Politie Wokra

Wezembeek-Oppem & Kraainem

Molenweg 20 - 1970 Wezembeek-Oppem - Tel.: 02 766 18 18

Openingsuren

Maandag t.e.m. vrijdag: 7 - 19u
Weekend en feestdagen: gesloten

Voorwoord

Een e-mail ontvangen van de notaris met de melding dat een verloren gewaande tante haar hele erfenis aan jou overlaat?

Via Facebook een Amerikaanse ex-militair leren kennen die je hoofd op hol heeft gebracht en je wil komen bezoeken in België, mits jij geld opstuurt voor de vliegtickets?

Een bericht van je kleindochter die zegt dat ze een nieuw oproepnummer heeft en geld nodig heeft omdat ze in de problemen zit?

Verdachte e-mails of oplichting via het internet herkennen is niet altijd even makkelijk. Cybercriminelen worden steeds vindingrijker en dus wordt het ook steeds moeilijker om valse berichten te onderscheiden van echte.

Op de volgende pagina's proberen we uit te leggen welke vormen van cybercriminaliteit er zijn en hoe je ze kan herkennen, geven we tips mee en zeggen we je wat je moet doen indien je toch slachtoffer bent geworden.

Nr.28 01/2023

Verantwoordelijke uitgever: Steve Vanhelmont

Ontwerp: Harry Fatoux

Version française au verso

Fraude bij online kopen

Dit is een vorm van oplichting waarbij je in contact komt met de oplichter via een valse advertentie op een legitieme site (2dehands, Autoscout, Immoweb, ...) of via een volledig frauduleuze website. De oplichter doet zich voor als verkoper en biedt een voorwerp aan, meestal aan een abnormaal lage prijs. Eenmaal het geld is overgemaakt verdwijnt de oplichter van de aardbol.

Alarmsignalen:
- De prijs is te mooi om waar te zijn.
- Gebruik van alternatieve betaal-methodes zoals Western Union of Moneygram.
- Contactname via Whatsapp
- Gebruik van tussenpersonen.
- Gebrekkig Nederlands en taalfouten.
- Buitenlands e-mailadres of gsm-nummer.
- Aanbiedingen via sociale media.
- Enkel populaire producten zoals iPhones, Airpods, PS5, Oled-tv's, ...

Tips:
- Geef geen persoonlijke info.
- Verbreek alle contact en betaal niets.
- Gebruik enkel gekende websites.
- Spreek fysiek af.
- Maak gebruik van Visa of Mastercard.
- Onderstaande website geeft je handige tips om de echtheid van een website te controleren: www.eccbelgie.be/themas/onlineaankopen/doe-de-webshop-check.
- Zoek naar gebruikerservaringen.

Fraude bij online verkopen

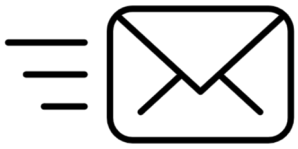
De oplichter reageert op een advertentie van jou en discussieert zelden over de prijs. Vervolgens kunnen er zich 4 scenario's voordoen:

1. De koper betaalt met een vervalste cheque van een buitenlandse bank. Je ontvangt het geld maar nadien blijkt de cheque vals en vordert de bank het geld terug. Je artikel is dan wel al opgestuurd...
2. De koper betaalt een hoger bedrag, opnieuw met een valse cheque, en vraagt het verschil terug te storten. Ditmaal ben je naast je artikel ook nog eens extra geld kwijt.
3. De koper vraagt je om geld voor te schieten voor bv. transportkosten. Dit moet je betalen via een alternatief betalingssysteem. Hierna verdwijnt de koper en ben je je geld kwijt.
4. De koper stuurt een valse screenshot van de betaling. Je stuurt het artikel op maar ontvangt nooit je geld.

Alarmsignalen:
- Geen discussie over prijs.
- Gebruik van alternatieve betaal- methodes zoals Western Union of Moneygram.
- Contactname via Whatsapp
- Screenshots van betalingen.
- Je moet een bedrag voorschieten.
- Gebruik van tussenpersonen.
- Gebrekkig Nederlands en taalfouten.
- Buitenlands e-mailadres of gsm-nummer.

