POLITIEZONE CARMA

VRAGENLIJST CYBERCRIME

Dringend terug te bezorgen per e-mail of per post

Ter attentie van:

Via e-mail (opsteller):
Per post
Dienst:
Adres:

Identiteit slachtoffer

Naam			
Geboorteplaats		Geboortedatum	
Adres			
Burgerlijke staat			
Beroep			
Nummer identiteitsdocumtent			
Telefooon / gsm			
E-mail			

Wat is er gebeurd?

Noteer kort wat er precies is gebeurd

Uitleg vragenlijst

Hieronder vind je de volledige vragenlijst cybercrime van Politiezone CARMA. De bedoeling is dat je de onderdelen invult die voor jou van toepassing zijn. Hieronder vind je de acht hoofdvragen van de lijst. Enkel bij de vragen waar je 'ja' op antwoordt, moet je verderop in het document ook de extra vragen beantwoorden.

Cybercriminaliteit is een heel technische materie. Je gaat dus ook heel wat technische informatie en termen tegenkomen in dit document. Helemaal achteraan geven we wat meer uitleg over de verschillende termen die in deze vragenlijst voorkomen.

1. Hoe werd je gecontacteerd?

Deze vraag moet je altijd invullen

2. Heb je geklikt op een link in een mail, whatsappberichtje, sms-je ...?

☐ Ja ☐ Nee

Ja? Vul de extra vragen bij vraag 2 in
Nee? Ga naar vraag 3

3. Werd je computer overgenomen vanop afstand door de verdachte?

☐ Ja ☐ Nee

Ja? Vul de extra vragen bij vraag 3 in
Nee? Ga naar vraag 4

4. Is er geld van je rekening verdwenen?

☐ Ja ☐ Nee

Ja? Vul de extra vragen bij vraag 4 in
Nee? Ga naar vraag 5

5. Werd er geld op je rekening gestort?

☐ Ja ☐ Nee

Ja? Vul de extra vragen bij vraag 5 in
Nee? Ga naar vraag 6

6. Heb je een product gekocht of verkocht?

☐ Ja ☐ Nee

Ja? Vul de extra vragen bij vraag 6 in
Nee? Ga naar vraag 7

7. Werd er een bestelling geplaatst op je naam?

☐ Ja ☐ Nee

Ja? Vul de extra vragen bij vraag 7 in
Nee? Ga naar vraag 8

8. Werd je account gehackt? Heeft iemand toegang gekregen tot je account zonder dat jij dit wist?

☐ Ja ☐ Nee

Ja? Vul de extra vragen bij vraag 8 in
Nee? Onderteken het document

Bijkomende vragen

Vul zo duidelijk mogelijk in wat voor jou van toepassing is

1. Hoe werd je gecontacteerd? Duid aan

☐ **Via social media**

- Welke (Instagram, Facebook ...)
- ID verdachte (vb. Facebook ID). Dit kan je opzoeken: https://lookup-id.com/
- Naam en voornaam verdachte (al dan niet fictief)
- Gebruikersnaam verdachte

Indien mogelijk, bezorg een screenshot van het profiel aan de politie

☐ **Via e-mail**

- E-mailadres verzender

Bezorg de e-mail aan de politie (hoe je dit kan doen, lees je op pagina 9).

☐ **Via Whatsapp**

- Telefoon- of gsm-nummer van de verdachte

Indien mogelijk, bezorg een printscreen van de gesprekken in Whatsapp aan de politie. Meld verdachte berichten ook aan Whatsapp. Dit kan je doen door het verdachte bericht te openen, op de 3 puntjes te klikken en te kiezen voor rapporteren.

☐ **Via telefoon**

- Telefoon- of gsm-nummer van de verdachte

☐ **Via een online advertentie**

- Gebruikersnaam van de persoon die het zoekertje plaatste
- Nummer van het zoekertje
- Exacte url van het zoekertje
- Datum en inhoud van de advertentie

Indien mogelijk, bezorg een kopie van het zoekertje aan de politie

2. Heb je geklikt op een link?

☐ Ja ☐ Nee

- Welke link (link-tekst)
- De exacte websitelink waarop je terecht kwam (zie pagina 8)

Indien mogelijk, bezorg een screenshot van de website aan de politie

3. Werd je computer overgenomen vanop afstand door de verdachte?

Ja Nee

- Met welk programma (vb. anydesk)
- Noteer het ID van de applicatie
- Wanneer was dit? Exact moment

Indien mogelijk, bezorg een screenshot van de website aan de politie

4. Is er geld van je rekening verdwenen?

Ja Nee

Maak eerst afdrukken van je rekening voordat die wordt geblokkeerd. Contacteer dan onmiddellijk je bank om de betaling eventueel nog te blokkeren of te recupereren. Contacteer ook Cardstop om je kaart meteen te blokkeren (078 170 170). Bezorg zeker zo snel mogelijk rekeningafschriften, printscreens, foto's ... aan de politie. Duid de frauduleuze verrichtingen aan op de afschriften.

