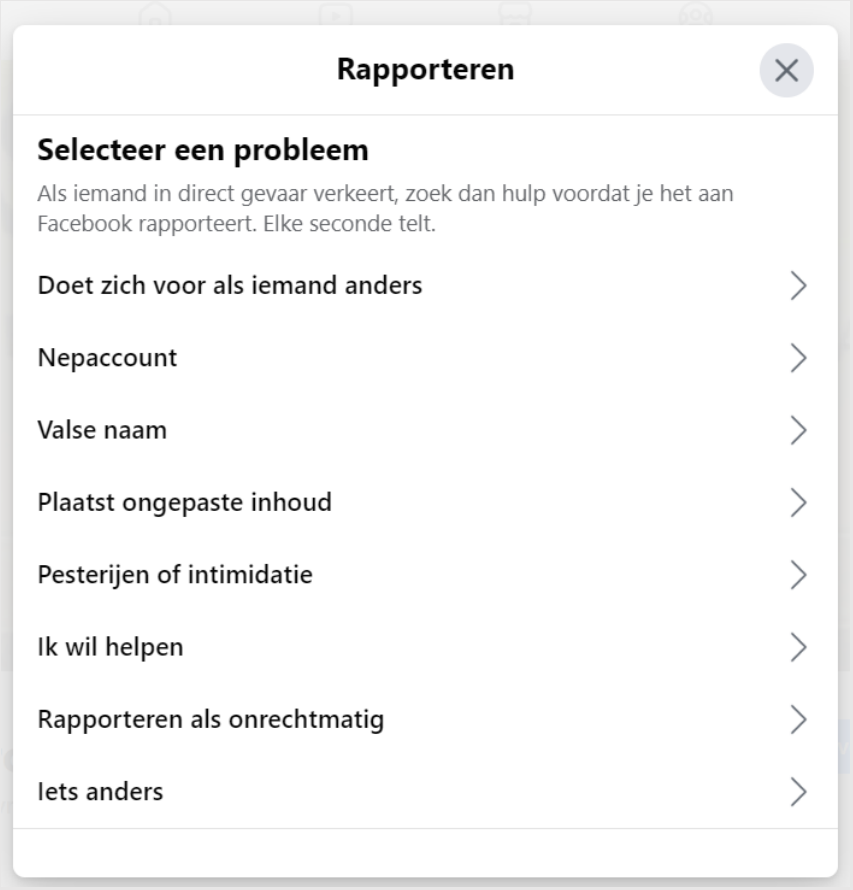
SOORTEN OPLICHTING / Sociale media

Gevaar:

- Vals profiel

SOORTEN OPLICHTING - Sociale media

- WEES WAAKZAAM bij **vriendschapsverzoeken** (mensen die u niet kent, bekende mensen, vrienden waarmee je reeds online bevriend bent…)
- In welke taal wordt u aangesproken en waarover?
- Opletten als ze beginnen over financiële problemen, vragen om geld te mogen lenen.
- Doe zelf wat onderzoek
  - Gemeenschappelijke vrienden?
  - Bekijk zorgvuldig het profiel
  - Kijk goed naar de profielfoto (google lens)
- Rapporteer
- Blokkeer het verzoek



SOORTEN OPLICHTING - Sociale media

Gevaar

- **Vriendschapsfraude:** Iemand die u online hebt ontmoet vraagt plotseling om geld

Voorbeeld

Een zogezegde Amerikaanse legergeneraal is verliefd op het slachtoffer en zegt dat hij na zijn pensioen zijn leven met het slachtoffer wil delen. Momenteel zit hij vast in Afghanistan, en hij vraagt wat geld omdat zijn bankrekening geblokkeerd is. Later vraagt hij grotere sommen, oa om zijn persoonlijke bezittingen naar het slachtoffer te laten overkomen. Kleine bedragen worden uiteindelijk een gigantische som….

SOORTEN OPLICHTING - Sociale media

Werkwijze vriendschapsfraude - waarschuwingssignalen

- Slachtoffer wordt gecontacteerd door de verdachte via spam-mail, datingsites, chatbox, sociale media, Whatsapp,...

- Verdachte bouwt meestal een emotionele band op met het slachtoffer via een vals profiel;
- Verdachte maakt gebruik van de gevoelens van het slachtoffer om deze geld afhandig te maken;
- Er is altijd een obstakel om elkaar niet te ontmoeten, en deze kunnen enkel opgelost worden door het overmaken van geld;
- De feiten blijven zich gedurende lange tijd herhalen zodat het slachtoffer uiteindelijk duizenden euro's kwijt is.

SOORTEN OPLICHTING - Sociale media

Bescherm uzelf tegen vriendschapsfraude

- Ga de echtheid van het profiel na
- Vertrouw niet zomaar iedereen
- Geef geen persoonlijke informatie
- Wees op je hoede voor 'zielige' verhalen
- Stort geen geld
- Melden bij de instantie zelf (Facebook,…)
- Blokkeren van het nummer/profiel

SOORTEN OPLICHTING - Sociale media

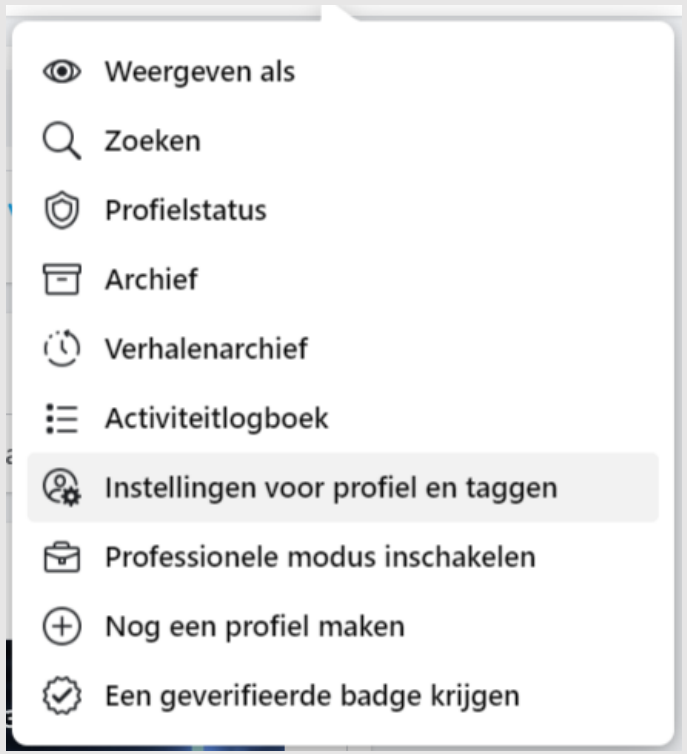
Hoe komen oplichters aan mijn persoonsgegevens?

