Oplichting via internet

PZ WOKRA – ACP Liebeth Caals

Overzicht

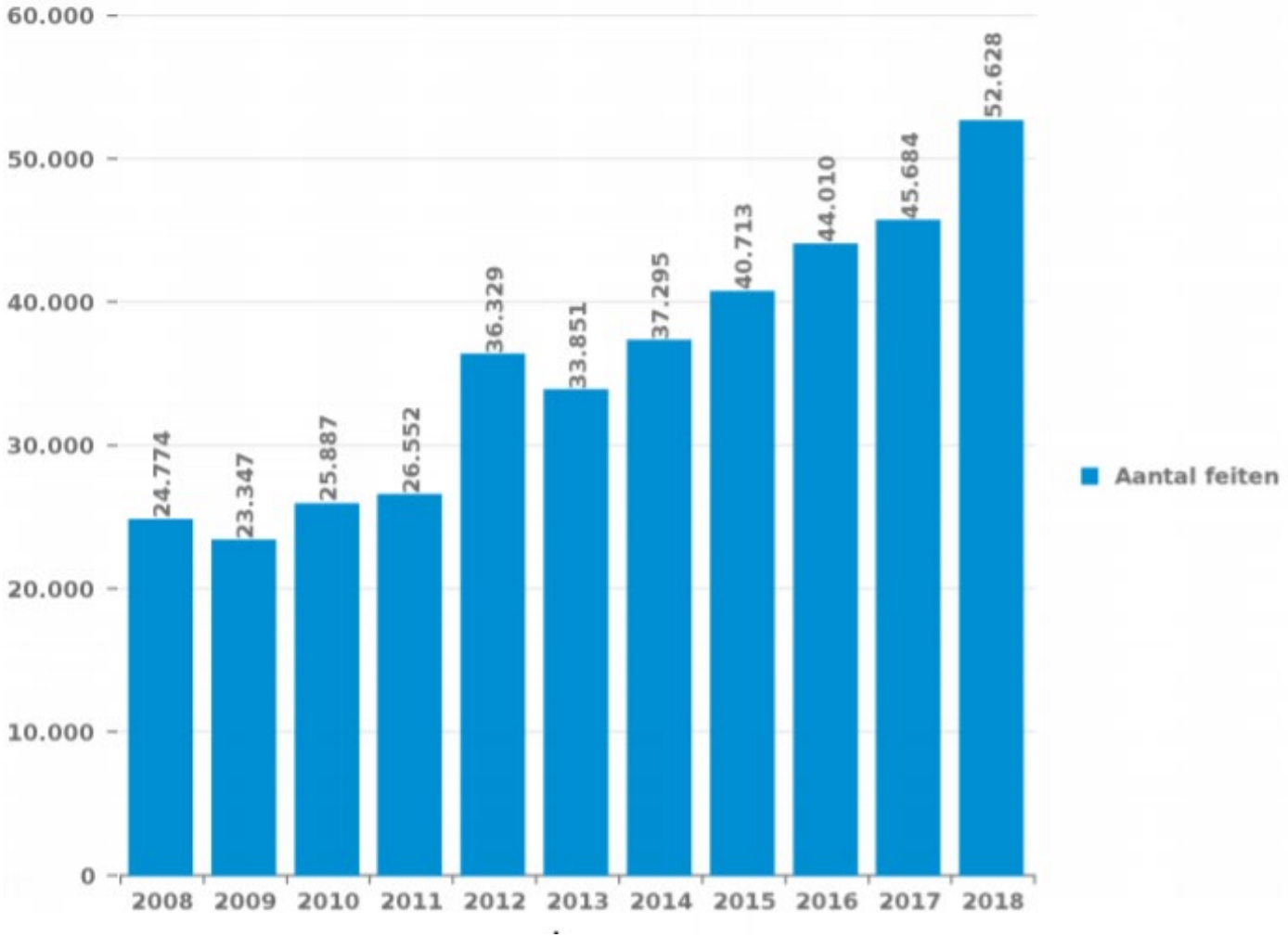
- Cijfergegevens
- Oorzaken evolutie
- Verschillende vormen van oplichting
- Tips & tricks
- Wat als je slachtoffer werd
- Interessante websites