- Totaal bedrag dat is afgehaald
- Werd er geld overgeschreven naar andere rekeningnummers? Hoeveel en naar welke rekening? Bezorg afschrift
- Werd er geld afgehaald aan een bankautomaat? Bedrag, welke bank, locatie automaat, tijdstip ...
- Werden er aankopen in online winkels gedaan? Bedrag, winkel, tijdstip ... Neem contact op met de winkel om de bestelling on hold te zetten.
- Werd gebruik gemaakt van moneytransmitters (vb. Western Union, Money Gram ...)? Bedrag, namen en transactiecodes ...
- Werden er betaalkaarten gekocht zoals Paysafecard, Neosurf ...? Vermeld de nummers
- Werd er een bedrag overgeschreven naar Paypal? Vermeld de Paypal account gegevens.
- Werden er bitcoins gekocht? Adres van bitcoins wallets en bitcoin transacties vermelden
- Is het geld vergoed of is de betaling tegengehouden door de bank?
- Rekeningnummer waarvan het geld verdween en vermelding van de bank

5. Werd er geld op je rekening gestort?

☐ Ja ☐ Nee

- Heb je je bankkaart nog in je bezit?
- Heb je je bankkaart heel de tijd bij jou gehad?
- Kan iemand op de hoogte zijn van je pincode?
- Als je je bankkaart niet meer hebt, waar en wanneer ben je hem verloren?
- Zat je pincode bij je bankkaart?

Bezorg rekeningsafschriften, printscreens, foto's ... aan de politie. Duid de frauduleuze verrichtingen aan op de afschriften.

6. Heb je een product gekocht of verkocht?

☐ Ja ☐ Nee

- Heb je betaald en het product niet of maar gedeeltelijk ontvangen?
- Heeft de verdachte niet betaald voor je geleverde product?
- Heb je betaald voor een dienst die niet geleverd werd? (vb. publiciteit, dakwerken, asfaltering ...)
- Welk voorwerp of welke dienst heb je gekocht of verkocht?
- Heb je een serienummer?
- Heb je een IMEI nummer?
- Heb je een MAC-adres? https://www.hcc.nl/kennis/vraag-van-de-week/3779-wat-is-het-mac-adres-precies
- Heb je accountgegevens van koppelingen met online netwerken? (vb. Playstation Network)

7. Werd er een bestelling geplaatst op je naam?

☐ Ja ☐ Nee

- Gebeurde de bestelling in een winkel of online?
- Bij welke winkel of bedrijf werd de bestelling geplaatst?
- Welke naam, gsm-nummer, e-mailadres, adres, IP-adres werd gebruikt door de verdachte om de bestelling te plaatsen?
- Waar werd het geleverd? Een afhaalpunt, een winkel of een thuisadres?

Neem onmiddellijk contact op met de winkel in de hoop de bestelling on hold te kunnen zetten. Vraag bij de winkel of het bedrijf een kopie op van de bestelbon en bezorg dit aan de politie.

8. Werd je account gehackt? Heeft iemand toegang gekregen tot je account zonder dat jij dit wist?

☐ Ja ☐ Nee

- Is er schade? Welke?
- Heb je verdachte gebeurtenissen, berichten of personen opgemerkt?
- Exacte tijdstippen van de gebeurtenissen
- Zijn er telefoonnummers of andere accounts gekoppeld aan het gehackte account?
- Gebruikersgegevens van het account (ID nummer, e-mailadres, gebruikersnaam ...)
- Werk je voor een bedrijf? Geef even aan of er recent iemand ontslagen is en of een IT'er bezig is met de zaak (noteer zijn contactgegevens)

Indien mogelijk, bezorg de volledige Logs/IP historiek van het gehackte netwerk, de server of het e-mailaccount aan de politie.

Werd er kwaadaardige software geïnstalleerd die je computer, tablet of smartphone blokkeert? Probeer volgende informatie aan de politie te bezorgen:

- Een screenshot of foto van het geblokkeerde scherm en het bericht waarin je wordt afgeperst
- 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
- Het adres van de webpagina met verdere instructies
- Het bitcoin-adres of adres van andere virtuele valuta waarop je losgeld moet betalen
- De achtergebleven digitale sporen van de besmetting (vb. header van de e-mail)
- Het besmette bestand uit de bijlage van de e-mail die de malware bevat
- De voorgestelde of gebruikte communicatiekanalen tussen jou en de dader(s).

