VRAGENLIJST CYBERCRIME

Zo duidelijk mogelijk invullen wat voor u van toepassing is

Hoe werd u gecontacteerd?

- Via sociale media:
  - Welke toepassing (instagram, facebook, …): ……..
  - Naam en voornaam (al dan niet fictief): ……..
  - Gebruikersnaam: ……..
  - ID-nummers (vb Facebook ID – kan via https://lookup-id.com/ - *zie bijlage.*

  Gelieve een screenshot te maken van het mediaprofiel en bezorgen aan politie

- Via mail:
  - E-mailadres verzender: ……..

  Hoe kan u het juiste mailadres bekomen? Zie bijlage

  Gelieve de mail als bijlage te verzenden naar de politie. (Hoe doet u dat? Zie bijlage)

- Via Whatsapp/telefoon:
  - Telefoon of GSMnr verdachte: ……..

  Kan u printscreens van de gesprekken (met het nummer van de verdachte) bezorgen aan politie?

  Hoe maak ik een printscreen? Zie bijlage.

  Slachtoffer: maak steeds zelf melding bij Whatsapp van het verdachte app-bericht. (Hoe? Open het verdachte bericht, klik op 3 puntjes => rapporteren)

- Via een online-advertentie:
  - Gebruikersnaam die zoekertje geplaatst heeft: ……..
  - Nummer van het zoekertje: ……..
  - Exacte URL van het zoekertje: ……..
  - Datum, inhoud van de advertentie: ……..

  Indien mogelijk een kopie van de advertentie mailen naar de politie.

- Kan u afdrukken/printscreens/foto's maken van de contacten (mailverkeer, berichten, gesprekken, …) en deze bezorgen aan politie (per post of mail) – *Hoe maak ik een printscreen? Zie bijlage)*

Heeft u moeten klikken op een link? ☐ Ja ☐ Nee

- Welke link (de link-tekst): ……
- De exacte URL: ……

Op welke site kwam u terecht als u op de link klikte?

Gelieve de volledige URL van de eigenlijke website te noteren (dus geen short URL zoals bvb tinyrl.com/xxx).

Wat is een URL? Hoe moet ik een URL van een bezochte website opzoeken? Zie bijlage.

- Kan u een afdruk/printscreen bezorgen van de link aan de politie

Werd uw PC overgenomen van op afstand door verdachte met een remote desktop applicatie zoals bv. Anydesk?

☐ Ja ☐ Nee

- Met welk programma (bv. Anydesk of …): ……
- Noteer het unieke ID: ……
- Wanneer (exacte tijdstippen): ……

Heeft u/werd er door verdachte geld overgemaakt? ☐ Ja ☐ Nee

- Is het recent gebeurd?
  - Contacteer onmiddellijk uw bank om de betaling eventueel nog te blokkeren/recupereren
  - Contacteer cardstop om uw kaart te deblokkeren (078/170.170)
- Welke bedragen werden van de rekening gehaald? Totale nadeel: ……
  Graag een opsomming van de verschillende bedragen en wat ermee gebeurd is:
  - Werd er geld overgemaakt naar andere rekeningnummers? Bedrag + naar welk(e) rekeningnummer(s)
    ……
    ……
    ……
    ……
  - Werd er door verdachte geld afgehaald aan een bankautomaat? Zo ja, bedrag + welke bank, locatie automaat, tijdstip afhalingen):
    ……
    ……
  - Werden er aankopen gedaan in online winkels? (bedrag + winkel + tijdstip):
    ……
    ……
    (Zo ja, onmiddellijke contactname met de online winkels teneinde de transactie tegen te houden)
  - Werd er gebruik gemaakt van moneytransmitters (bvb Western Union, Money Gram, …)? Graag bedragen + namen en unieke transactiecodes van money transmitters:
    ……
    ……
  - Werden er betaalkaarten gekocht zoals Paysafecard, Neosurf, …? Noteer de nummers:
    ……
    ……
    Het zijn Prepaid betaalkaarten waarmee je snel en anoniem op websites kan betalen. Hiermee kan je op een volledig anonieme manier online betalen voor internetdiensten, online spellen, kansspelen, websites en meer.
  - Werd er een bedrag overgeschreven naar Paypal? Graag de Paypal account gegevens:
    ……
    ……
  - Werden er bitcoins gekocht? Adres van bitcoin wallets en bitcoin transacties (TX ID):
    ……
    ……
    Een wallet heeft een adres bestaande uit letters en cijfers. Waar kan ik de transactie ID(TXID vinden? Zie bijlage.