Cijfergegevens

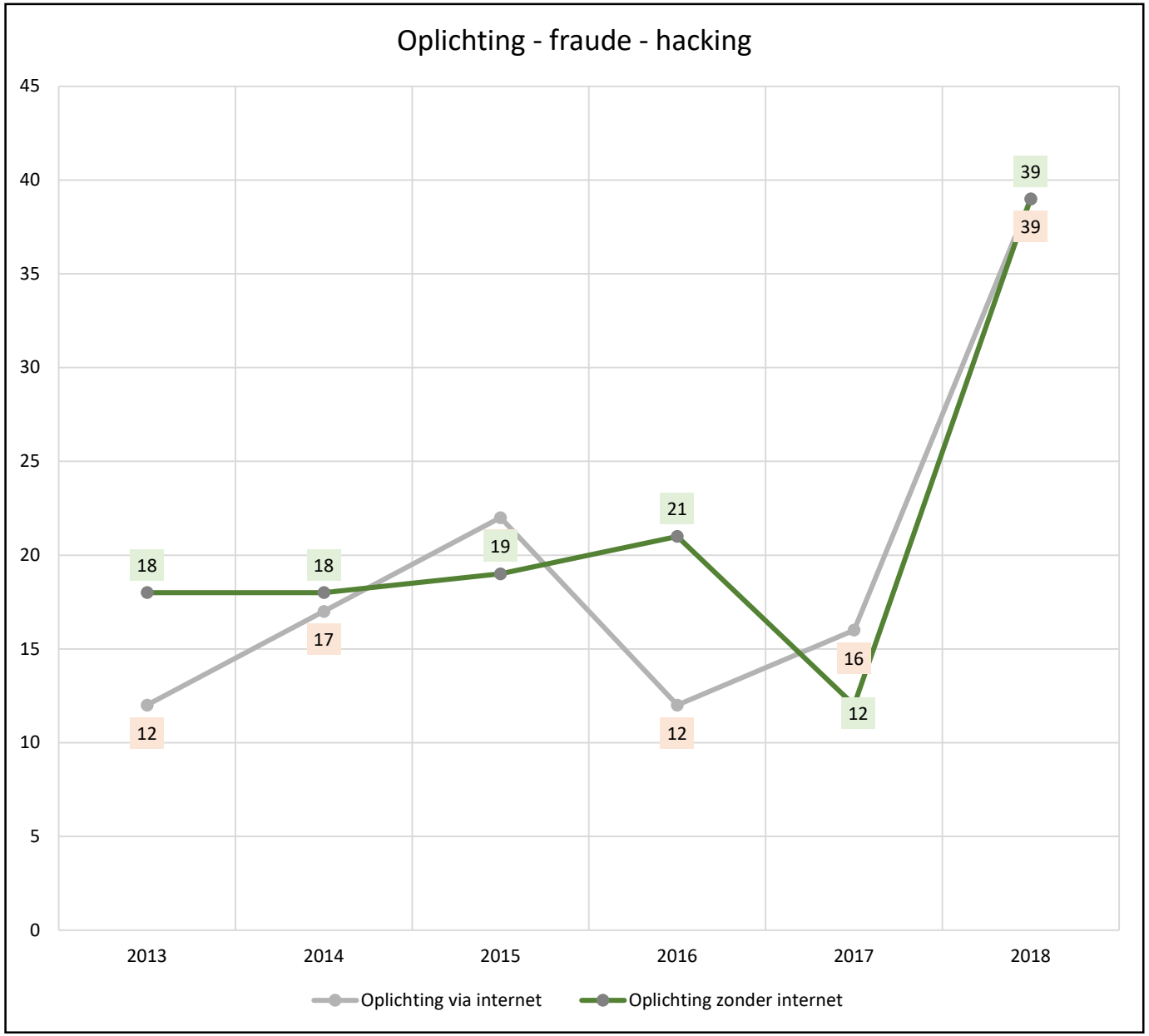
BELGIË

Totaal aantal misdrijven met een ICT/online element sinds 2008

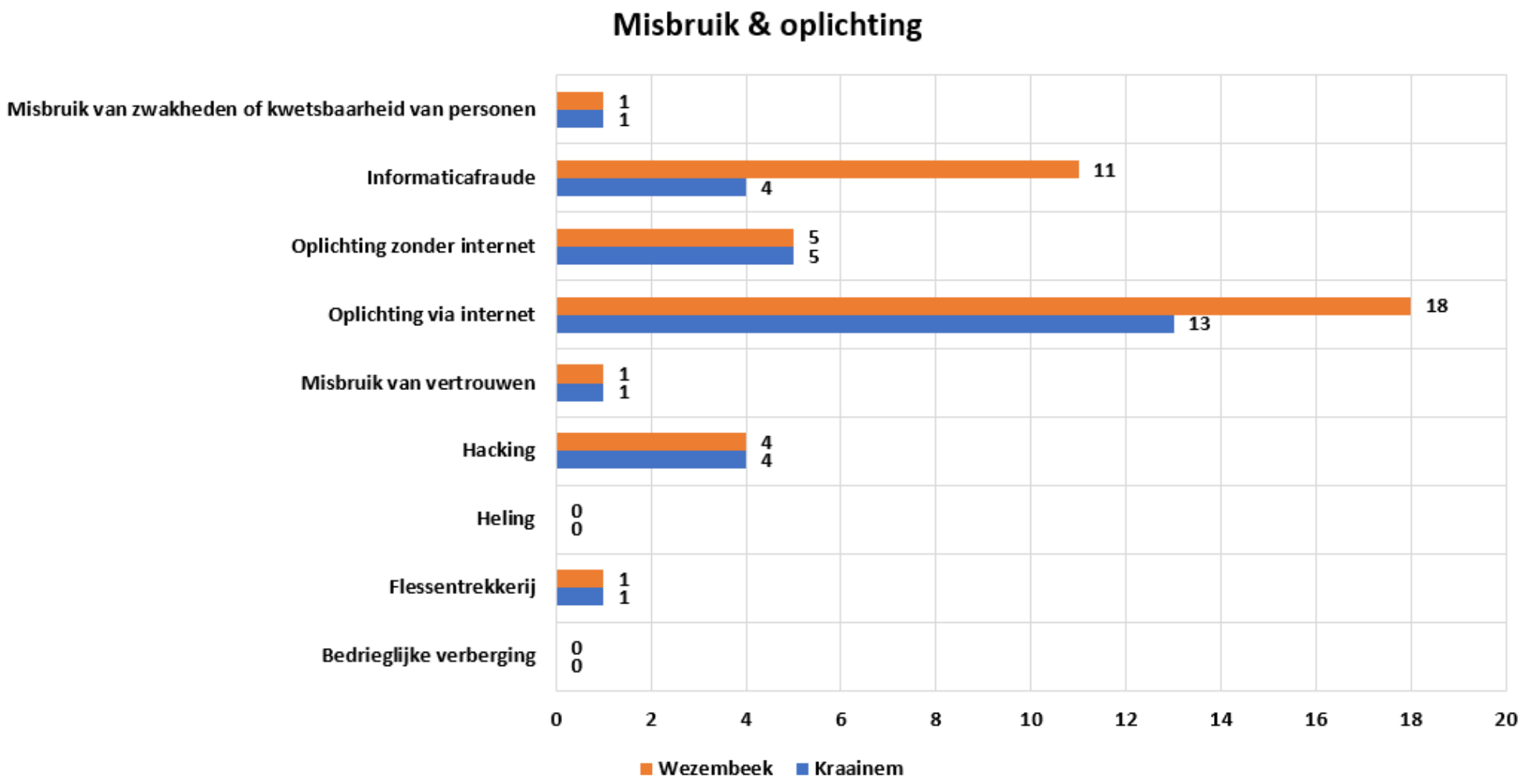
(deze cijfers kunnen een onderschatting zijn, dit afhankelijk van vattingspraktijken en technische beperkingen)



Evolutie Politiezone Wokra 2017 - 2018



Cijfers januari – september 2019



Dark number

- 8% van de bevolking zegt minstens 1 keer slachtoffer te zijn geweest.
- Slechts 20% heeft hiervan aangifte gedaan bij de politie.
- Gevolg het dark number is 80%.
- Naar schatting werden in de periode 2017 – 2018
  200.000 informatica gerelateerde misdrijven niet aangegeven.

