CYBER-CRIMINALITEIT

DICHTERBIJ DAN JE DENKT!

Tijd voor een mentaliteits-

SWITCH?

ZEKER EN VAST!

Politie
Sint-Truiden
Gingelom
Nieuwerkerken

MOGELIJKE VORMEN VAN CYBERCRIMINALITEIT

Je woning beveiligen tegen inbrekers vindt iedereen vanzelfsprekend. Dit zou ook zo moeten zijn voor je digitale wereld.
De manier waarop je op het internet surft, contacten onderhoudt met je bank, de overheid of een potentiële partner moet gepaard gaan met een zekere voorzichtigheid.

→ Sociale media (Facebook, Instagram, …)

Kan je niet meer in je eigen account, werden ongevraagd wijzigingen aangebracht (sabotage computersystemen) of heeft iemand ongeoorloofd toegang genomen tot je account/mailbox/website/…?

- *Neem schermafbeeldingen/screenshots!*
- *Waarschuw al je contacten zodat zij niet door de verdachte in de val worden gelokt.*

→ Online betaaldiensten – Fraude betaalmiddelen

Controleer regelmatig je rekeningafschriften. Klopt er iets niet? Contacteer dan de helpdesk van de betrokken betaaldienst en je bank.

- *Zorg dat je de politie de kaart- en rekeningnummer kan meedelen alsook de naam van je bank of online provider en zoveel mogelijk gegevens (e-mail, telefoonnummer, …) van de oplichters.*

→ Phishing via e-mail, WhatsApp, sms, ...

Door phishing trachten criminelen via het internet naar je persoonlijke informatie en bankcodes te hengelen. Zo hopen ze geld afhandig te maken. Denk maar aan een e-mail van je bank om je gegevens en codes in te geven, telefoontjes van Microsoft, e-mails in naam van de politie of gerechtsdeurwaarders.

- *Neem zo snel mogelijk contact op met Card Stop op het nummer 070 344 344 en je bank.*

→ Advertenties en veilingen (2dehands, Marktplaats, eBay, …)

Oplichters blijven nieuwe manieren vinden om te frauderen. De koper doet een bod dat veel hoger is dan de vraagprijs of de koper stelt voor om het ophalen van de spullen te regelen via een koeriersbedrijf.
Je moet echter zelf eerst 100 euro storten.
Ken de verkoper! Ken je product! Ken je betaalmiddel!

- *Neem buiten de politie ook contact op met de verstrekker van de dienst en/of het betaalplatform dat werd gebruikt (Bancontact, Paypal, …) en vraag of ze de gepaste maatregelen kunnen treffen.*

→ Hulpvraagfraude

Je wordt benaderd door iemand die zich uitgeeft voor een kennis, een ouder of een familielid, die dringend hulp nodig heeft. De fraudeurs vragen via e-mail, sms of appberichten om financiële hulp.
Contacteer de betrokkene via een ander communicatieplatform en tracht meer informatie te bekomen met wie je contact hebt.

- *Ook hier kunnen screenshots handig zijn voor als je klacht indient bij de politie. Hou voor de rest alle informatie bij die je wordt meegedeeld (telefoonnummers, e-mail, bankrekeningnummers, …).*

→ Ontoegankelijk gemaakte apparaten/ransomware/hacking

Ransomware is schadelijke software - ook malware genoemd - die door encryptie (versleutelen van de gegevens) je toestel onbruikbaar maakt. Er wordt betaling gevraagd om het toestel te ontgrendelen of om de bestanden terug vrij te geven (decrypteren), maar het is zeker niet gegarandeerd dat dit ook effectief lukt.

- *Neem eerst een schermafdruk (of foto) van het scherm dat je ziet, schakel je computer uit en verbreek de internetverbinding en de connectie met de externe harde schijven.*
- *Vraag desnoods hulp aan een expert om de malware te verwijderen. Deze expert zal je ook kunnen helpen om de back-up terug te plaatsen indien deze nog niet versleuteld werd. Wil je zelf proberen: sommige decryptiesleutels staan gepubliceerd op de website www.nomoreransom.org*

→ CEO-fraude

Een medewerker van een bedrijf of vereniging wordt telefonisch of per mail benaderd (bijv. de penningmeester) en verzocht een dringende financiële transactie uit te voeren. Meestal zijn de verdachten zeer behendig om de urgentie te benadrukken terwijl ze zich voordoen als één van de managers of werknemers.

→ Bedreigingen, belagingen, laster en eerroof

Sociale media is ook een forum geworden om iemand te bedreigen, te belagen dan wel om diens naam door het slijk te halen. Soms worden valse profielen opgesteld.