Tips:
- Geef geen persoonlijke info.
- Verbreek alle contact en betaal niets.
- Stuur niets op voor je het geld ziet.

Mailfraude



Mailfraude is een vorm van oplichting waarbij men e-mails verstuurt vanuit een gehackt of een op het origineel gelijkend e-mailadres, om dan vervolgens betalingen of een levering te vragen. Tevens kan het gaan om facturen die per e-mail verzonden worden met een gewijzigd rekeningnummer om op te betalen.

Alarmsignalen:
- Er is een factuur toegevoegd en je ziet duidelijk dat deze gemanipuleerd werd (Tipp-Ex, doorhalingen, verschillende rekeningnummers, ...)
- Gebrekkig Nederlands en taalfouten.
- Dreigend taalgebruik
- Het e-mailadres of rekeningnummer is niet hetzelfde als gewoonlijk.
- De afzender zendt zijn facturen normaal nooit via e-mail.
- Je verwacht geen factuur van de afzender.
- Je wordt niet persoonlijk aangesproken.
- De e-mail zit reeds in je Spam-folder.

Tips:
- Neem contact op met de afzender (niet via de contactgegevens in de e-mail).
- Geef geen persoonlijke info.
- Verbreek alle contact en betaal niets.

Fraude met vakantiehuizen

De oplichter doet zich voor als eigenaar van een vakantiewoning die te huur wordt aangeboden. Er worden foto's gebruikt van bestaande vakantiewoningen om de schijn van echtheid op te wekken. Ook kan er gebruik worden gemaakt van valse websites. Eenmaal betaald verdwijnt de verhuurder of sta je in het ergste geval in Spanje aan de voordeur van een kantoorgebouw in plaats van aan die mooie vakantiewoning.

Alarmsignalen:
- De prijs is te mooi om waar te zijn.
- Gebrekkig Nederlands en taalfouten.
- Slordige website.
- Korting voor snelle beslissers.
- Gebruik van alternatieve betaal- methodes zoals Western Union of Moneygram.
- De rekening van de verhuurder is afkomstig uit een ander land dan waar de woning staat.

Tips:
- Geef geen persoonlijke info.
- Boek via een erkende organisatie.
- Doe opzoekingen via Google en lees reviews.
- Zoek het adres op via Google Maps.
- Via Google kan je ook zoeken op afbeeldingen. Op de homepage van Google klik je rechtsboven op afbeeldingen. Je kan dan de afbeelding van de woning uploaden of de URL kopiëren. Als je dan op zoeken klikt, krijg je een overzicht van alle pagina's waar de afbeelding voorkomt.
- Verbreek alle contact en betaal niets.

Whaling

Bij whaling doet de oplichter zich voor als een bekende, bv. je zoon of kleindochter, en neemt contact met je op via een onbekend nummer onder het voorwendsel dat zijn/haar GSM kapot of verloren is, dat het originele nummer geblokkeerd is,...
De persoon verklaart in nood te zitten en vraagt om een dringende betaling uit te voeren. Het geld zal nadien zo snel mogelijk teruggestort worden.

Alarmsignalen:
- Gebrekkig Nederlands en taalfouten.
- Een bekende die je via SMS of Whatsapp contacteert om geld te storten? Op zijn minst bizar!

Tips:
- Contacteer de persoon op zijn originele oproepnummer.
- Probeer op een andere manier in contact te komen met de bekende. Via vaste telefoon, via de partner, ...
- Doe nooit de gevraagde betaling. Er is nooit een rekening die niet kan wachten.
- Geef geen persoonlijke info.
- Verbreek alle contact en betaal niets.
- Het kan ook voorvallen dat het originele oproepnummer gehackt werd.

Beleggingsfraude

Bij beleggingsfraude kunnen de oplichters te werk gaan op twee manieren.

1. Een eerste manier is het ongevraagd benaderen van slachtoffers via cold calling of via e-mail met het aanbod om te beleggen in een bepaald product. Uiteraard komt dit samen met de belofte van een verdacht hoog rendement.
2. De tweede manier, dewelke meer en meer voorkomt, is het gebruik van frauduleuze advertenties via sociale media en of volledig opgezette websites.

Eenmaal je je geld hebt geïnvesteerd, hoor je niets meer van de beleggers of beloven ze je het geld terug over te maken als je nogmaals een bedrag stort.