Oorzaken evolutie

- Evolutie naar een cybermaatschappij
  - Leef en werkomgeving verschuift meer en meer naar het internet
    - E-mail
    - E-Banking/E-Commerce
    - Sociale media
    - Data en verwerking in “The Cloud”
  - Steeds meer verschillende toegangen tot internet
    - Smartphones
    - Tablets

Oorzaken evolutie (2)

- Voordelen voor oplichters
  - Hoeven zich niet te verplaatsen.
  - Toegang tot een zeer groot potentieel aan slachtoffers.
  - Kunnen de tijd nemen om een tactiek uit te werken.
  - Hebben weinig financiële middelen nodig.
  - Bij betrapping zeer snel hun sporen uitwissen.

Verschillende vormen van oplichting via internet

- Phishing
- Oplichting bij online (ver)kopen
- Fraude met cryptomunten
- Ransomware
- Emotiefraude
  - Vriendschapsfraude
  - SOS fraude
  - Valse liefdadigheid

Phishing

- Wat is het?
  - Samentrekking van “fishing” en “phreaking”.
  - Achterhalen van vertrouwelijke gegevens om er misbruik van te maken.
  - Sterke stijging tussen 2017 – 2018 (475 t.o.v. 1.277).

- Hoe werkt het?
  - Oplichters sturen een e-mail/bericht dat afkomstig lijkt van een bank of andere bekende organisatie en vragen om bankgegevens te delen door te klikken op een link die leidt naar een professioneel ogende pagina.
  - Met de verkregen gegevens doen ze overschrijvingen naar hun eigen rekeningen.

6 mythes over phishing

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

Hoe phishing herkennen?

- Kijk naar de domeinnaam: begint het met “https://” en is het woord voor .be, .com, .eu, .org,.. en voor de allereerste “/”, ook echt de naam van de organisatie?
  - **https://www.ing.be**
  - **http://https.www.argenta.be.madlart.com/nl/aanvraag.**
- Eigenschappen van Phishingberichten:
  - Zijn onverwacht.
  - Dwingend karakter of maken je nieuwsgierig.
  - Voorzien van onpersoonlijke aanspreking.
  - Vragen om op een link te klikken of een bijlage te openen.
  - Vragen naar persoonlijke gegevens.


1 ONGELEZEN BERICHT
VANDAAG
250 Eur te winnen bij Delhaize via WhatsApp: Kijk: http://delhaize-be.site waardebonnen van €250 van Delhaize. Ze vieren hun verjaardag. Ik denk dat de aanbieding beperkt is. Ik heb de mijne al geclaimd. ❤️
13:17
Type a message

de post <noreply@xyz542.be>
To YOU

de post

Dag,

BOLSY heeft je een pakje met nummer 3232000179598199566320 40 gestuurd. Vandaag, tussen 08:00 en 17:00 komt de post het jou bezorgen.
Wij hopen dat je dan aanwezig zal zijn.

Je kan de status van jouw pakje raadplegen via onze track & trace applicatie. Indien je de link niet kunt openen, gelieve dan onze tool te downloaden om jouw pakje live te volgen.

Met vriendelijke groeten,
de post.

Uw nieuwe bankkaart - importance: high

QWT35 Bank Klantendienst <info@vnnabsbns.com>

Geen afbeeldingen in deze e-mail? Lees hem dan online.

QWT35 BANK

Uw nieuwe bankkaart

Geachte Cathy Jansens,

Uit onze administratie blijkt dat u, ondanks eerdere berichten, nog gebruikt maakt van de verouderde versie van de QWT35 Bank bankkaart.

Zichtrekeninghouders van QWT35 Bank hebben tot 21 juli 2017 de mogelijkheid om kosteloos een vernieuwde QWT35 Bank bankkaart te bestellen.

Zichtrekeninghouders die voor 21 juli 2017 geen gebruik maken van de eenmalige actie, krijgen automatisch een vernieuwde QWT35 Bank bankkaart toegestuurd. De kosten voor het automatisch toesturen van de vernieuwde bankkaart zijn € 17,95 en wordt automatisch in rekening gebracht. Zichtrekeninghouders ontvangen hierover bericht.*

Bespaar en klik hier om kosteloos uw vernieuwde bankkaart te bestellen.

Met vriendelijke groeten,

Uw QWT35 Bank team

Herinnering eerste aanmaning voorkom een tweede verhoging - importance: high

Federale Politie <federalepolitie@hsruhaw.com>

Bel **101** voor dringende politiehulp

Politie

Geachte heer/mevrouw,

Bij deze willen wij u per mail mededelen dat u nog een bedrag bij ons heeft openstaan wegens het overtreden van een verkeersvoorschrift. Wij hebben u per brief verzocht om de betaling te voldoen. Hiervoor hebt u al één herinnering ontvangen.

