



BROCHURE PREVENTIE & REMDIËRING VOOR SLACHTOFFERS CYBERCRIME



OPLICHTING VIA INTERNET

Preventief:

- Wat te mooi is om waar te zijn is meestal niet waar
- Wees op uw 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 te contracteren
- Zorg dat u 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 (vb. consulteer HOWARD op www.eccbelgie.be)
- www.polfed-fedpol.be, www.infoshopping.be

Remediëring:

- Klacht indienen bij FOD Economie (www.economie.fgov.be/nl/geschillen)
- Consumentenlijn: 0800/120.33
- Maak een melding op www.consumentenbedrog.be
- Klacht indienen bij het Europees Centrum van de Consument (www.eccbelgie.be)
- Betaling via PayPal? Dien daar klacht in via www.paypal.com
- Contacteer uw bank en probeer een terugbetaling te bekomen
- Bekijk de helpdesk van de website zelf

MISBRUIK BETAALKAARTEN

Preventief:

- Controleer regelmatig uw bankuittreksels
- Bewaar uw geheime code nooit bij uw betaalkaarten
- Informeer u goed als u een betaalkaart aanschaft
- Een bank zal nooit online vragen om persoonlijke gegevens of codes

Remediëring:

- Klacht indienen bij de FOD Economie (www.economie.fgov.be/nl/geschillen)
- Bel CARD STOP: 070/344.344
- Neem contact op met uw bank + bezorgen ook het proces-verbaal van aangifte

SABOTAGE + VIRUSBESMETTING

Preventief:

- Verschillende open bronnen analyseren uw bestanden op virussen (vb. www.virustotal.com, ...)
- Maak regelmatig een back-up van uw gegevens
- Zorg voor een goed paswoord (zie vb. www.cert.be)
- Zorg voor een goede anti-virus, firewall en anti-spyware (vb. www.mcafee.com, www.norton.com, www.lavasoft.com, www.zonelabs.com)

Remediëring:

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

LASTER EN EERROOF OP HET INTERNET

Preventief:

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

Remediëring:

- Stel het elektronisch bewijsmateriaal veilig voor u de computer reset (naam Facebook account, ID, 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

VALS PROFIEL + VALSE NAAMDRACHT

Preventief:

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

Remediëring:

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

SKIMMING

Preventief:

- Controleer regelmatig uw bankuittreksels of er geen verrichtingen gebeurd zijn die u niet zelf verricht heeft
- Let op voor verdachte voorwerpen rond geldautomaten

Remediëring:

- Bel CARD STOP: 070/344.344
- Neem contact op met de bank in kwestie en eventueel uw eigen bank
- Maak een melding op www.consumentenbedrog.be
- Contacteer uw bank en probeer een terugbetaling te bekomen

HACKING

Preventief:

- Zorg voor een goed paswoord (zie vb. www.cert.be)
- Zorg voor een goede anti-virus, firewall en anti-spyware (vb. www.mcafee.com, www.norton.com, www.lavasoft.com, www.zonelabs.com)
- 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 bijlages, deze kunnen besmette software bevatten die kan dienen om uw computer te hacken
- Onbekende afzender? → DELETEN

Remediëring:

- Er bestaan verschillende open bronnen die oplossingen bieden (vb. www.pepermunt.net, ...)
- Raadpleeg de helpdesk van de site (vb. www.facebook.com/help/hacked, help.yahoo.com, support.microsoft.com, support.google.com)
- Koppel het gehackte systeem los van het internet
- Verander uw paswoorden zo snel mogelijk indien dit nog kan

CYBERSTALKING

Preventief:

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

Remediëring:

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

Nuttige links:

- www.polfed-fedpol.be
- www.hoaxbuster.com
- www.spamsquad.be
- www.saferinternet.be
- www.clicksafe.be
- www.veiligonline.be
- www.safeinternetbanking.be
- www.web4me.be
- www.internetsporen.nl



Openbare bronnen vormen dikwijls een goed medium om problemen op te lossen, de raadpleging ervan is steeds op eigen verantwoordelijkheid

V.u.: Parket van de procureur des Konings Oost-Vlaanderen
Contactpersoon: Jurgen Coppens, Zwarte Zusterstraat 2-4-6,
9200 Dendermonde