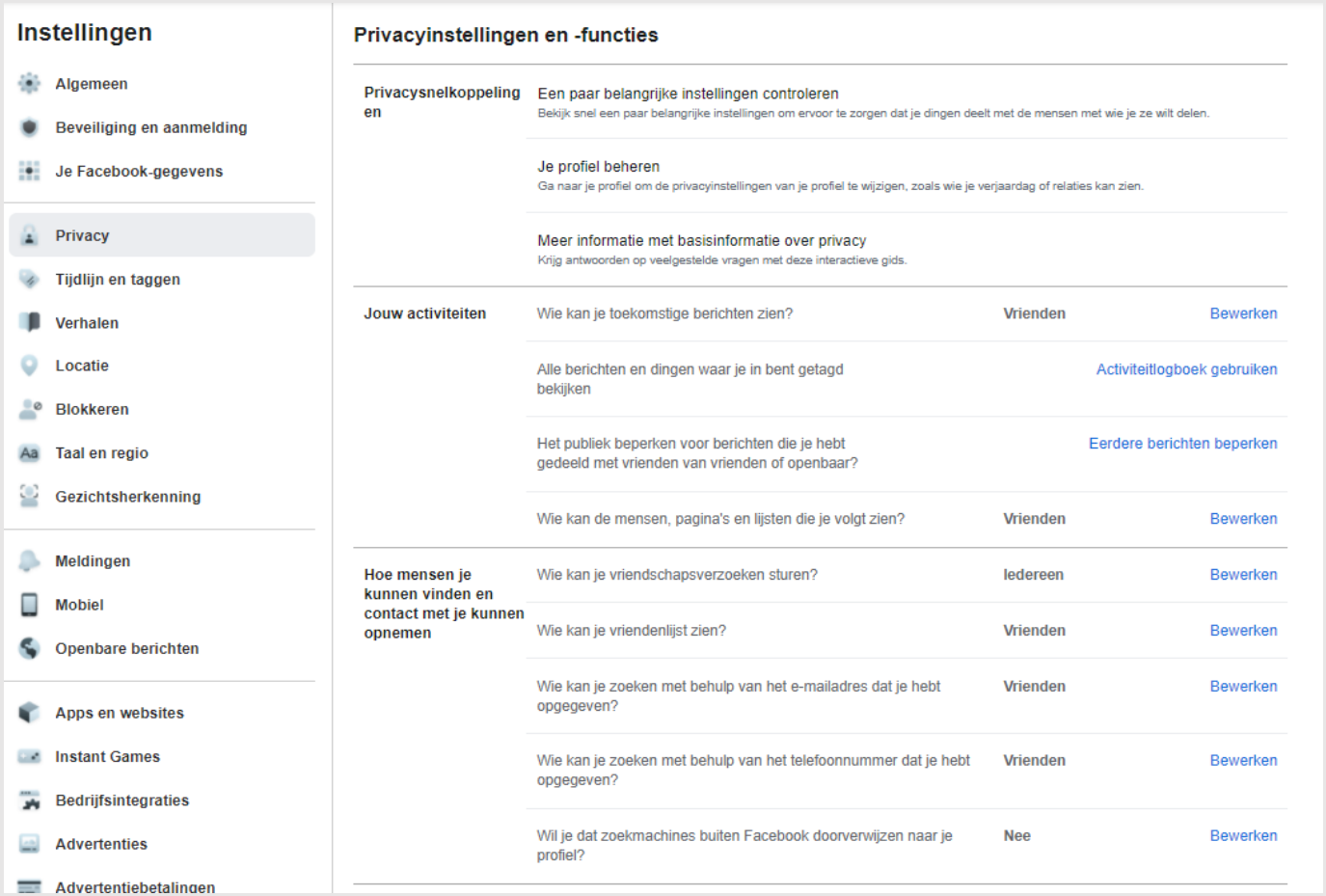
- Criminelen gebruiken gegevens die je zelf (per ongeluk) verspreidt
    - → privacy-instellingen TIP!
    - → cookies TIP!
    - → sociale media, dating sites (Tinder),... TIP!
- Criminelen misleiden slachtoffers om gegevens te delen
    - → phishing, oplichting
- Criminelen stelen (digitale) gegevens
    - → datalekken op websites, hacking (belang van goed wachtwoordbeheer) TIP!

SOORTEN OPLICHTING - Sociale media

Privacy - instellingen

- Op **alle** sociale media kan je je privacy-instellingen wijzigen.





SOORTEN OPLICHTING - Sociale media

Werkwijze

Het enige wat een cyberaanvaller hoeft te doen is een website die je gebruikt te **hacken**, alle wachtwoorden te stelen, inclusief die van u, en vervolgens uw wachtwoord te gebruiken om in te loggen op al uw andere accounts.

Wachtwoord:

- Kies sterk wachtwoord voor jouw 'digitale burcht'

  Wachtwoord met 10 kleine letters → 3u en 40 min
  Wachtwoord met 10 karakters van ≠ soorten → 109 eeuwen !!

- Kijk op de websites:

  https://haveibeenpwned.com/ : datalek?
  https://security.org/how-secure-is-my-password/ : sterk wachtwoord?

SOORTEN OPLICHTING - Sociale media

Wachtwoord

- Kies een wachtzin of afkorting: makkelijk te onthouden en veiliger
  - IkwerklieveropeenPCdanopeenMAC
  - Iwlo1PCdo1MAC
- Vorm een lang wachtwoord, tussen de 14 en 20 karakters
- Gebruik hoofd- en kleine letters, cijfers en symbolen
- Om de 3 maanden wachtwoord wijzigen
- Kies een ≠ wachtwoord voor elke account
- Verkies dubbele controle / tweetrapsverificatie
- Bewaar je wachtwoord niet in je browser
- Geef je wachtwoord niet door aan derden
- Wachtwoordmanager (LastPass, 1Password, Dashlane, KeePass, ...)

SOORTEN OPLICHTING - Sociale media

Varianten

- **Nigeriaans oplichting**

- Het slachtoffer wordt gecontacteerd door een onbekende in het buitenland die hulp/geld nodig heeft, maar die belooft achteraf rijkelijk te belonen;
- Of het slachtoffer wordt gecontacteerd inzake een erfenis, valse loterij of een gewonnen prijs;
- De contactname vindt meestal plaats via een chat of e-mail;
- Er wordt een bijzonder lucratief voorstel gedaan maar waarbij er voorafgaandelijk kosten dienen betaald te worden;

- **CEO-fraude**

Een personeelslid van een bedrijf (secretaresse, boekhouder, ...) wordt telefonisch of elektronische weg (mail, whatsapp, ...) benaderd door iemand die zich voordoet als één van de managers of werknemers van het bedrijf met het verzoek een dringende financiële transactie uit te voeren. De betaalgegevens staan in het bericht. Het bericht blijkt naderhand vals te zijn.

SOORTEN OPLICHTING - Sociale media

Varianten

- **Whaling - hulpvraagfraude**

Slachtoffer krijgt een SMS of WhatsApp van iemand die zich voordoet als de zoon/dochter/goede kennis die zogezegd een nieuw nummer heeft omdat de GSM defect is (in het toilet gevallen, zat in de wasmachine ...). Vervolgens vraagt men om voor hem/haar een dringende betaling te doen.