- *Best is om screenshots te maken van dergelijke berichten gezien de vluchtigheid van het internet.*

→ **Persoonlijk gerichte fraude (vriendschapsfraude, wraakporno, sexting, grooming, cyberpesten, …)**

In het verlengde van het vorige punt (laster, eerroof, bedreigingen, belagingen) is het ook hier van belang om screenshots te nemen van de storende berichten. Als je bijv. gebeld wordt, is het belangrijk om het tijdstip te noteren en het nummer dat de betrokkenen gebruiken. Reageer niet op de e-mails/berichten van de stalker.

- *Ben je in een dergelijke situatie verzeild geraakt als slachtoffer? Onderschat de impact hiervan niet. Praat met iemand die je vertrouwt. Schaam je niet! Stap naar de politie, deze behandelen je probleem uiterst discreet.*
- *Sta ook zelf stil bij wat je post op het net of welke commentaren je geeft.*

NUTTIGE LINKS

Een overzicht van nuttige links in verband met cybercriminaliteit en de preventie ervan, is terug te vinden op onze website:
www.politie.be/5376/vragen/cybercriminaliteit
Deze lijst wordt constant up-to-date gehouden.

Op deze pagina kan je ook de online versie van de brochure terugvinden.

PREVENTIETIPS

- Gebruik een sterk wachtwoord, dus niet ‘1234’ of ‘azerty’ (voor tips zie www.safeoneweb.be). Als het kan, gebruik een tweestaps-verificatie. Dit is bijv. een app op je GSM waarin je moet bevestigen dat je wil inloggen nadat je je wachtwoord hebt ingegeven.
- Gebruik consequent één mailadres voor ‘officiële’ contacten zoals je elektriciteitsleverancier, watergroep, bankcontacten, …
  Voor websites, digitale nieuwsbrieven, klanten-/lidkaarten, …
  gebruik je best een ander.
- Geef nooit gevoelige, persoonlijke informatie of codes door via telefoon of mail.
- Ga nooit in op een vraag van mensen die je niet kent om software op je PC te laten installeren.
  Hiermee zouden criminelen dan jouw PC kunnen overnemen.
- Denk twee keer na voor je iets op het internet plaatst. Wat je deelt op het internet blijft op het internet. (bijv. via de gratis mailprogramma’s!) Dus ook foto’s van jezelf of je kinderen.
- Wees voorzichtig met het openen van links in e-mails. Krijg je een waarschuwing via je e-mail? Ga dan via de rechtstreekse applicatie en log in via gewone weg, niet via de link in je e-mail.
- Zorg dat je computer en de programma’s up-to-date zijn. Een oud slot op je voordeur kan zo gekraakt worden. Een PC die niet meer in orde is met zijn software ook!
- Overweeg een virusscanner aan te schaffen en installeer een firewall.
- Als het te mooi is om waar te zijn, wees dan wantrouwig. Snel geld verdienen, een koper biedt veel meer dan de vraagprijs, een te mooi profiel van je droomprins(es), …

LOOPT HET TOCH FOUT!?

→ Weet dat je niet de enige bent die zich laat beetnemen!
Schaam je niet! Stap naar de politie, deze behandelen je probleem uiterst discreet.

→ Contacteer onmiddellijk je bank als je vreest dat onbekenden aan je bankgegevens (bankcode, Itsme, paypal, …) zijn geraakt. Blokkeer indien nodig je kaart/rekening/… via Cardstop 070 344 344.

→ Koppel je computer of gsm los van het internet. Andere externe apparaten kan je ook best loskoppelen van je computer.

→ Indien mogelijk, hou de communicaties, het elektronisch bewijsmateriaal bij. Neem screenshots van goede kwaliteit en liefst met zo veel mogelijk details van je computer of gsm.
Het internet is zeer vluchtig en soms worden accounts afgesloten nog voor je de kans hebt gehad naar de politie te stappen.

→ Verander je wachtwoorden! Gebruik eventueel de herstelopties om toegang te verkrijgen tot je account en verander zo de wachtwoorden.

→ Heb je een antivirusprogramma? Laat dit lopen op zowel je geïnfecteerd apparaat als op je andere toestellen.

AANGIFTE DOEN VAN EEN ONLINE MISDRIJF?

Maak een afspraak via **WWW.POLITIE.BE/5376** of **011-70 19 10**

LOKALE POLITIE SINT-TRUIDEN – GINGELOM – NIEUWERKERKEN
SLUISBERG 1, 3800 SINT-TRUIDEN
Tel.: 011 70 19 10
E-mail: pz.poltrudo@police.belgium.eu
Website: www.politie.be/5376
Facebook: Lokale politie Sint-Truiden – Gingelom – Nieuwerkerken
Instagram: politie_trudo

Voor dringende politiehulp bel 101.

V.U.: Burgemeester Veerle Heeren, Politiehuis, Sluisberg 1, 3800 Sint-Truiden

Sint Truiden
Gingelom
Natuurlijk Nieuwerkerken
Heerlijk Hospengoed
Politie
Sint-Truiden - Gingelom - Nieuwerkerken