Het openstaande bedrag is tot op heden (nog) niet voldaan.

Informatie over de overtreding en de onmiddelijke schikking.

Omschrijving overtreding	Overschrijding maximum snelheid op (auto)wegen buiten bebouwde kom gewone wegen, met 22 km/h	
Datum	12-08-2017	
Tijdstip	19:36	
Toegelaten snelheid	100km/h	
Gemeten snelheid	128km/h	
Gecorrigeerde snelheid	120km/h	
Fotofilmnummer	1805076184	
Zaaknummer	1822719	
Opgelegde sanctie	€ 97,50	De sanctie is gebaseerd op de gecorrigeerde snelheid
Administratiekosten	€ 06,00	
Te betalen	€ 103,50	

Voorkom herinneringskosten

Wij stellen u thans nog eenmaal in de gelegenheid het verschuldigde bedrag van € 103,50 uiterlijk voor vrijdag 8 januari te voldoen via Bancontact/Mistercash gelinkt aan 3V Payment Group. U betaalt alleen het oorspronkelijke bedrag van € 103,50 dat u verschuldigd bent. U kunt via onderstaande link het bedrag via onze site voldoen.

Klik hier om het openstaande bedrag via Bancontact/Mistercash te voldoen

Zodra u het openstaande bedrag hebt voldaan, ontvangt u een unieke 19-cijferige code per mail. Om de onmiddelijke schikking volledig te voldoen is het van belang dat u de 19-cijferige invult op onze website. Klik hier om de 19-cijferige code in te vullen op onze en om de onmiddelijke schikking te voldoen.

Na dat u de 19-cijferige code zorgvuldig heeft ingevuld zult u automatisch worden doorverwezen naar onze homepage. Indien wij het bedrag niet niet voor bovenstaande van u ontvangen, zal het openstaande bedrag verder worden worden verhoogd met de wettelijke herinneringskosten.

Wij vertrouwen erop u voldoende te hebben geïnformeerd.

Hoogachtend,

Federale Politie.

Politie

Bel **101** voor dringende politiehulp

Enkele tips

- Controleer het e-mailadres op spellingsfouten en de correcte bedrijfsnaam.
- Vertrouw geen alarmerende e-mailberichten van banken, grote bedrijven, verzekeringsmaatschappij,…
- Open geen bijlagen aan e-mails die je niet vertrouwt.
- Een bankinstelling zal nooit via e-mail of telefoon om vertrouwelijke gegevens vragen.
- Ga naar je homebank via de website en nooit via een link in een e-mail.
- Op het moment dat u een betaling doet, kijk naar de URL dat deze begint met “https://” dit wijst op een beveiligde omgeving.

Oplichting bij online kopen en verkopen

- Wat is het?
  - Koper betaalt maar ontvangt niets of iets minderwaardigs.
  - Verkoper verstuurt het goed maar wordt niet betaald of met valse betaalmiddelen.

Voorbeeld

Politie waarschuwt voor valse zoekertjes op immosites: “Sommige van die woningen bestaan helemaal niet”

02/03/2019 om 07:38 door gjs | Bron: VRT NIEUWS - Print - Corrigeer

Werkwijze wanneer u koper bent

- Contact met de oplichter via:
  - een valse advertentie op een legitieme site (vb. 2dehands.be, Immoweb,...),
  - of een verkoopsite die volledig frauduleus is opgezet.
- De oplichter doet zich voor als verkoper en biedt object(en) te koop aan voor een abnormaal lage prijs.
- De “verkoper” vraagt over het algemeen om het afgesproken bedrag over te maken via een geldtransfersysteem (vb. Western Union of MoneyGram).
- Betaling verricht, oplichter verdwijnt en is niet meer te contacteren.

Modus operandi wanneer u verkoper bent

- Slachtoffer komt in contact met de oplichter via een advertentie op een legitieme veilingsite (Vb. 2dehands.be, Immoweb,...).
- De “koper” zal zelden discussiëren over de prijs.
- Drie mogelijke scenario’s:
  - “Koper” betaalt het gevraagde bedrag met valse/vervalste cheque van een buitenlandse bank. Artikel wordt opgestuurd. Bank vordert het geld terug van de verkoper.
  - “Koper” vraagt om een bedrag voor te schieten voor vb. transportkosten. Voorschot wordt betaald via geldtransfersysteem (vb. Western Union). Nadien verdwijnt de “verkoper”.
  - “Koper” betaalt meer dan afgesproken met valse/vervalste cheque van een buitenlandse bank. Zegt dat het om een vergissing gaat en vraagt om het verschil terug te storten. Artikel wordt verstuurd, “koper” verdwijnt.