Neem zelf *op een andere manier* contact op met deze persoon
+ in kennis stellen van vermoedelijke hacking van account

- **Emotiefraude**

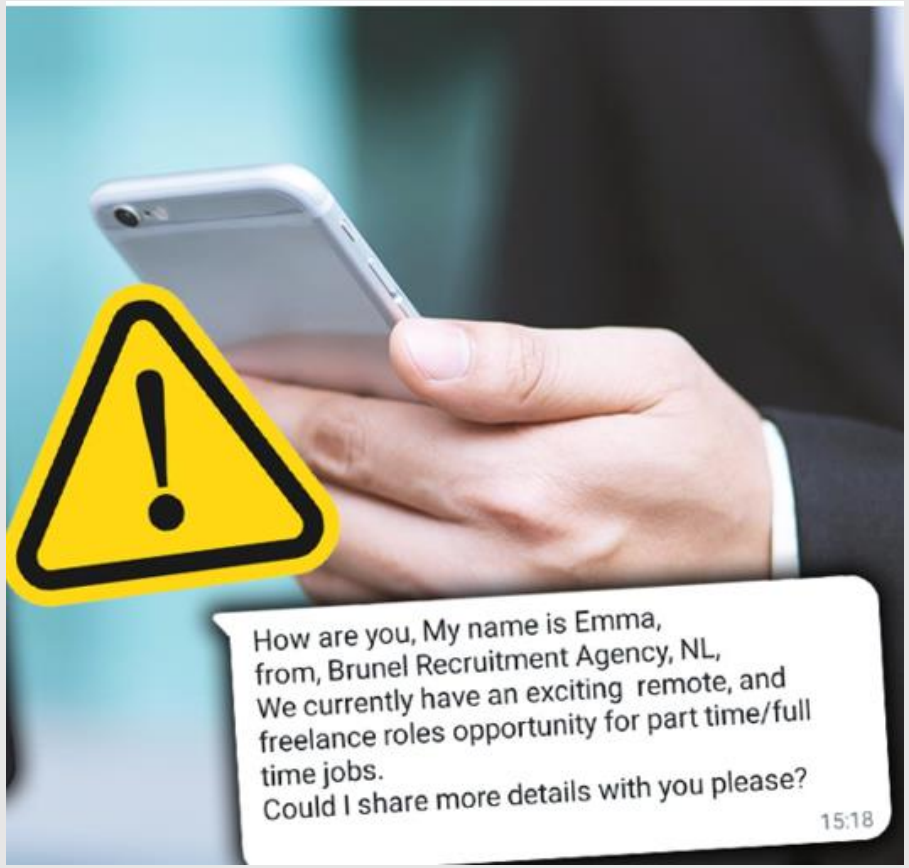
- Valse liefdadigheid
- Voorschotfraude
- ....

SOORTEN OPLICHTING - Sociale media

Varianten

- **Vacaturefraude via WhatsApp**

Ongevraagde benadering door 'recruiter' van een bestaand uitzendbureau met een lucratieve jobaanbieding waarbij tot 950 euro per week verdiend kan worden met een uur werk per dag. Er is vaak geen vooropleiding vereist en je kan meteen beginnen. Ga je in op dit aanbod, dan vragen de oplichters je om kleine bedragen over te maken in bitcoin, voor de administratieve afhandelingen zoals de activatie van het werknemersaccount.



→ Te mooi om waar te zijn…. (eigen hebzucht)
→ Buitenlands telefoonnummer

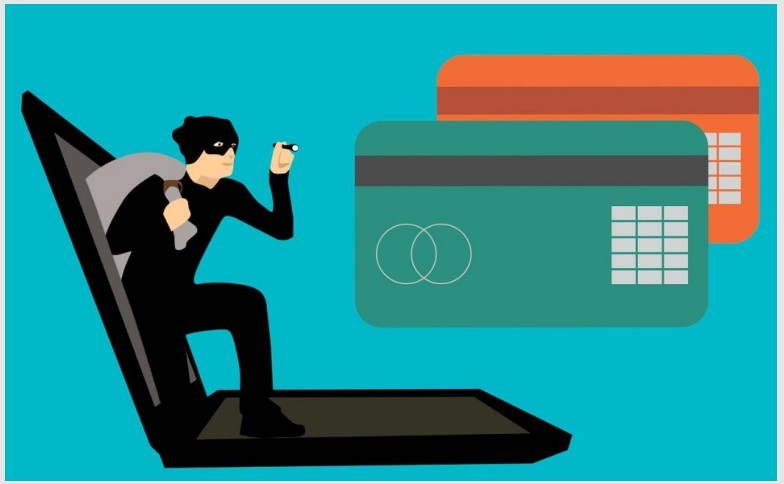
TIP! Nummer blokkeren en melden bij meldpunt.belgie.be en verdacht@safeonweb.be

Soorten oplichting

PZ Regio Tielt

1. Internetbankieren
2. Sociale media
3. **Zoekertjes**
4. Te mooi om waar te zijn
5. Phishing
6. Beleggingsfraude

SOORTEN OPLICHTING - Zoekertjes



Fraude bij online aankoop

De oplichter doet zich voor als verkoper van goederen binnen een valse advertentie op een legitieme veiligsite of via zoekertjessites (2dehands.be, Marketplace, Ebay,…) of via een valse verkoopsite. Na betaling worden de goederen niet geleverd en is de oplichter niet meer te contacteren.

Vaak vraagt de valse verkoper om het afgesproken bedrag over te maken via een geldtransfersysteem van het type Western Union of MoneyGram.

Sommige oplichters gebruiken daarbij een transportfirma of tussenpersoon. In realiteit is de tussenpersoon een medeplichtige van de verkoper.

SOORTEN OPLICHTING - Zoekertjes

Fraude bij online verkoop

Het slachtoffer plaatst zelf een advertentie op een legitieme veilingsite (Autoscout, Immoweb, ...) of sociale mediasite. De oplichter, die zich voordoet als koper, zal zelden discussiëren over de prijs.

De valse koper vraagt aan de verkoper om zelf een bedrag voor te schieten (bijvoorbeeld de vrachtkosten om een wagen naar het buitenland te laten brengen). Dat voorschot moet meestal betaald worden via een geldtransfersysteem van het type Western Union of MoneyGram. Vanzelfsprekend hoort de verkoper daarna niks meer van de valse koper.

Facebook Marketplace

2dehands.be

SOORTEN OPLICHTING - Zoekertjes

Voorbeeld:

Ik heb op www.2dehands.be een gouden ring te koop aangeboden voor 1.500 EUR. Het profiel 'ARWAN' reageert: hij wil de ring kopen. Wij bereiken een akkoord over de verkoopprijs, namelijk 1.400 euro.

De persoon laat weten dat hij op 31/08 de ring komt halen. Hij woont in Brussel doch heeft een vriend in Wingene wonen die hij dan een bezoekje kan brengen. Hij contacteert me de dag zelf wel op welk uur hij zal langskomen. Ik vraag hem het bedrag op mijn rekening over te schrijven. Hij wil dit niet omdat hij zegt dat hij al eens werd opgelicht. Hij zal ter plaatse komen en dan de overschrijving online doen in mijn bijzijn. Ik geef hem alvast mijn rekeningnummer door.

Op 31/08 krijg ik telefoon van het nummer 0031 687431281. Het betreft de man. Een half uur later biedt de man zich aan bij mij. Bij aankomst toont hij mij op zijn smartphone de overschrijving van 1.400 euro. De overschrijving vermeldt mijn naam en mijn rekeningnummer. De man laat weten dat ik dit waarschijnlijk nog niet op mijn rekening kan nagaan gezien dergelijke transacties de beveiliging van de banken dienen te passeren. Ik weet dat dit klopt. Ik overhandig hem de ring. Hij vertrekt.

SOORTEN OPLICHTING - Zoekertjes

Resultaat

De man is heel vriendelijk en vertrekt met de ring. Na enkele dagen stel ik vast dat het geld nog steeds niet overgeschreven is. Ik krijg argwaan. Na een week besef ik te zijn opgelicht. Ik doe aangifte bij de politie.

Alarmbellen

- Het profiel 'ARWAN'?
- Het telefoonnummer?
- Geld staat niet zichtbaar op eigen rekening?
    - Instant overschrijvingen?
    - Vervalsing van getoonde overschrijving?
    - Alternatief: cash of payconic

Noteer de nummerplaat! Trek een foto van het voertuig.