Alarmsignalen:
- Gebrekkig Nederlands en taalfouten.
- Je wordt ongevraagd gecontacteerd.
- Het geboden rendement is te mooi om waar te zijn.
- Buitenlandse websites of tussenpersonen.
- Gebruik van bekende personen.
- Geld overmaken naar het buitenland.
- Vraag om extra betalingen.
- Je moet 'snel belissen'.

Tips:
- Geef geen persoonlijke info.
- Controleer de identiteit van de persoon of het bedrijf.
- Doe geen betalingen naar het buitenland, zeker niet buiten de EU.
- Via www.fsma.be/nl/let-op-voor-fraude kan je via een test nagaan of het om fraude gaat.

Phishing

Bij phishing probeert men achter je bankgegevens te komen door je te lokken naar een valse website, die meestal een kopie is van de echte website. Vervolgens moet je inloggen met je gebruikersnaam en wachtwoord of met je kaartlezer en bankkaart. Hierdoor krijgt de oplichter je gegevens in handen met alle gevolgen van dien.
Meestal worden slachtoffers gelokt via een valse e-mail of bericht namens betrouwbare instellingen zoals banken, overheidsinstanties, de politie, ... In de boodschap staat meestal een link naar een website waar je moet inloggen.

Alarmsignalen:
- Gebrekkig Nederlands en taalfouten.
- Er wordt verwezen naar een site die lijkt op de originele.
- Je wordt niet persoonlijk aangesproken.
- De e-mail zit reeds in je spamfolder.
- De toon is dringend.
- Bericht via Whatsapp.
- Je moet een tool downloaden.

Tips:
- Officiële instanties zoals banken, overheidsdiensten, de politie, itsme, enz. zullen nooit per e-mail of sms vragen om in te loggen, laat staan met behulp van je kaartlezer en bankkaart.
- Geef nooit je pincode en voer geen verrichtingen uit met de kaartlezer.
- Deel in het algemeen nooit je persoonlijke codes of wachtwoorden.
- In plaats van te klikken op een link, zoek je beter zelf naar de juiste website.
- Indien je op de link hebt geklikt en je twijfelt, controleer dan de domeinnaam in de url van de website. Die vind je bovenaan de pagina. Is de domeinnaam, het woord voor .be, .com, .org, .eu, ... en voor de allereerste slash "/", ook echt de naam van de organisatie?
- Staat achter de @ in het e-mailadres de officiële domeinnaam?
- Contacteer de instantie via het officiële telefoonnummer.
- Geef geen persoonlijke info.
- Beantwoord de e-mail of het bericht niet.
- Open de bijlages niet.
- Stuur geen foto's van je bankkaart of identiteitskaart.
- Als je twijfelt, vraag om hulp.

Hacking

Hacking is het inbreken in een computersysteem of netwerk. Dit kan gebeuren door middel van virussen of spyware, maar ook door het kraken van de code van een systeem. Het doel is meestal het systeem over te nemen, gegevens te stelen of het systeem en de gegevens onbruikbaar te maken.
Bij hacking van online accounts gaat het over online accounts zoals e-mail, sociale media, accounts op verkoopsites, ... Dit gebeurt meestal omdat je wachtwoord te simpel is of doordat de hacker het antwoord op je geheime vraag kent. Eenmaal ingebroken in je account kan men gebruik maken van je persoonlijke gegevens, spam versturen in jouw naam, mensen oplichten in jouw naam, aankopen doen of andere criminele feiten plegen.

Alarmsignalen:
- Je systeem of netwerk doet vreemde dingen.
- Je systeem is geblokkeerd.
- Er zijn valse e-mails in jouw naam in omloop.
- Je kan niet meer op je accounts.

Tips:
- Zorg voor een voldoende sterk wachtwoord: ten minste 8 tekens, hoofdletters, kleine letters, symbolen, ...
- Gebruik geen voor de hand liggende paswoorden zoals namen van kinderen, huisdieren, geboortedatum, ...
- Gebruik tweestapsverificatie voor je wachtwoorden
- Zorg voor goede antivirussoftware en laat je systemen regelmatig updaten.