Kenmerken van frauduleuze zoekertjes

- Te goedkoop.
- De beschrijving van het product stemt niet overeen met de foto.
- Er staan schrijffouten in het zoekertje.
- Contactgegevens ontbreken of situeren zich in het buitenland.

Enkele tips

- Geef geen persoonlijke informatie (identiteitsdocumenten, bankgegevens). Oplichters kunnen ze gebruiken voor het plegen van andere criminele feiten.
- Ga niet in op het voorstel om de afhandeling via een ander platform te doen.
- Maak eventueel gebruik van een afzonderlijke kredietkaart voor online aankopen die niet gelinkt is aan andere rekeningen, zo blijft bij oplichting de schade beperkt tot een minimum.

Fraude met cryptomunten

Wat is het?

- Nepadvertenties op sociale media waarin BV's zeggen rijk te zijn geworden met bitcoins (= een virtuele munt).

- Cryptomunten zijn de hype van het jaar. Het zijn een soort digitale en volledig virtuele munteenheden in de vorm van cryptografische (versleutelde) codes. Die codes veranderen naarmate er transacties gebeuren met de munt. Dit principe wordt "blockchain" genoemd.

Voorbeelden

SPECIALE BERICHTGEVING: De meest recente investering van Philippe geubels verbaast experts en maakt grote banken doodsbang

Belgen verdienen al miljoenen euro's vanuit huis door gebruik te maken van deze maas in de wet om rijk te worden. Maar is het legaal?

Zoals Bericht Door

NOS | V | d | ELSEVIER | de Gelderlander

Hoe werkt het?

- Mensen worden geleid naar sites waar men kan beleggen in virtuele munten, met de belofte van hoge winsten.
- Oplichters huren marketingbedrijven in om mensen naar hun sites te lokken. Deze bedrijven werken met tussenpersonen die de advertenties met bekende personen maken en verspreiden. Zij moeten inschatten welke bekende personen populair genoeg zijn om aan te slaan bij het grote publiek.
- Vb. in België: Philippe Geubels, Gert Verhulst, Marc Coucke, Eddy Planckaert en Stromae.

Enkele tips

- Weet met wie je te doen hebt.
  - Controleer je tegenpartij. Beschikken ze over een website? Hoe oud is die? Welke personen zitten er achter, zijn ze gekend voor fraude?
- Deel nooit persoonlijke gegevens.
  - Oplichters vragen vaak om een kopie van je identiteitskaart, een foto, bewijs van domicilie of de nummer van je bankkaart of kredietkaart. Soms beweren ze dat dit wettelijk verplicht is.
- Eis duidelijke en verstaanbare informatie van je gesprekspartner.
  - Laat je niet opjagen of intimideren. Het feit dat je de tegenpartij in levende lijve hebt ontmoet/gehoord is geen garantie dat je niet opgelicht wordt.
- Wees op je hoede voor beloftes van buitensporige winst.
  - Als het rendement je te mooi lijkt om waar te zijn, is het dat meestal ook. Winst is nooit gegarandeerd.

Ransomware
(=gijzelsoftware)

- Malware die een computer en/of gegevens die erop staan blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te “bevrijden” middels een tegen betaling versterkte code.

- Betalen blijkt echter niet (altijd) tot deblokkering van de besmet geraakte computer te leiden.

- Zelfs wanneer na betaling de code succesvol wordt gebruikt blijft de software op de computer staan en kan deze enkele maanden later opnieuw het systeem blokkeren en om nog meer geld vragen.

Voorbeelden

Hoe werkt het?

- Computers van slachtoffer worden geïnfecteerd zoals bij het verspreiden van een virus.
- Bij de heropstart van de computer verschijnt de melding dat de computer geblokkeerd werd.
- Vaak wordt de indruk gewekt dat het bericht afkomstig is van een betrouwbare (overheids)instantie en dat er een boete moet worden betaald wegens misbruik van het internet, bijvoorbeeld het downloaden van auteursrechtelijk beschermd materiaal.