SOORTEN OPLICHTING - Zoekertjes

Tips

- **Persoonlijk contact** wordt aangeraden. Afhandelen met **cash geld** liefst voor de deur of op een drukke publieke plaats. Neem een tweede persoon of getuige mee. Pas op voor last minute veranderingen naar bijvoorbeeld een afgelegen plek.
- **Iets wat te mooi is om waar te zijn, is meestal te mooi om** … (eigen hebzucht!).
- Bod boven vraagprijs?! (oplichter=koper) <-> Abnormaal lage prijs?! (oplichter=verkoper)
- Check het profiel koper/verkoper (sterren, hoe lang reeds profiel, vals profiel?)
- Opgepast met bewijzen van banken
- Indien opsturen: check de verzendkost, geef rek. nr., en **wacht tot geld op uw rekening** staat!
- GEEN Western Union en Moneygram! Deze geldovermakingsbedrijven zijn erkende spelers, MAAR…

SOORTEN OPLICHTING - Zoekertjes

Alarmbellen

- Er wordt gevraagd de verkoop af te handelen buiten de zoekertjessite

  ⚠ **Betaal nooit via een link die een koper of verkoper je doorstuurt.**
  Die links brengen je naar een valse website waar oplichters je bankgegevens opvragen.
  Blijf chatten/handelen op het platform. Blijf baas over je eigen transactie!

- Er wordt gevraagd te betalen via een pakjes- of transportbedrijf

- Er wordt gevraagd een bankverificatie te doen (1-cent truc!)

- Er wordt gevraagd een voorschot te betalen om de verkoop te bevestigen

→ stop de verdere afhandeling van de (ver)koop.

Soorten oplichting

PZ Regio Tielt

1. Internetbankieren
2. Sociale media
3. Zoekertjes
4. **Te mooi om waar te zijn**
5. Phishing

SOORTEN OPLICHTING - Te mooi om waar te zijn

Veilig?

Voorbeeld

Een promotiecampagne voor de verjaardag van Delhaize.

- Er staat een hartje aan einde bericht.
- De link naar de website (http://delhaize-be.site).
- Delhaize stuurt deze promo via Whatsapp.
- De promo is te mooi om waar te zijn.

SOORTEN OPLICHTING – Te mooi om waar te zijn

Gevaar

- Loterij
- Erfenis Spaanse nonkel
- Valse liefdadigheid
- Hulp
- …

Veilig?

- Eerst formaliteiten afhandelen
- Geld aftroggelen, **eerst administratieve kosten** betalen
- Uw persoonlijke gegevens gebruiken

SOORTEN OPLICHTING - Te mooi om waar te zijn

Tips

- Direct deleten!
- Je kan niet winnen aan een wedstrijd waar je niet aan deelneemt!
- Grote firma's organiseren geen loterij door e-mailadressen uit te loten…
- Maak alleen geld over aan een organisatie waarmee je vertrouwd bent.
- Is de **hulporganisatie geregistreerd**? https://donorinfo.be/nl

SOORTEN OPLICHTING - Te mooi om waar te zijn

Gevaar

- **Nigeriaanse oplichting**
  - Via e-mail wordt hulp gevraagd, meestal afkomstig uit Zwart Afrika bv. een geblokkeerde erfenis,
  - Ze hebben hulp nodig voor een grote transactie en voor de hulp krijg je een vergoeding,
  - **Je moet eerst administratieve kosten** betalen,

Tips

- Als de mail afkomstig is van een onbekende: weg ermee!
- Als de e-mail afkomstig lijkt van één van uw kennissen, vraag dan **OP EEN ANDERE WIJZE**
  of die persoon hem daadwerkelijk heeft verstuurd en uw hulp nodig heeft (sms, tel, whatsapp…)

SOORTEN OPLICHTING - Te mooi om waar te zijn

Gevaar

- Appartement, auto, puppy tegen weggeefprijs

    - Verkoper uit het buitenland
    - Waarborg moet overgemaakt worden via Western Union

Voorbeeld

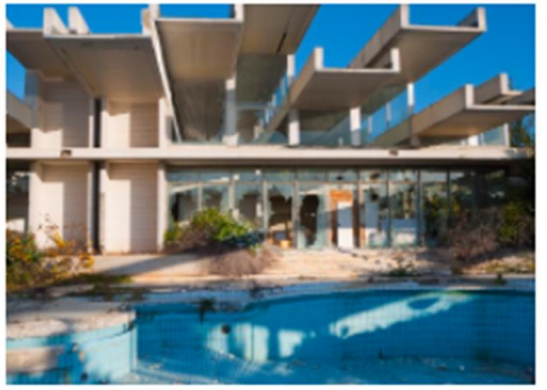
Zoekertje:
Dame geeft puppy weg, omdat ze sinds kort een baby heeft en niet meer voor het beestje kan zorgen. Net naar Londen verhuisd. Ze verstuurt SO foto's van het hondje, neemt op Facebook contact en nodigt haar uit om haar blog te bezoeken. Daar ziet SO verschillende familiefoto's staan, wat haar vertrouwen geeft. SO beslist om het een kans te geven.

Uiteindelijk krijgt SO te horen dat de vrouw de puppy op de luchthaven heeft afgezet en haar zal contacteren. 'Airpets' neemt contact met SO en vraagt € 388 voor de vlucht, te storten via Western Union. SO ontvangt vliegticket, de documenten van de hond en de vluchturen via mail. De volgende dag blijkt hond niet aangekomen. Hij zit zogezegd vast in Duitsland om chip te krijgen. SO moet nog eens € 464 betalen, maar van de hond is er nog steeds geen spoor. SO beseft uiteindelijk dat ze is opgelicht, maar haar geld ziet ze niet meer terug."

SOORTEN OPLICHTING – Te mooi om waar te zijn

Gevaar

- Vakantiewoningen die niet bestaan



En dan blijkt dat vakantiehuis in New York ineens niet te bestaan

Tips

- Vermijd rechtstreekse betalingen aan de verhuurder en werk via platforms die als tussenpersoon optreden: check deze! (vakantiewoningverhuur.be, vakantieverhuur.be, booking.com, …)
- Blijf op hun site voor de communicatie!
- Geen afleiding naar e-mail, whatsapp, sms…

SOORTEN OPLICHTING - Te mooi om waar te zijn

Gevaar

- Valse websites

Voorbeeld

U botst op een website, eventueel via Social Media… U ziet aantrekkelijke prijzen…
U bestelt en krijgt een bevestigingsmail met betalingsgegevens.
U betaalt en krijgt een bevestigingsmail van uw bestelling
U wacht, en wacht, en wacht…

SOORTEN OPLICHTING - Te mooi om waar te zijn

Tips

- Betrouwbare webshops bevatten :
  - **Ondubbelzinnige identiteit** van de verkoper
  - **Duidelijke prijs** voor de producten
  - informatie over waar u de spullen kan **terugsturen** en wie u kan **contacteren** bij problemen
  - Belgische webshops? Kijk uit naar het **BeCommerce-label.**

- Nagaan of een website in België werd aangemeld als frauduleus ? https://temooiomwaartezijn.be/#check-een-site-op-fraude op de site van FOD Economie (https://economie.fgov.be/)

SOORTEN OPLICHTING - Te mooi om waar te zijn

Tips

- **Hoe ken ik deze site? Bij wat koop ik?** Het imago zegt veel over de betrouwbaarheid. Google het bedrijf en lees de recensies.
- **Bij wie koop ik?** De verkoper moet de naam, fysiek adres en ondernemingsnummer op de website zetten. Check deze via KBO (FOD Economie).
- **Wat zijn de voorwaarden?** Levering? Herroepingsrecht 14 dagen? Retourneren naar? Garantie?
- **Wat en hoe betaal ik?** Extreem goedkoop = verdacht! Op welke rekening vraagt men mij te betalen?
- Doe de WebshopCheck - ECC België (eccbelgie.be): is een webshop veilig?

