Slachtoffer geworden?

Ben je slachtoffer geworden van een vorm van cybercriminaliteit? Maak een onderscheid tussen "ik ben geen geld kwijt" en "ik ben wel geld kwijt".

Aangifte doen?

Geen geld kwijt?

Aangifte bij de politie is niet nodig.

Stuur het valse bericht door naar verdacht@safeonweb.be. Daar worden ze centraal verzameld en onderzocht.

Op deze manier kunnen frauduleuze websites of e-mail-adressen geblokkeerd worden.

Wel geld kwijt?

Heb je betalingsgegevens doorgegeven? Verwittig onmiddellijk Card Stop op 078 170 170.

Contacteer je bank zodat de laatste betaling of frauduleuze rekening eventueel geblokkeerd kan worden. Doe dit snel, binnen de 24 uur!

Doe aangifte bij de politie. Breng alle nuttige bewijzen mee: zoekertjes, berichten, mails, screenshots, toestel, ...

Contact en afspraak maken

Politiezone Noord (Kapellen - Stabroek)

Christiaan Pallemansstraat 57
2950 Kapellen
03 660 09 30

Maak een afspraak op www.pznoord.be

SCAN ME

Nuttige links

> Download de Safeonweb-app om meldingen te krijgen over actuele risico's. Op www.safeonweb.be vind je ook veel nuttige informatie.

> Verdachte mails of berichten? Stuur ze door naar verdacht@safeonweb.be.

> Kaart verloren, gestolen of betalingsgegevens doorgegeven? Bel Card Stop op 078 170 170.

> Bedrog, fraude of oplichting melden? Surf naar meldpunt.belgie.be

Politie
Noord
Kapellen - Stabroek

Cybercrime

criminaliteit via je gsm, computer of tablet

Wat is cybercrime?

Cybercrime is een overkoepelende term voor misdrijven die gepleegd worden met tussenkomst of gebruik van smartphones, computers en/of netwerken.

Je hoeft zelf geen computer of internetaansluiting te hebben om slachtoffer te worden van computercriminelen. Ook telefoons, bankkaarten, moderne auto's en bedrijfssystemen hebben vandaag computerchips die gemanipuleerd kunnen worden.

Tips om niet in de val te lopen

- ✓ Wat te mooi klinkt om waar te zijn, is het meestal ook.
- ✓ Een officiële instantie zal nooit via e-mail, sms, Whatsapp of telefoon vragen naar je wachtwoord, bankgegevens of andere persoonlijke/gevoelige gegevens.
- ✓ Beveilig je accounts met sterke wachtwoorden en/of tweestapsverificatie.
- ✓ Houd je toestellen up-to-date door software-updates altijd te installeren wanneer ze worden voorgesteld.
- ✓ Installeer antivirussoftware op je computer en hou ook deze up-to-date. Installeer op je smartphone of tablet enkel applicaties uit de officiële appstores (Google Play en Apple Store).
- ✓ Deel geen intieme beelden van jezelf via internet en al zeker niet met mensen die je niet (persoonlijk) kent.

Phishing

Cybercriminelen sturen valse berichten met links naar hun websites. Via dreigende taal, of met aanbiedingen die te mooi zijn om waar te zijn, lokken ze je in de val zodat je op hun link klikt. Zo kunnen ze jouw persoonlijke gegevens en bankgegevens stelen, je accounts overnemen of je rekeningen plunderen.

Emotiefraude

Oplichters spelen in op de gevoelens van hun slachtoffers om hen geld te ontfutselen.

Bij vriendschapsfraude komt het slachtoffer in contact met de oplichter via spammail, een datingsite, sociale media, ... Nadat er een vertrouwensband is opgebouwd, vraagt de persoon om geld: voor een reis naar België, om kleren te kopen, om de hospitaalkosten van het dochtertje te betalen, om een erfenis vrij te krijgen, ...

Bij SOS-fraude ontvang je een bericht van "je zoon" of "je dochter" met een nieuw gsm-nummer en de vraag om dringend wat geld over te maken.

Datasabotage en hacking

Je computer wordt geblokkeerd door een (al dan niet echt) virus. Criminelen vragen losgeld om je gegevens terug vrij te geven.

Bij hacking verkrijgen oplichters toegang tot je account en kunnen ze berichten verspreiden in jouw naam. Dat kan zijn om financieel voordeel te halen, maar het kan ook om een vorm van pesten of laster gaan.

Sextortion

Sextortion is een ander woord voor seksuele afpersing. Slachtoffers worden op het internet overtuigd om intieme beelden van zichzelf door te sturen. Daarna dreigen de afpersers de beelden te verspreiden als het slachtoffer niet met geld over de brug komt.

Aankoopfraude

Kijk uit voor oplichters op online verkoopsites. Herken je een van de situaties? Wees dan zeker waakzaam en stop de verdere afhandeling van de koop.

- Er wordt gevraagd de verkoop af te handelen buiten de zoekertjessite.
- Er wordt gevraagd te betalen via een pakjes- of transportbedrijf.
- Er wordt gevraagd een bankverificatie te doen.
- De koper biedt je een hoger bedrag aan dan je vraagt.
- Er wordt gevraagd een voorschot te betalen om de verkoop te bevestigen via Western Union of Moneygram.

Spoofing

E-mail spoofing is het verzenden van e-mails waarbij het e-mailadres van de afzender vervalst wordt. Dat wil zeggen dat de eigenlijke afzender bijvoorbeeld je eigen e-mailadres kopieert en gebruikt om je om de tuin te leiden.

Dit zijn enkele veel voorkomende vormen van cybercriminaliteit, er bestaan (en ontstaan er elke dag) nog meer.