Enkele tips

- Actuele software gebruiken. De fabrikanten van software brengen regelmatig updates uit om beveiligingslekken te dichten, zoals Microsoft Windows, Adobe Reader, Flash Player ...
- Niet surfen op het internet zonder up-to-date antivirusprogramma.
- Gebruik van een firewall.
- Niet openen van verdachte bijlagen aan e-mails.
- Niet downloaden en installeren van nepprogramma's of van gehackte (illegale) software.
- Niet zo maar links activeren zoals "klik hier“.

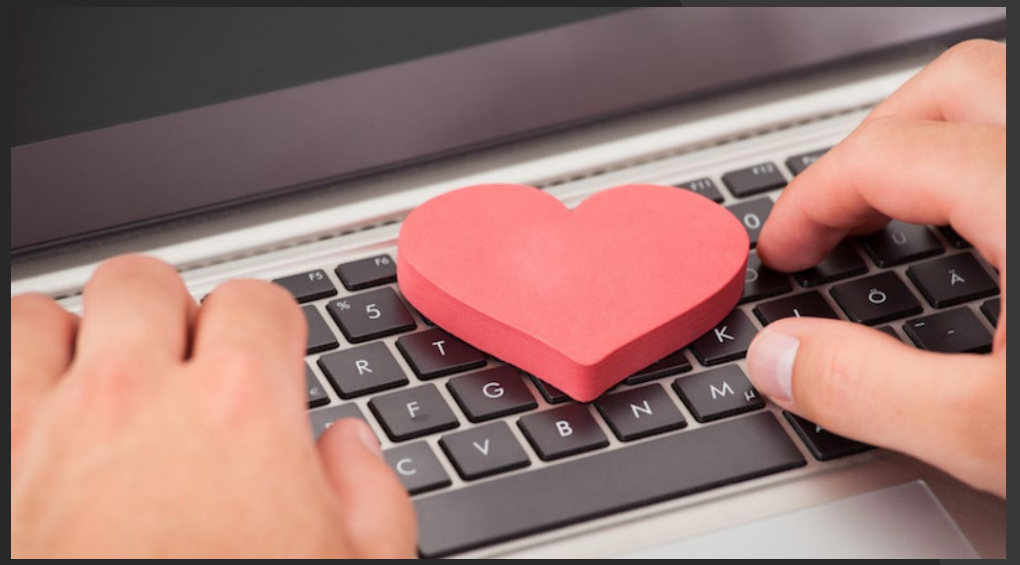
Wat indien je slachtoffer werd?

- Zet je wifi uit of trek je internetkabel uit.
- Koppel onmiddellijk alle andere toestellen los.
- Kijk op de website www.nomoreransom.org of de sleutel voor de ransomware beschikbaar is.
- Laat je toestel helemaal opnieuw installeren en gebruik achteraf een back-up of reservekopie om je gegevens terug te zetten.
- Betaal in geen geval.

Emotiefraude

- Wat is het?
  - Oplichters spelen in op de gevoelens van de slachtoffers om hen geld te ontfutselen.

- Verschillende vormen van emotiefraude:
  - Vriendschapsfraude of datingfraude
  - SOS fraude
  - Valse liefdadigheid



Vriendschapsfraude

Een kankerbehandeling, een vriend in het ziekenhuis, een ticket voor een exotische schone. Zo proberen 'vriendschapsfraudeurs' geld af te troggelen

28/01/2019 om 06:34 door krs

■ Een vriend in het ziekenhuis, een ticket voor een exotische schone: zo proberen

In 2018: 5,4 miljoen euro buit

Aantal meldingen van vriendschapsfraude verdubbeld

om 13:42 door adm | Bron: BELGA - Print - Corrigeer

Werkwijze

- Oplichters zoeken hun potentiële slachtoffers via datingsites en -applicaties, maar gebruiken ook e-mail, chats of sociale media.
- Ze gebruiken een vast profiel, fictieve naam of een gestolen identiteit van een werkelijk persoon.
- Verklaren hun liefde op zeer korte tijd.
- Doel is een vertrouwensband op te bouwen.
- Proberen je te overtuigen om de gesprekken verder te zetten via een ander communicatiekanaal dan datgene waarin de eerste kennismaking tot stand kwam.
- Men verzint allerhande verhalen om geld te doen overschrijven.
- Als je wil afspreken om elkaar te zien is er altijd wel een excuus om dit niet te doen.
- Bij sommigen een “never ending story” of plots blijft het stil aan de andere kant.