SOORTEN OPLICHTING- Andere

Gevaar

- **Valse boete**

- Criminelen doen zich voor als politiedienst en sturen valse boetes.
- Geen vermelding **nummerplaat**, noch **identiteit eigenaar**, noch **exacte locatie van de overtreding.**
- Het bericht is **dwingend**!

SOORTEN OPLICHTING - Andere

- **De politie zal nooit via e-mail eisen om een boete te betalen!**
- Wees alert als je grote bedragen moet overschrijven.
- E-mailadres van de politie eindigt op **@police.belgium.eu**

Ontving u een valse boete of factuur per mail, stuur deze door naar verdacht@safeonweb.be

Safeonweb.be

10 miljoen verdachte berichten naar Safeonweb in 2023

Afgelopen jaar stuurden oplettende burgers bijna 10 miljoen berichten door naar verdacht@safeonweb.be. In 2022 waren dat er al 6 miljoen. Gemiddeld kregen we maar liefst 27.000 berichten per dag toegestuurd. 2 februari 2023 was een absolute...

Doe aangifte via het meldpunt. https://meldpunt.belgie.be/meldpunt/

SOORTEN OPLICHTING- Andere

Gevaar

- Bank-aan-huisfraude

Je krijgt als nietsvermoedend slachtoffer een telefoontje van iemand die zich voordoet als bankmedewerker met de melding dat er verdachte transacties op je rekening hebben plaatsgevonden en hij stelt voor om bij jou thuis langs te komen om het probleem op te lossen. Kort daarna biedt er zich een zogenaamde bankmedewerker aan aan je woning die je aanspoort om aan de computer te gaan zitten en in te loggen bij je bank. Je moet dringend een som geld overschrijven naar een andere 'veilige' rekening om verdere fraude te voorkomen. In werkelijkheid gaat het om een valstrik en stort je hierbij zelf geld op de rekening van de oplichter. Terwijl jij inlogt noteert de oplichter de pincode van je bankkaart. Daarna stelt hij voor om je kaart doormidden te knippen. De chip blijft daarbij leesbaar. De oplichter neemt je kaart mee en kan er probleemloos verder geld mee afhalen.

SOORTEN OPLICHTING- Andere

Hoe herkennen?

- **De bank stuurt nooit iemand bij je langs!**

- De bank vraagt je nooit om je betaalpas aan iemand mee te geven of op te sturen. Ook niet nadat je de pas hebt doorgeknipt.

- Als je betaalpas vervangen moet worden, knip dan altijd de betaalchip (het goudkleurige vierkantje op de pas) door en gooi de pas daarna weg. Als je alleen de kaart, maar niet de chip doormidden knipt, kan een oplichter met die doorgeknipte betaalpas (en je pincode) nog steeds geld opnemen bij een geldautomaat. Dus onthoud: knip de chip.

- **Een bankmedewerker vraagt nooit naar je inloggegevens, pincode of andere beveiligingscodes.**

- **De bank stuurt je nooit een e-mail, sms of app met daarin een link die direct naar de website van de bank gaat.**

Soorten oplichting

PZ Regio Tielt

1. Internetbankieren
2. Sociale media
3. Zoekertjes
4. Te mooi om waar te zijn
5. **Phishing**
6. Beleggingsfraude

SOORTEN OPLICHTING - Phishing

Gevaar

- Phishing overkomt mij niet.
- Phishingberichten staan vol schrijffouten.
- Phishing wordt alleen via e-mail verstuurd.
- Mijn bank kan telefonisch naar mijn codes vragen.
- Bij mobiel bankieren loop ik meer kans op phishing.
- Een antivirusprogramma beschermt me tegen phishing.

SOORTEN OPLICHTING / Phishing

Voorbeeld

Ik ontvang op vrijdag een sms-bericht van ING Bank. Mijn **inlog van mijn banking-app verloopt** vandaag. Om mijn toegang te verlengen en blokkade te voorkomen dien ik te klikken op de link : 'https://ING-be.com'.

Thuisgekomen klik ik de link aan en kom op een site van ING terecht. Om mijn toegang te verlengen dien ik mijn rekeningnummer in te geven en mijn digipass te gebruiken. Het begin van mijn rekeningnummer staat reeds ingevuld. Zoals voorgeschreven op de site steek ik mijn bankkaart in de digipass en geef mijn code die verschijnt op de digipass.

Er verschijnt een zandlopertje op het scherm. Na 2 minuten stel ik vast dat de aanvraag niet lukt dus sluit ik de site af. Ik ga me maandag aanbieden bij de bank en daar een verlenging aanvragen.

SOORTEN OPLICHTING / Phishing

Resultaat:

Op maandag nadien bied ik mij aan bij de bank. Daar verneem ik dat ik opgelicht ben. Bij nazicht blijkt dat er 3 transacties gebeurd zijn (1 euro, 500 euro en 750 euro). Ik verneem van de bankbediende dat het geld niet meer kan gerecupereerd worden. De bank weigert terugbetaling want ik klikte immers zelf door…

Phishing (= hengelen naar uw persoonsgegevens en uw geld)

- U wordt via een bericht (e-mail, sms, whatsapp…) naar een **valse website** gelokt.
- Deze lijkt sterk op de originele site van een bank of een commerciële site. (LNG/ing)
- U geeft uw gebruikersnaam en paswoord in, maar de oplichter **onderschept** en gebruikt dit om zelf transacties of aankopen uit te voeren.
- Soms vraagt men u software te installeren. Zo nemen ze vanop afstand uw **computer over of zien ze uw toetsaanslagen:** men steelt uw inloggegevens.

TeamViewer AnyDesk

SOORTEN OPLICHTING / Phishing

Voorbeeld

Ik verkoop via ‘www.2dehands.be’ een broek voor 30 euro. Gisteren ben ik gecontacteerd door het nummer 0031657224834 3. De persoon geeft zich uit voor Rachelle DE BOERE. Wij komen een prijs overeen van 35,5 euro, namelijk met mijn verzendkosten bij.

De persoon wenst mijn betrouwbaarheid te verifiëren en vraagt mij 0,1 euro over te schrijven via de link : ‘https://ing-betaling.net/pay/K8un584y’. Ik klik hierop en wordt naar een betaalsite gestuurd. Ik dien gebruik te maken van digipass en uiteraard bankkaart. Het rekeningnummer en de verificatiecode op de digipass dien ik in te vullen op de site. Een eerste poging mislukt dus ik probeer een tweede keer. Ook deze poging mislukt.

Ik stel vast dat de communicatie plots stopt.

Bij nazicht blijkt dat er 3 transacties zijn gebeurd op mijn rekening. Namelijk 2 x 250 euro en 1 x 450 euro is overgeschreven. Gezien de transacties nog lopende zijn hebben wij onmiddellijk cardstop gebeld.

