Politie
Gent

CYBERCRIME

HOE CYBERCRIME VERMIJDEN & WAT DOEN ALS JE TOCH SLACHTOFFER BENT

OPLICHTING MET INTERNET

Preventief:

- Wat te mooi is om waar te zijn, is meestal niet waar.
- Wees op je hoede als een onbekende Western Union, Moneygram, ... voorstelt.
- Geef geen identiteits- of bankgegevens aan onbekenden.
- Contacteer eventueel de klantenservice van de desbetreffende organisatie/website alvorens een contract af te sluiten.
- Zorg dat je goed op de hoogte bent van de advertentie en wie de verkoper is.
- Er bestaan verschillende publieke bronnen om de betrouwbaarheid van een website na te gaan (bv. doe-de-webshop-check op www.eccbelgie.be).
- Op www.infoshopping.be vind je goede praktijken in e-commerce.

Toch slachtoffer?

- Dien klacht in bij de FOD Economie (https://meldpunt.belgie.be). Breng een afdruk hiervan mee naar de politie als je aangifte doet.
- Consumentenlijn: 0800/120 33.
- Dien klacht in bij het Europees Centrum van de Consument (www.eccbelgie.be).
- Betaling via PayPal? Dien klacht in via www.paypal.com.
- Contacteer je bank en probeer een terugbetaling te bekomen.
- Bekijk de helpdesk van de website zelf.

MISBRUIK BETAALKAARTEN

Preventief:

- Controleer regelmatig je rekeninguittreksels.
- Bewaar je geheime code nooit bij je betaalkaarten.
- Informeer je goed als je een betaalkaart aanschaft.
- Een bank zal nooit telefonisch of via e-mail vragen om persoonlijke gegevens of codes.
- Bij twijfel contacteer je lokaal bankkantoor via een vertrouwd kanaal.

Toch slachtoffer?

- Dien klacht in bij de FOD Economie (https://meldpunt.belgie.be). Breng een afdruk hiervan mee naar de politie als je aangifte doet.
- Bel CARD STOP: 078 170 170.
- Neem contact op met je bank en bezorg hen ook het proces-verbaal van je aangifte.

SKIMMING

Preventief:

- Controleer regelmatig je rekeninguittreksels op verrichtingen die je niet zelf verricht hebt.
- Let op voor verdachte voorwerpen rond geldautomaten.

Toch slachtoffer?

- Bel CARD STOP: 078 170 170.
- Neem contact op met de bank in kwestie en eventueel je eigen bank.
- Contacteer je bank en probeer een terugbetaling te bekomen.

VALS PROFIEL

Preventief:

- Zorg voor een goed paswoord (zie tips op www.safeonweb.be).
- Stel je persoonlijke gegevens zo min mogelijk ter beschikking op internet.
- Versnipper persoonlijke documenten voor je ze weggooit.
- Geef identiteitsdocumenten nooit zomaar aan onbekenden.
- Let op met wat je blootgeeft op sociale media.

Toch slachtoffer?

- Neem contact op met de beheerder van de website en maak duidelijk dat een nepprofiel van jou te vinden is. De beheerder zal verder zelf de nodige stappen ondernemen.
- Stel het elektronisch bewijsmateriaal veilig en verzamel zoveel mogelijk intacte informatie/sporen.

SABOTAGE & VIRUSBESMETTING

Preventief:

- Verschillende open bronnen analyseren je bestanden op virussen (bv. www.virustotal.com).
- Maak regelmatig een back-up van je gegevens.
- Zorg voor een goed paswoord (zie tips op www.safeonweb.be).
- Zorg voor een goede antivirus, firewall en anti-spyware.

Toch slachtoffer?

- Koppel het besmette systeem los van het internet.
- Contacteer een gespecialiseerde computerzaak voor hulp.
- Er bestaan verschillende open bronnen om zelf virussen te verwijderen (bv. www.virusalert.nl).

LASTER EN EERROOF OP HET INTERNET

Preventief:

- Beschuldig niemand onterecht wanneer je geen bewijzen hebt.
- Beschuldig niemand onterecht van iets waarvan je zelf ook niet onterecht beschuldigd wil worden.
- Wees voorzichtig met wat je verkondigt op het internet.

Toch slachtoffer?

- Stel het elektronisch bewijsmateriaal veilig voor je de computer reset (naam Facebook account, ID, e-mailheader, print screen, schakel eventueel een deurwaarder in).
- Verzamel zoveel mogelijk intacte informatie/sporen die naar de eventuele dader kunnen leiden en geef deze aan de politie.

CYBERSTALKING

Preventief:

- Geef nooit persoonlijke informatie (bv. woonplaats, telefoonnummer, ...) door aan onbekenden.
- Ga geen anonieme discussies aan.
- Scherm je e-mailadres af voor onbekenden.

Toch slachtoffer?

- Bewaar het bewijsmateriaal dat de stalker kan identificeren (naam Facebook account, ID, e-mailheader, print screen, schakel eventueel een deurwaarder in)
- Maak de stalker duidelijk dat de stalking ongewenst is en dat hij de stalking onmiddelijk dient te stoppen.
- Contacteer je telecom- of internetoperator en meld de feiten.
- Schrijf je uit van de mailinglijst, website, groep, ... waar de stalking plaatsvindt.
- Verander je e-mailadres, gsm-nummer.

HACKING

Preventief:

- Zorg voor een goed paswoord (zie tips op www.safeonweb.be).
- Zorg voor een goede antivirus, firewall en anti-spyware.
- Lees de algemene regels en voorwaarden van de website.
- Ga er van uit dat niemand is wie hij zegt dat hij is.
- Wees voorzichtig met het klikken op verdachte links en bijlagen, deze kunnen besmette software bevatten die kan dienen om je computer te hacken.
- Onbekende afzender = VERWIJDEREN.

Toch slachtoffer?

- Er bestaan verschillende open bronnen die oplossingen bieden (bv. www.safeonweb.be/nl/eerste-hulp).
- Raadpleeg de helpdesk van de site (bv. www.facebook.com/help/hacked, help.yahoo.com, support.microsoft.com, support.google.com).
- Koppel het gehackte systeem los van het internet.
- Verander je paswoorden zo snel mogelijk indien dit nog kan.

Bij elke vorm van cybercrime doe steeds aangifte bij de politie van je woonplaats.

NUTTIGE LINKS

www.safeonweb.be
www.polfed-fedpol.be
www.hoaxbuster.com
www.saferinternet.be
www.clicksafe.be
www.veiligonline.be
www.safeinternetbanking.be
www.internetsporen.nl

Gebaseerd op bijlage OBOV2014012 - Parket OVL.

Politie Gent

Antonius Triestlaan 12
9000 Gent
09 266 61 11

www.politiegent.be
@GentseFlikken

Politie
Gent

01/2022 - VU PZ Gent, Antonius Triestlaan 12, 9000 Gent