Sextorsion

De oplichter benadert je via sociale media of je hebt hem/haar ontmoet in een chatroom. Jullie beginnen te praten, van het één komt het ander en al snel wordt het gesprek erotisch getint. Jullie delen erotische teksten en ze krijgen je zover dat je compromitterende foto's of videomateriaal van jezelf deelt. Hierna dreigen de afpersers de beelden te verspreiden als je niet met geld over de brug komt.
Wat ook kan gebeuren is dat je een e-mail ontvangt waarin staat dat de oplichter naaktbeelden van je heeft en dat hij deze zal openbaar maken indien je geen som geld overmaakt. Dit is echter niet het geval, maar uit vrees betaal je toch.

Alarmsignalen:
- Gebrekkig Nederlands en taalfouten.
- Vriendschapsverzoeken op sociale media die te mooi zijn om waar te zijn.

Tips:
- Aanvaard geen verzoeken op sociale media van onbekenden.
- Wissel geen erotische content online uit.
- Geef geen persoonlijke info.
- Verbreek alle contact en betaal niets.
- Rapporteer de oplichter.

Ransomware

Ransomware is een soort van schadelijke software die je bestanden of zelfs je volledige systeem blokkeert door middel van encryptie. De criminelen geven je vervolgens de keuze om zaken te doen met hen of afscheid te nemen van je bestanden.

Ransomware komt meestal binnen via een e-mail met een geïnfecteerde bijlage. Je kan het echter ook binnen krijgen via pornografische websites of illegale downloadsites. Wanneer je op die bijlage klikt, begint een zogenaamde trojan je bestanden te versleutelen. Vervolgens krijg je een boodschap in beeld waarin vermeld wordt dat je bestanden versleuteld werden. Je wordt dan aangemaand om binnen x-aantal uur een bedrag of bitcoins over te maken om de bestanden terug te ontsleutelen. Doe je dit niet, zijn al je bestanden voorgoed verloren.

Alarmsignalen:
- Een boodschap op je scherm die je meldt dat je systeem geëncrypteerd werd.
- Vreemde e-mails met bijlagen.

Tips:
- Maak back-ups van je bestanden.
- Open geen e-mails of bijlagen van verdachte afzenders.
- Zorg voor goede antivirussoftware.
- Laat je systemen en software regelmatig updaten.
- www.nomoreransom.org

Toch slachtoffer:
- Doe zo snel mogelijk aangifte bij de politie.
- Betaal niets.
- Neem een foto van het scherm.
- Neem een foto van de cryptowallet/Bitcoinadres of rekeningnummer.
- Alle informatie over het besmette systeem.
- Informatie over hoe de besmetting mogelijk is voorgevallen.
- Schakel de computer volledig uit en verbreek connectie met internet en externe harde schijven.
- Soms is het mogelijk om de bestanden te decrypteren. Sommige van deze decryptiesleutels staan op www.nomoreransom.org.

Vriendschapsfraude

Oplichters proberen steeds vaker op de gevoelens van hun slachtoffers in te spelen om hen geld te ontfutselen. De contacten kunnen beginnen op diverse manieren: via een spammail, een datingsite, sociale media, een chatroom, ...
Gedurende enkele weken proberen ze een vertrouwensband op te bouwen en wanneer deze sterk genoeg is vragen ze om geld. Dit geld dient dan zogezegd voor een reis naar België, om kleren te kopen, om voor familie te zorgen, om ziekenhuiskosten te betalen, om een erfenis te krijgen. Noem maar op.
Na het betalen van enkele bedragen blijft het plots stil en besef je dat de persoon nooit heeft bestaan.

Alarmsignalen:
- Gebrekkig Nederlands en taalfouten.
- Vriendschapsverzoeken op sociale media die te mooi zijn om waar te zijn.
- Gebruik van alternatieve betaalmethodes zoals Western Union of Moneygram.

Tips:
- Aanvaard geen verzoeken op sociale media van onbekenden.
- Google de naam van de 'vriend' eens.
- Geef geen persoonlijke info.
- Verbreek alle contact en betaal niets.
- Rapporteer de oplichter.