SOORTEN OPLICHTING - Phishing

Gevaar

- Phishing

Tips

- Domeinnamen, bedrijfsnaam staat steeds voor .be of .com en voor de "/"
  - Bij de link www.safeonweb.be/tips (domein = 'safeonweb')
  - Bij de link www.safeonweb.tips.be/safeonweb (domein = 'tips', je wordt naar een andere website geleid)

- ALTIJD OPGEPAST met **linken**!!!
  - Bij mail, SMS of bericht op sociale media. Is het van een kennis? Is zijn profiel niet gehackt? Schrijfstijl, waarom stuurt hij zo'n link? Bij wantrouwen, bel deze persoon op!
    Ga met je muis over de link en check of de url klopt met deze van de officiële site.

SOORTEN OPLICHTING - Phishing

Spoofing (=nabootsing):

- De link in phishingberichten leidt naar een valse website die er uitziet als de echte website van uw bank
- Een e-mail die van uw bank lijkt te komen, maar die toch nep blijkt te zijn
- Oplichters bellen vanuit het buitenland, terwijl er een Belgisch telefoonnummer zichtbaar is

Phishing gaat gepaard met spoofing.

Hoe spoofing herkennen?

- Bij e-mailspoofing: Hebt u eerder mails gehad van die afzender en komt het e-mailadres overeen? Klopt het taalgebruik en het logo van de organisatie? Kijk ook waar de linkjes naartoe leiden, door er met de muis overheen te bewegen.
- Bij websitespoofing: Controleer de url van de website.
- Bij telefoonnummerspoofing: Vraagt een medewerker van een organisatie om persoonlijke gegevens, zoals een wachtwoord of pincode? Hang dan op, zoek het nummer van de betreffende organisatie op internet op en bel om te vragen of zij echt contact met u hebben opgenomen.

SOORTEN OPLICHTING - Phishing

Pas op voor een tweede slachtofferschap: Na een poging tot phishing kunt u ook nog eens gebeld worden door een medewerker van de bank. Deze deelt mee dat er gepoogd is geld van je rekening te halen. De medewerker laat weten dat er **snel** moet gehandeld worden. Om de poging te blokkeren moet ik mijn kaart in de digipass steken en de nodige stappen ondernemen op de site.

Pas op: Vertrouwen winnen: Mijn rekeningnummer staat reeds deels ingevuld, MAAR: Dit betreft een vast nummer waar elk rekeningnummer van deze bank mee begint.

Installeer/activeer uw spamfilter!! Maar **spam** komt er soms toch door…

SOORTEN OPLICHTING - Phishing

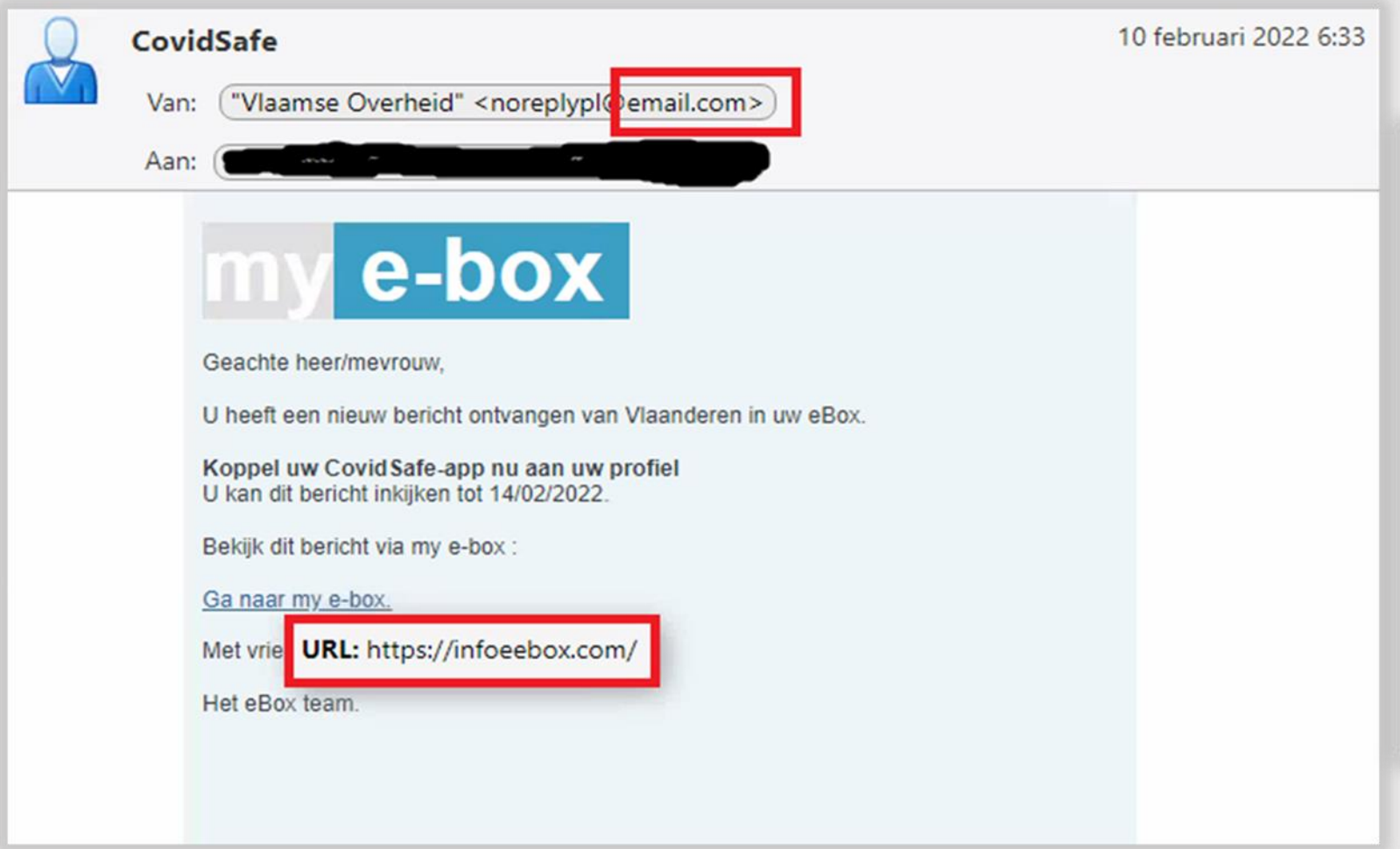
Veilig?

- Uw bank zal u nooit via e-mail, sms, pop-up bericht of telefoon vragen om vertrouwelijke gegevens door te geven of uw bankkaart op te sturen.

- Zo'n bericht is dan ook per definitie een phishingbericht:
  - Het bericht is **plots en onverwachts** toegestuurd.
  - Het **afzenderadres** van de e-mail kan er raar uitzien. Indien u twijfelt, contacteer dan uw bank.
  - De toon is **dringend en dwingend**.
  - Let op **spelling- en grammaticale fouten**.
  - **Controleer de link** in de e-mail door er **met uw muis over te zweven** (maar niet klikken): u ziet nu de URL waar u wordt naartoe geleid. Als deze niet naar de officiële website leidt, is het hoogstwaarschijnlijk een phishingmail.

SOORTEN OPLICHTING - Phishing

Voorbeelden



CovidSafe 10 februari 2022 6:33

Van: "Vlaamse Overheid" <noreplypl@email.com>

Aan: [redacted]

my e-box

Geachte heer/mevrouw,

U heeft een nieuw bericht ontvangen van Vlaanderen in uw eBox.

Koppel uw CovidSafe-app nu aan uw profiel
U kan dit bericht inkijken tot 14/02/2022.