Handtekening slachtoffer/melder

Hoe maak ik een printscreen?

Met een Windows-computer

1. Druk op de knop 'print screen', 'PrtScr'. Deze knop staat op de bovenste rij van je toetsenbord. Je kan ook de combinatie Win+shift+s op je toetsenbord gebruiken.
2. Open Word en druk tegelijk op de toets ctrl en v. Of je klikt op je rechtermuisknop en kiest 'plakken'. Je printscreen wordt nu in je Worddocument geplakt.

Met een MAC

1. Druk op de toetsen CMD (appeltje), Shift en 3. Er wordt nu een printscreen gemaakt.
2. Door de toetsen CMD en V in te drukken kan je je printscreen in word of een andere tekstverwerker plakken.

Op je tablet of smartphone (Android)

1. Maak een schermafbeelding door één van de volumetoetsen en de powerknop tegelijk ingedrukt te houden. Na ongeveer drie seconden flitst je scherm en is het screenshot gemaakt.
2. Je afbeelding vind je terug in je galerij

Op je tablet of smartphone (iOS)

1. Druk één van je volumetoetsen en de thuisknop tegelijk in. Na ongeveer drie seconden flitst je scherm en is het screenshot gemaakt.
2. Je vindt de afbeelding terug in je galerij.

Stuur het document of de foto door naar de politie of druk het af en breng het mee naar het commissariaat.

Link/URL van een bezochte website opzoeken

De URL is het adres van een website. Een URL begint altijd met http:// of https://. Elke website heeft zijn eigen URL en elke pagina binnen een website heeft ook een aparte URL.

Hoe kan ik de juiste URL vinden?

1. Kijk in de geschiedenis van je browser (CTRL + H) of door bovenaan in je browser op de drie puntjes te klikken en te kiezen voor 'geschiedenis'.
2. Je kan ook met je muis over de link bewegen die vermeld is in het bericht. Je kan de link kopiëren:
    a. Computer of laptop: rechtermuisknop drukken en klikken op kopiëren of CTRL+C drukken
    b. Tablet of smartphone: op de link blijven drukken en dan kopiëren selecteren.

Hoe kan ik het e-mailadres van de afzender vinden?

1. Open de e-mail
2. Klik op 'beantwoorden'. Het e-mailadres dat nu verschijnt, is het e-mailadres dat je moet invullen.

Hoe kan je een e-mail doorsturen als bijlage?

Algemene e-mailprogramma's

1. Open je e-mailprogramma
2. Klik op 'Nieuw' en kies 'E-mail'
3. Laat dit nieuwe venster openstaan en zoek in je inbox naar de verdachte e-mail
4. Open de verdachte e-mail niet, maar sleep het naar het nieuwe e-mailbericht dat je hebt geopend. Het bericht wordt nu al bijlage toegevoegd.
5. Vul het e-mailadres in van de persoon naar wie je de mail wil sturen
6. Vul het onderwerp in
7. Verstuur de e-mail

Gmail

1. Selecteer de ongewenste e-mail (of meerdere)
2. Klik op 'Meer' (de drie puntjes bovenaan in de balk)
3. Kies 'doorsturen als bijlage'
4. Voeg ontvangers toe bij het veld 'Aan'
5. Vul het onderwerp in
6. Verzend de e-mail

Hoe kan je een Facebook-ID opzoeken?

Een Facebook-ID is een uniek nummer dat gekoppeld is aan elk Facebookaccount. Het bestaat ID bestaat uit 15 cijfers.

1. Ga naar het Facebookprofiel waarvan je de ID wil achterhalen
2. Kopieer de URL van het profiel dat je wil opzoeken
3. Ga naar de website https://lookup-id.com/ en plak de link in de balk en klik op 'lookup'
4. Je ontvangt het Facebook-ID, dit is het nummer dat je moet invullen

Logs/IP historiek opvragen

Voor Google kan je dit terugvinden via https://myaccount.google.com/security
Voor Facebook kan je het opvragen via deze methode

1. Ga naar je Facebookaccount
2. Klik op het pijltje omlaag naast je profiel
3. Kies voor instellingen en privacy
4. Kies activiteitenlogboek

Wat is een bestandsextensie?

Een bestandsextensie of kortweg extensie is een toevoeging aan het einde van een bestandsnaam waarmee wordt aangegeven over welk soort bestand het gaat. Een bestandsextensie bestaat uit een of meerdere letters na de laatste punt in de naam van je bestand. (vb. .bat, .avi, .jpg, .pdf, .csv ...)

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

Dit is afhankelijk van de coins die aangekocht werden. Via onderstaande websites vul je het ontvangstadres in. 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. Dit is 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