Wangiri fraude

Je ontvangt een SMS van een buitenlands nummer, meestal in het Frans. Je hebt blijkbaar iets gewonnen en je moet naar een bepaald nummer bellen om de prijs te ontvangen. Een andere methode is dat je wordt gebeld door een buitenlands nummer en nog voordat je kan opnemen stopt het bellen. Ze hopen dan natuurlijk dat je terug gaat bellen.
In beide gevallen gaat het om een duur betaalnummer waar men je zo lang mogelijk aan het lijntje probeert te houden.

Alarmsignalen:
- Gebrekkig Nederlands en taalfouten.
- Gebruik van buitenlandse oproepnummers.
- Computerstemmen en wachtmuziekjes.

Tips:
- Ga niet in op de sms'en.
- Bel niet terug.
- Blokkeer het nummer via je smartphone.

Nigeriaanse fraude

Als potentieel slachtoffer word je gecontacteerd door iemand uit het buitenland die zich uitgeeft als:

- Een erfgenaam van een bekend persoon of een rijke zakenman;
- Iemand die dodelijk ziek is en geen erfgenamen heeft;
- Een bankbediende die een som geld heeft ontdekt die jou toekomt.

Telkens gaat het dus om iemand die over een grote som geld beschikt en dit zogezegd het land uit wil krijgen. Jij krijgt dan een percentage van dit bedrag in ruil voor hulp. Die hulp bestaat uit het voorschieten van een bedrag voor notariskosten, de douane, belastingen, ... Telkens je betaalt, duikt er weer een nieuwe kost op en uiteraard ontvang je zelf nooit iets. Na enkele betalingen hoor je niets meer van de tegenpartij.

Alarmsignalen:

- Een onbekende uit het buitenland die je geld aanbiedt?
- Het gaat meestal om miljoenen euro's of dollars.
- Meestal gaat het om een Afrikaans of Aziatisch land.
- Gebruik van alternatieve betaalmethodes zoals Western Union of Moneygram.
- Je wordt niet persoonlijk aangesproken.
- Gebrekkig Nederlands en taalfouten.

Tips:

- Geef geen persoonlijke info.
- Verbreek alle contact en betaal niets.

Wat als het toch misloopt

Ondanks alle voorzorgen die je neemt, alle voorzichtigheid die je inbouwt en alle informatie omtrent oplichtingen die je hebt, toch kan het zijn dat het misloopt en je het slachtoffer van een oplichting wordt. Je zal niet de eerste zijn en al zeker niet de laatste.
Vaak schamen mensen zich ook om ervoor uit te komen dat ze opgelicht zijn. Echter is het belangrijk om de nodige stappen te ondernemen zodat niet alleen jijzelf geholpen wordt, maar ook dat anderen niet onnodig het slachtoffer worden.

Best maak je een onderscheid tussen het feit of je geld kwijt bent of niet:

Geen geld kwijt?

- Aangifte bij de politie is niet nodig.
- Stuur het valse bericht dat je ontving door naar verdacht@safeonweb.be. Op deze manier kunnen valse websites of e-mailadressen geblokkeerd worden.
- Verander je wachtwoorden indien nodig.

Wel geld kwijt of gehackt?

- Bel onmiddellijk Card Stop (078 170 170) als je betalingsgegevens hebt doorgegeven.
- Contacteer je bank. Mogelijks kan een betaling nog tegengehouden worden.
- Doe aangifte bij de politie.

Wat meebrengen bij je aangifte?

- Laptop en/of smartphone.
- Exacte URL van de frauduleuze website, indien mogelijk een screenshot.
- Screenshots van berichten, mails, sociale media, ...
- Identiteitsgegevens, e-mailadres, rekeningnummer, oproepnummer, ... van de verdachte.
- Overzicht van frauduleuze transacties.
- Informatie van goederen die op jouw naam werden aangekocht.
- Alle andere informatie met betrekking tot de oplichting, beter te veel dan te weinig.

Nuttige links

- www.safeonweb.be - download ook de app zodat je meldingen krijgt van actuele risico's.
- Verdachte mails of berichten kan je doormailen naar verdacht@safeonweb.be.
- Bedrog, fraude of oplichting melden: meldpunt.belgie.be
- www.nomoreransom.org
- www.cert.be
- www.eccbelgie.be
- www.clicksafe.be
- www.cybersimpel.be
- www.veiligonline.be
- www.ccb.belgium.be
- www.safeinternetbanking.be
- www.besafe.be