Bekijk dit bericht via my e-box :

Ga naar my e-box.

Met vrie **URL:** https://infoeebox.com/

Het eBox team.

Text Message
Today 05:20

Geachte Klant,
Referentie: 7588412

Wij hebben uw rekening in de 'quarantaine zone' geplaatst. u dient uw Mobiel Bankieren op uw apparaat voor 17/04/21 te bevestigen om blokkade te voorkomen: kb-starten.info
Alvast bedankt voor uw medewerking.
Klantenservice KBC

SOORTEN OPLICHTING - Phishing

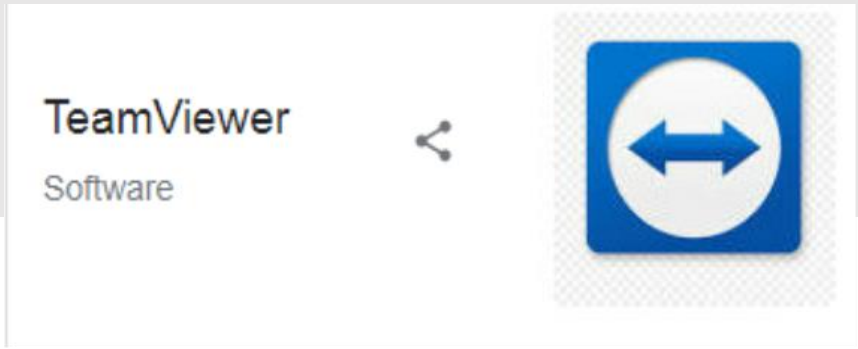
Gevaar

- Helpdeskfraude (bv. Microsoft Scam)

- Dit betreft een vorm van **Phishing** (nl. *vishing*) waarbij cybercriminelen proberen misbruik te maken van iets waar je in gelooft of van iemand die je vertrouwt.

- **Telefonische** oproep door iemand die zich voordoet als **medewerker van de helpdesk** van Microsoft, Apple of een andere computerfirma.

- Vaak enkel in het (gebrekkig) **Engels**.



SOORTEN OPLICHTING - Phishing

Veilig?

- De oplichter krijgt door uzelf **toegang tot je computer**.
- Men wijst vervolgens naar **logbestanden met foutrapporten**
- Om het (zogezegde) probleem op te lossen moet je **betalen**
- De oplichter probeert je **bankgegevens te verkrijgen** en vraagt een betaling te doen.

SOORTEN OPLICHTING - Phishing

Tips

- **Wantrouw** altijd telefoons van bedrijven die u vragen om een aantal acties uit te voeren op uw computer. Microsoft, Apple of andere computerbedrijven zullen u niet ongevraagd contacteren om een probleem te melden
- Ga nooit in op dergelijke telefoontjes
- Noteer indien mogelijk het **oproepnummer** van waar gebeld wordt
- **Verbreek de verbinding**

SOORTEN OPLICHTING - Phishing

4 basisregels om phishing te voorkomen:

- Geef **nooit** uw codes om te internetbankieren via e-mail, sociale media, sms of telefoon. Uw codes om te internetbankieren zijn even geheim als de pincode van uw bankkaart!

- Ga **nooit via een link** naar de betaalsite of mobiele app van uw bank. Uw bank vraagt nooit naar codes via een link.

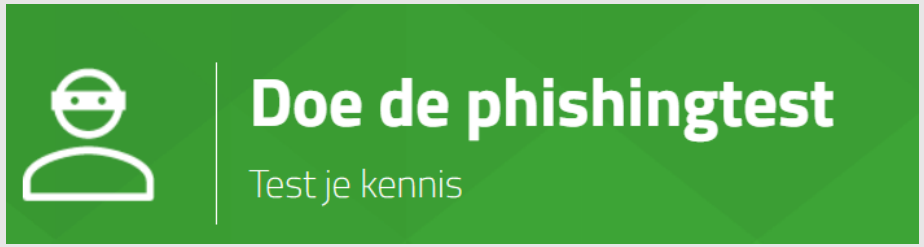
- **Typ altijd zélf het adres** van uw (bank)website in je browser. U kan ook het adres opslaan in uw favorietenlijst van je browser. Of open zelf de mobiele app van uw bank.

- **Als u twijfelt, kan u beter stoppen**. (‘verstojtnie? Bluufterof!’): Kreeg je dus een wat vreemd bericht en weet u niet wat gedaan, neem dan het zekere voor het onzekere en stop alles.

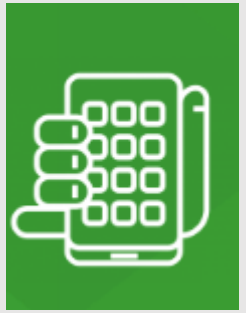
SOORTEN OPLICHTING - Phishing

Safeonweb.be

1. Doe de phishingtest op safeonweb.be



2. Installeer de Safeonweb-app, die je waarschuwt voor cyberdreigingen en online oplichting.



3. Installeer de Safeonweb browser extensie

SOORTEN OPLICHTING – Varianten op Phishing

Vishing *('voice fishing')*:

- Variant van phishing waarbij men door de 'valse' bank of helpdesk wordt opgebeld;
- Hierbij worden eveneens de inloggegevens gevraagd.

Smishing:

- Variant van phishing waarbij men wordt ge-sms't (bv. Whatsapp, Messenger,...) om naar een valse website te surfen;
- Hierbij worden eveneens de inloggegevens gevraagd.

Quishing:

- Variant van phishing waarbij (frauduleuze) QR-codes worden gebruikt;
- Een nietsvermoedend slachtoffer scant de QR-code met zijn smartphone;
- Het slachtoffer wordt vervolgens omgeleid naar de kwaadaardige website of de malware wordt gedownload op hun apparaat.

Soorten oplichting

PZ Regio Tielt

1. Internetbankieren
2. Sociale media
3. Zoekertjes
4. Te mooi om waar te zijn
5. Phishing
6. **Beleggingsfraude**

SOORTEN OPLICHTING - Beleggingsfraude

Gevaar

- **Fraude met vals beleggingsplatform – 'boiler room'-fraude**

Slachtoffer wordt (met belofte van grote winsten) naar een vals beleggingsplatform gelokt, waar je met de belofte van een hoog rendement kan 'beleggen' in fictieve Bitcoins of andere cryptomunten. De 'verkopers' zetten je zwaar onder druk zodat je steeds meer geld zou storten (vandaar de benaming 'boiler-room). De oplichters gaan vernuftig te werk. Ze doen zich voor als dienstverleners met een vergunning, met een professioneel uitziende website. Ze zullen er ook voor zorgen dat je eerste investering altijd winstgevend lijkt. Op die manier winnen ze je vertrouwen. Wanneer nadien geprobeerd wordt om geld af te halen of winsten te verzilveren blijkt dit niet te lukken. De "geïnvesteerde" gelden blijken verdwenen.

SOORTEN OPLICHTING - Beleggingsfraude

Gevaar

- **Fraude met vals beleggingsplatform – 'recovery room'-fraude**

Wanneer je doorhebt dat je geld verdwenen is, kan het nog dat je wordt gecontacteerd door advocaten die je willen helpen je geld te recupereren. Het enige wat je moet doen, is hun ereloon vooraf betalen. Dit zijn natuurlijk dezelfde fraudeurs die hierna dan ook weer verdwijnen, en jij bent nog meer geld kwijt. Dit heet 'recovery room'-fraude. Opgelet dus dat je je geen twee keer laat vangen!