- Is het nadeel al (geheel of gedeeltelijk) vergoed (bvb door bank)? ……
- Rekeningnummers (+ vermelding van de bank) van SLACHTOFFER waarvan geld verdween:
  ……
  ……
- Werd er ook geld op uw rekening gestort? ☐ Nee ☐ Ja. Indien ja:
  - Heeft u uw bankkaart nog in uw bezit?……
  - Is de kaart voortdurend in uw bezit geweest?……
  - Kan iemand op de hoogte zijn van uw pincode?……
  - Als u niet meer in het bezit bent van de kaart, in welke omstandigheden bent u de kaart verloren?……
  - Zat de pincode bij de bankkaart?……

  Bezorg rekeningafschriften/printscreens/foto's aan politie

  - Gelieve de frauduleuze verrichtingen aan te duiden op de afschriften.

Werden er voorwerpen verhandeld? ☐ Ja ☐ Nee

- Werd een betaald goed niet of slechts gedeeltelijk geleverd?……
- Werd een geleverd goed niet betaald door verdachte?……
- Werd een bepaalde dienst waarvoor u heeft betaald niet gepresteerd (publiciteit, dakwerken, asfaltering, …)?
  ……

Zo ja:

- Welk voorwerp/dienst: ……
- Heeft u een serienummer(s): ……
- IMEI-nummers: ……
- MAC-adressen: ……
- Accountgegevens van koppelingen met online netwerken (bv. Playstation Network): ……
  ……

Werd er een bestelling geplaatst op uw naam?

- Hoe en wanneer werd de bestelling geplaatst? ☐ In winkel ☐ Online
- Bij welke winkel/bedrijf: ……
  Gelieve bij winkel/bedrijf of provider een kopie van de bestelbon op te vragen en aan de politie te bezorgen

- Welke naam/GSMnr/e-mailadres/adres/IP-adres werd gebruikt door de verdachte bij de aanvraag/bestelling:
  ……
  ……
- Waar werd het goed geleverd? Een afhaalpunt, een winkel of op een thuisadres?
  ……

Werd uw account gehackt? Heeft iemand zich toegang verschaft tot uw account zonder uw medeweten?

- Geeft concreet aan of er schade toegebracht werd en welke:
  ……
- Werden er recent verdachte gebeurtenissen, berichten of personen opgemerkt?
  ……
- Bedrijf:
  - Is er recent iemand ontslagen?
    ……
  - Is er een ICT deskundige bezig met het geval? Zo ja, contactgegevens:
    ……
    Bezorg een kopie van eventuele rapporten van een ICT-dienst/forensische deskundige
- Exacte tijdstippen van de gebeurtenissen (liefst met opgave van de tijdzone):
  ……
- Zijn er telefoonnummers / accounts / … gekoppeld aan het gehackte account?:
  ……
- Juiste gebruikersgegevens van het account (ID nummer / platformaccount (e-mail, gebruikersnaam, …):
  ……
  ……
  Tracht een historiek van de transacties op te lijsten
  Als het mogelijk is: volledige logs / IP-historiek van het gehackte netwerk, server of e-mailaccount en bezorgen aan de politie
  Waar vind ik deze logs terug? (zie bijlage)

Werd er kwaadaardige software op de computer geplaatst die de computer / tablet / smartphone blokkeert?

RANSOMWARE: tracht – indien mogelijk volgende informatie te bekomen:

- Een screenshot of foto van het geblokkeerd scherm en het afpersingsbericht.
- De vermelde campagnenaam (een Ransomware-aanval gaat meestal gepaard met een naam waaronder de aanval gekend is (vb Locky, WannaCry, Bad Rabbit, Cryptolocker, …).
- De extensies van de versleutelde bestanden. *Wat is een extensie => zie bijlage*
- Het adres van de webpagina met verdere instructies.
- Het bitcoin-adres of adres van andere virtuele valuta waarop het losgeld moet betaald worden.
- De achtergebleven digitale sporen van de manier van de besmetting (vb de header van de e-mail).
- Het besmette bestand in de bijlage van de mail die de malware bevat.
- De voorgestelde of gebruikte communicatiekanalen tussen u en de daders.
  Slachtoffer melding maken bij https://www.nomoreransom.org/nl/index.html

Bijlage aan vragenlijst Cybercrime – aangever / slachtoffer

Hoe maak ik een printscreen?

- Met een Windows PC met de knop 'printscreen / prnt scrn" of Win + Shift + S op je toetsenbord; meestal bovenste rij van je toetsenbord. Vervolgens open je Word en druk je Ctrl + V (Ctrl ingedrukt houden terwijl je de V intoetst) of met rechtermuisknop kopiëren en plakken. Een kopie van je schermweergave wordt nu in Word geplakt. Dit document kun je opslaan en meesturen als bijlage.
- Met een Mac: maak je met CMD (appeltje), Shift en 3 een printscreen in Word of andere tekstverwerker plakken.
- Op tablet of smartphone:
    - Android: maak een schermafbeelding door één van de volumetoetsen en de powerknop tegelijk ingedrukt te houden. Na ongeveer 3 seconden flitst het scherm en is je screenshot gemaakt. Je schermafbeelding vind je terug in de galerij.
    - IOS: Bij een Iphone of Ipad druk je één van de volumetoetsen en de thuisknop tegelijkertijd in. Na ongeveer 3 seconden flitst het scherm en is je screenshot gemaakt. Je schermafbeelding vind je terug in de galerij.

