VRAGENLIJST CYBERCRIME

Dringend terug te bezorgen per mail of per post

Ter attentie van: Opsteller : ……

Ingevuld formulier te bezorgen:

Via mail (mailadres opsteller) : ……
Per post aan : Dienst ……
Adres ……
Telnr ……

Identiteit slachtoffer:

Naam : **……**
Geboren te : **…… op ……**
Verblijvende te : **……**
Burgerlijke staat : **……**
Beroep : **……**
Identiteitsdocument en nr.: **……**
Telnr. : **……**
GSM : **……**
E-mail : **……**

Noteer (beknopt) uw relaas der feiten:

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

BIJKOMENDE VRAGEN (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/) : ……
  - *Graag een screenshot 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 gsm-nr verdachte : ……
  - *Kan u printscreens van de gesprekken (met het nummer van verdachte) bezorgen aan politie?*
  - *Hoe maak ik een printscreen? Zie bijlage.*
  - *Slachtoffer: maak steeds zelf melding van het verdachte app-bericht aan Whatsapp.*
  - *(Hoe? Open het verdachte bericht, klik op de 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 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 (per mail of post)**

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

- □ Met welk programma (vb Anydesk of …) : ……
- □ Noteer het unieke Anydesk ID (of ID andere gebruikte applicatie): ……
- □ 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 blokkeren (070/344.344).

□ Welke bedragen werden van de rekening afgehaald? Totale nadeel: ……..
Graag een opsomming van de verschillende bedragen en wat er mee gebeurd is:
- Werd er geld overgemaakt naar andere rekeningnummers? (Bedrag + Naar welke rekeningnummer):
  ……
  ……
  ……
  ……
- 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 gebruikt gemaakt van moneytransmitters (bvb Western Union, Money Gram, …)? Graag bedragen + namen en unieke transactiecodes van money transmitters:
  ……
  ……
- Werden er betaalkaarten gekocht zoals Paysafecard, Neosurf, …. ? Vermeld de nummers:
  ……
  ……
  Het zijn Prepaid betaalkaarten waarmee je snel én 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 (+ vemelding 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 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 (per mail of per post)**
- **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 politie te bezorgen** welke naam/gsm-nummer/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?

- □ Geef 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/forensisch 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 geblokkeerde 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 (bv. 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*

Hoogachtend,

_____

Handtekening slachtoffer/melder

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 op 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. Met CMD + V (CMD-knop ingedrukt houden en letter V indrukken) kun je de 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 drie 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 drie 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 diezelfde 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
  - Tablet/smartphone: op de link blijven drukken en dan kopiëren selecteren

Hoe kan je het juiste mailadres bekomen?

De mail beantwoorden en noteren/kopiëren welk mailadres er dan verschijnt.
(Om het risico te verkleinen op het bekomen van een gespooft e-mailadres is het E-mail adres vermeld bij return path en afzender het meest interessante.)
Een gespooft e-mailadres is een fictief 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-mail venster openstaan en zoek het door u ontvangen bericht (vb. een spam bericht).
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 andere e-mail programma'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, 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 is een uniek nummer dat gekoppeld is aan ELK Facebookaccount. Het bestaat enkel uit cijfertjes (15-tal). Hoe kan ik dit opzoeken?

1. Ga naar het Facebookprofiel waarvan je de ID wil achterhalen
2. Kopieer de URL van het profiel welke je wil opzoeken. Bvb: https://www.facebook.com/politie5418/
3. Ga naar de website https://lookup-id.com/ Plak de link in de balk en klik op "lookup".
4. 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=sessions&view
  - Je Facebook-gegevens -> Activiteitlogboek -> 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. Je krijgt dan alle transacties te zien die van en naar dit adres zijn gedaan. Boven iedere transactie staat de unieke code voor die specifieke transactie, de TXID.

-Voor bitcoin: http://blockchain.info/
-Voor ether: http://etherscan.io/
-Voor litecoin: http://insight.litecore.io/
-Voor ripple: https://bithomp.com/explorer/
-Voor bitcoin cash: https://explorer.bitcoin.com/bch

Wat is een bestandsextensie ?

Een bestandsextensie 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 een of meer letters na de laatste punt in de naam. (vb.bat , avi, csv,dll……)