SOORTEN OPLICHTING - Beleggingsfraude

- Wees **waakzaam** bij **beloofde buitensporige winst**. Als een rendement te mooi is om waar te zijn, ….
- **Check de identiteit van de aanbieder** (naam, maatschappelijke zetel, vestigingsland, contactgegevens,…).
- Wees op je hoede voor **'cold calling'** (iemand contacteert je ongevraagd met een financieel aanbod)
- Kijk uit als je contactpersoon je vraagt om geld over te maken naar een bankrekening in een ander land dan waar de aanbieder is gevestigd
- Vraag de aanbieder om duidelijke informatie en lees deze met een kritische blik
- Onder **druk** gezet worden om **snel** te beslissen over dit uniek aanbod
- Als de aanbieder een bijkomende betaling vraagt, is dat vaak een teken van fraude
- Meld slachtofferschap aan de FSMA (Autoriteit voor Financiële Diensten en Markten), die naast de NBB toezicht houdt op de Belgische financiële sector + check je aanbieder via de website https://www.fsma.be/nl/check-uw-aanbieder

Wees alert en vertrouw uzelf!

PZ Regio Tielt

Vertrouw niet uitsluitend op de technologie om je te beschermen: JIJ ZELF bent de beste verdediging. Door gezond verstand kun je veel aanvallen herkennen en stoppen!

Herken de 4 kruiden van oplichting:

- Hun geloofwaardigheid:
  - Te mooi om waar te zijn? = te mooi om waar te zijn
- Uw tijdsdruk
  - U ervaart paniek of tijdsdruk: U dient, u moet… OF ER VOLGT…
- Uw hebzucht
  - Grote winst/korting
- Uw angsten
  - Uw goedheid als mens

"Ellebogen": **twijfel is géén twijfel!**

Slachtoffer?

Wat nu?

PZ Regio Tielt

Contactnames:

- Fraudedienst bank (app!) – blokkeren transactie?
- Card stop 24/7 : 078/170.170
- Atos Worldline (transacties + tijdstip + locatie afhaling)

Melden/klacht indienen:

- Bij de uitgever van de kredietkaart (terugstorting van nadeel via “charge back” systeem maar dit is geen verplichting).
- De website waar u gehackt bent en volg hun procedure (bv. Facebook, eBay, Paypal, 2dehands.be…)
- www.mijnkaart.be: fraudeuleuze transacties betwisten
- Meldpunt FOD Economie: meldpunt.belgie.be
- Nazicht inzake kwaadwillige oproepen: Ombudsdienst voor telecommunicatie.
- verdacht@safeonweb.be

Slachtoffer?

Wat nu?

PZ Regio Tielt

Privégegevens beschermen

- Voor vragen rond de bescherming van uw gegevens kan je terecht bij de gegevensbeschermingsautoriteit: www.gegevensbeschermingsautoriteit.be.

Aanvullende acties

- Waarschuw uw vrienden dat u hen een vals bericht hebt doorgestuurd.
- Verander uw wachtwoord.
- Annuleren online bestelling (schade proberen beperken)

Slachtoffer?

Wat nu?

PZ Regio Tielt

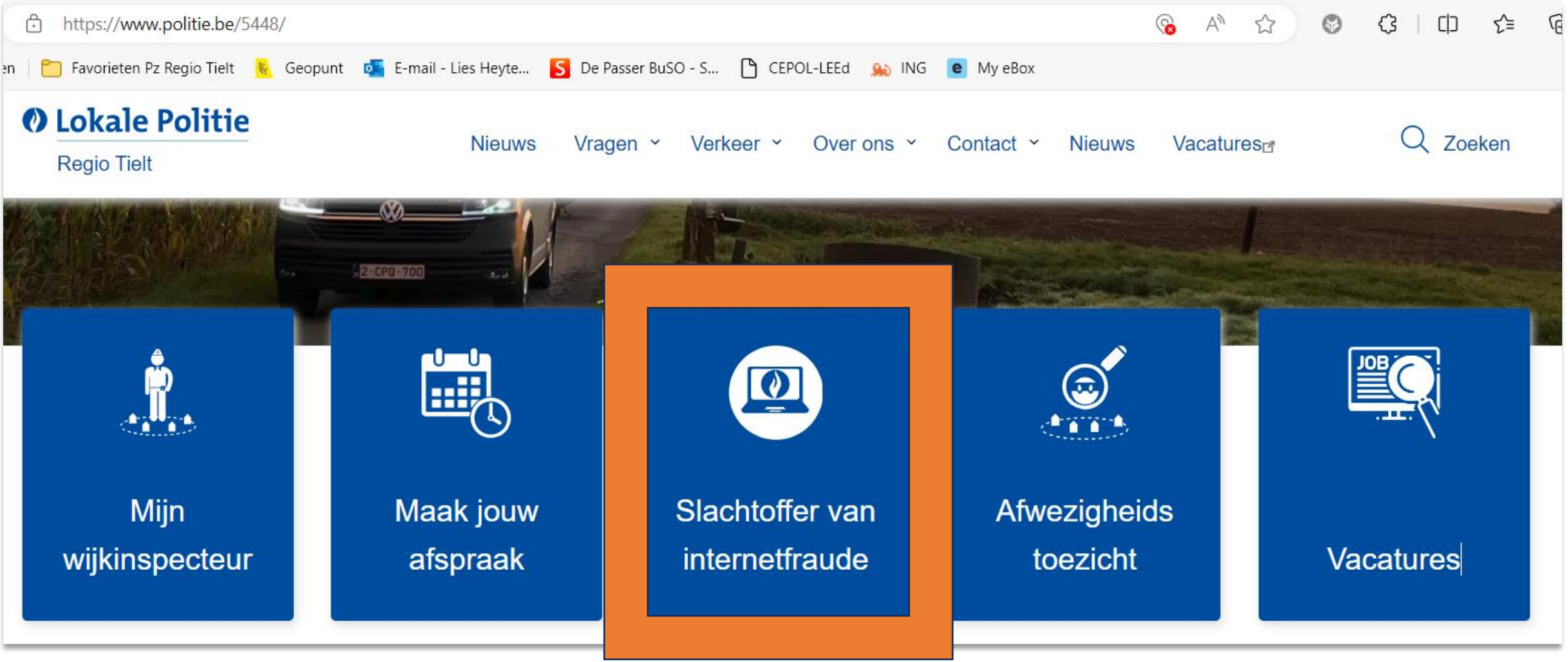
Slachtoffer van een misdrijf: Klacht indienen bij de politie.

Maximale infogaring en aandacht voor identificeerbare elementen (= jouw verantwoordelijkheid als SO):

Eigen rekeningnummers en dat van de verdachten, screenshots, rekeningafschriften, links, e-mails van de verdachte en hun e-mailheaders, URL van de phishing site, Facebook-ID van de verdachte, printscreen van zoekertje, accountgegevens van oplichter zoals Facebook ID waarop zoekertje staat, telefoonnummers, bitcoinadres, logfiles en screenshots van de hack van de sociale media-account (+tijdzone van de logfiles en het vermoedelijke IP-adres van de verdachte), rapporten van de, door het slachtoffer ingehuurde, ICT-dienstverleners worden best ook toegevoegd,…

Meer info

https://www.politie.be/5448/



Meer info

PZ Regio Tielt

- www.safeonweb.be
- www.febelfin.be
- www.ccb.belgium.be
- www.cybersimpel.be

Vragen?

PZ Regio Tielt