Link/URL van een bezochte website opzoeken:

URL staat voor Uniform Resource Locator. Het is het adres van een website. Een URL begint met http(s)//. Iedere website heeft zijn eigen URL, maar ook iedere pagina op die website heeft weer een eigen URL.

Hoe kan ik de juiste URL bekomen?

- Door in de geschiedenis van uw browser te kijken (meestal CTRL + H) of …
- Door met de cursor over de link te gaan die vermeld is in het bericht en dan de link te kopiëren
    - Link kopiëren:
        - PC/laptop: rechtermuisknop drukken en op link kopiëren drukken of op CTRL + C drukken.
        - Tabliet/smartphone: op de link drukken en dan kopiëren selecteren.

Hoe kan je het juiste e-mailadres bekomen?

De mail beantwoorden en noteren/kopiëren welk e-mailadres er dan verschijnt.

Om het risico te verkleinen op het bekomen van een gespooft e-mailadres is het e-mailadres vermeld bij return path en afzender het meest interessante. Een gespooft e-mailadres is een fictief e-mailadres dat zichtbaar is voor de ontvanger, maar aangemaakt is om het echte e-mailadres te verdoezelen.

Hoe een e-mail als bijlage doorsturen?

Een eenvoudige manier is het bericht in bijlage slepen:

- Start uw e-mail programma. Klik op "Nieuw" en kies "e-mailbericht".
- Laat dit e-mailvenster openstaan en zoek het door u ontvangen bericht (vb een spambericht).
- Open het spambericht niet, maar sleep het op het bijlage icoon (of in het onderwerp veld). Het bericht wordt zodoende als bijlage aan uw e-mail toegevoegd.
- Vul bestemmeling en onderwerp in.
- Verstuur het e-mailbericht.

Bovenstaande manier werkt in Outlook en in ander e-mailprogramma's, zoals Thunderbird.

Gmail:

- Selecteer de gewenste e-mails.
- Klik op “meer” (de 3 puntjes bovenaan in de balk) en kies dan “doorsturen als bijlage”.
- Voeg ontvangers toe aan het veld “Aan”. Je kunt ook ontvangers toevoegen in de velden “Cc” en “Bcc”.
- Voeg een onderwerp toe, schrijf je bericht en klik onderaan op “verzenden”.
- Opmerking: als je een bericht als bijlage wilt doorsturen, kun je ook met de rechtermuisknop op een bericht klikken of het bestand slepen en neerzetten in de hoofdtekst van je bericht.

Hoe kan ik een Facebook ID opzoeken?

Een Facebook ID os een uniek nummer dat gekoppeld is aan ELK Facebookaccount. Het bestaat enkel uit cijfertjes (15-tal). Hoe kan ik dit opzoeken?:

- Ga naar het Facebookprofiel waarvan je de ID wil achterhalen.
- Kopieer de URL van het profiel welke je wil opzoeken. Bvb. https://www.facebook.com/PolitieGetevallei.
- Ga naar de website https://lookup-id.com/ Plak de link in de balk en klik op “lookup”.
- Je ontvangt de Facebook-ID. Noteer deze. Dit nummer is heel belangrijk voor het verder onderzoek.

Logs/IP historiek opvragen:

- Voor Google is dit terug te vinden via https://myaccount.google.com/security.
- Facebook: https://www.facebook.com/settings?tab=security&section=session&view.
    - Je Facebook gegevens => activiteitenlogboek => actieve sessies (dubbel klikken).

Waar kan ik de Bitcoin transactie ID (TXID) vinden?

- Dit is afhankelijk van de coins die aangekocht werden.
- Bij onderstaande websites vul je het ontvangstadres is. Je krijgt dan alle transacties te zien die van en naar dit adres zijn gegaan. Boven idere transactie staat de unieke code voor die specifieke transactie, de TXID.
    - voor Bitcoin: http://blockchain.info/
    - voor Ether: http://etherscan.io/
    - voor Litecoi: http://insight.litecore.io/
    - voor Ripple: https://bithomp.com/explorer/
    - voor Bitcoin cash: https://explorer.bitcoin.com/bch

Wat is een bestandsextensie?

Een bestandsextentie of kortweg extensie is een toevoeging aan het eind van een bestandsnaam waarmee aangegeven kan worden om wat voor soort bestand het gaat. Een bestandsextensie bestaat uit 1 of meer letters na de laatste punt in de naam (vb bat, avi, csv, dll, …)