Enkele tips

- Ga de echtheid van het profiel na. Vraag voldoende informatie en ga de identiteit na via andere kanalen.
- Vertrouw niet zomaar iedereen. Persoonlijke informatie houd je best voor jezelf.
- Wees op je hoede voor “zielige verhalen”. De oplichters zullen snel op je gemoed beginnen werken. Vraag je af waarom jij degene bent aan wie financiële steun gevraagd wordt.
- Houd je portemonnee absoluut dicht. Besef dat het om een wildvreemde gaat, iemand die je nooit in het echt hebt ontmoet.

SOS-fraude

- Gaat steeds gepaard met de hacking van een e-mailaccount.
- Hacker stuurt een noodoproep naar alle contacten in het adresboek.
- Voorbeeld: Iemand is op vakantie zijn/haar bankkaart kwijtgespeeld en heeft dringend geld nodig om terug te keren. Uiteraard zal het verschuldigde bedrag worden terugbetaald. Er wordt gevraagd om het geld over te maken via Western Union of MoneyGram.

Hoe reageren?

- Niet antwoorden op de e-mail.

- Probeer de rechtmatige eigenaar via een andere weg te contacteren om hem/haar op de hoogte te brengen dat het e-mailaccount gehackt werd.

Valse liefdadigheid

- Wat is het?
  - Zeer snelle reactie gevraagd op gebeurtenissen uit de actualiteit.
  - Fictieve hulporganisaties of misbruik van de naam van een gereputeerde instelling.
  - Er bestaat ook *spam* met hartverscheurende berichten over natuurrampen of ernstig zieke kinderen waarbij gevraagd wordt een gulle bijdrage te storten aan een onbekende organisatie.

- Hoe gaan ze te werk?
  - Oplichters maken handig gebruik van het medeleven van mensen en spelen hierbij vaak slim in op de actualiteit. Telkens wanneer er een ramp heeft plaatsgevonden, zijn ze er als de kippen bij om uit naam van een gekende of fictieve liefdadigheidsorganisatie fondsen te verzamelen.

Voorbeelden

PAYPAL.ME

Pay help animals using PayPal.Me

Go to paypal.me/helpanimalsos and type in the amount. Since it's PayPal, it's easy and secure. Don't have a PayPal account? No worries.

Showbizz

Helmut Lotti waarschuwt voor oplichters: "Laat mijn fans en vrienden met rust!"

TDS | 24 juli 2019 | 06u00 | Bron: TV Familie

DEEL 1 REACTIE

Onderscheid oplichters en echte liefdadigheid

- Nagaan wanneer de groep/stichting werd opgericht.
- U wordt onder druk gezet om medelijden te voelen.
- Bevat onduidelijke of ontbrekende ondersteunende documentatie.
- Reacties op vragen om opheldering worden niet beantwoord en snel verwijderd.
- Verwijzing naar zogenaamde websites van stichtingen.
- Help anderen maar blijf kritisch nadenken!

Algemene Tips en Tricks

- Geef nooit je pincode of codes om te internetbankieren via e-mail, sociale media, sms of telefoon.
- Negeer elk bericht dat je via een link naar de betaalsite of app van je bank leidt.
- Typ altijd zelf het adres van een website in je browser. Zeker voor de website van je bank. Of open zelf de app van je bank.
- Kijk de URL na: “https://” wijst op een beveiligde website.
- Zorg ervoor dat je weet met wie je te doen hebt.
- Als het te mooi is om waar te zijn, is het dat ook!

Wat indien je slachtoffer werd?

- Verwittig onmiddellijk Card Stop (www.cardstop.be of 070 344 344) indien je kaartgegevens hebt doorgegeven.
- Neem contact op met je bank.
- Verander zo snel mogelijk je codes.
- Doe aangifte bij de politie.
- Ga naar https://meldpunt.belgie.be/meldpunt/

Interessante websites

- **https://www.safeonweb.be/**
- **https://www.safeonweb.be/nl/doe-de-phishingtest**
- **https://temooiomwaartezijn.be/#check-een-site-op-fraude**