REMEDIËRING

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

VALS PROFIEL + VALSE NAAMDRACHT

PREVENTIEF :

- Zorg voor een goed paswoord (zie v.b. 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.

HACKING

PREVENTIEF

- Zorg voor een goed paswoord (zie v.b. www.cert.be)
- Zorg voor een goede anti-virus, firewall en anti-spyware (v.b. www.macafee.com - www.norton.com - www.zonelabs.com - www.avg.com - www.bitdefender.nl)
- 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 (v.b. www.pepermunt.net, …)
- Raadpleeg de helpdesk van de site (v.b. 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

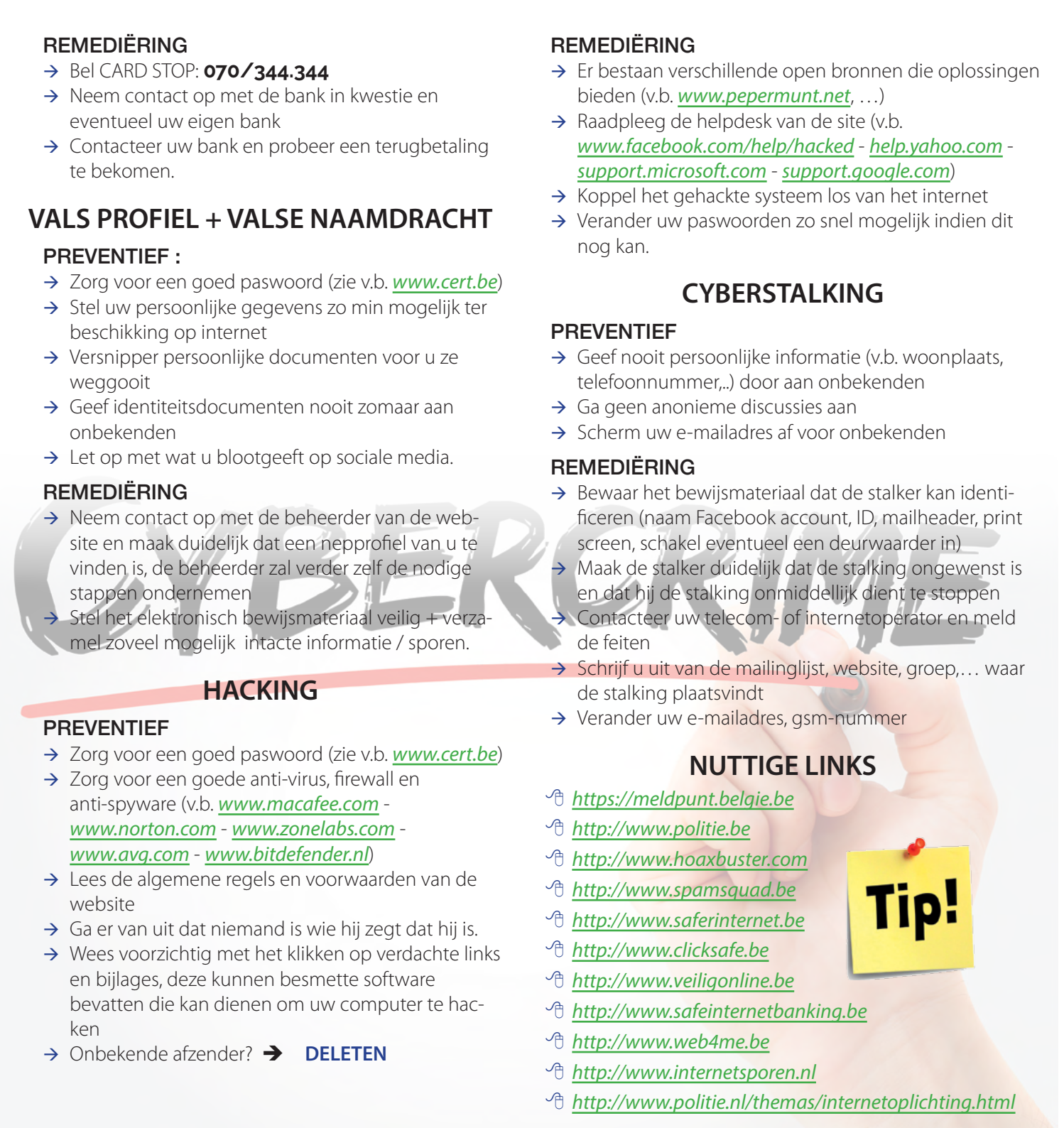
- Geef nooit persoonlijke informatie (v.b. woonplaats, telefoonnummer,..) door aan onbekenden
- Ga geen anonieme discussies aan
- Scherm uw e-mailadres af voor onbekenden

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

- https://meldpunt.belgie.be
- http://www.politie.be
- http://www.hoaxbuster.com
- http://www.spamsquad.be
- http://www.saferinternet.be
- http://www.clicksafe.be
- http://www.veiligonline.be
- http://www.safeinternetbanking.be
- http://www.web4me.be
- http://www.internetsporen.nl
- http://www.politie.nl/themas/internetoplichting.html



openbaar ministerie

Provincie Antwerpen

BROCHURE PREVENTIE & REMEDIËRING VOOR SLACHTOFFERS CYBERCRIME

Geachte burger,

Om de virtuele tuin geleid worden kan grote gevolgen hebben. Cybercriminaliteit kost onze maatschappij jaarlijks 3,5 miljard euro aldus de Belgian Cyber Security Coalition. Het federale cyber emergency team (CERT.be) bevestigt dit cijfer.
Volgens het CERT neemt het aantal gevallen van computerpiraterij onrustwekkend toe. Mobiele technologieën zijn vlot toegankelijk, en bijgevolg extra kwetsbaar voor gerichte aanvallen van doorgewinterde fraudeurs.
Slachtoffers van cybercriminaliteit daarentegen weten zelden bij wie ze moeten aankloppen. Aangifte doen ze helaas niet of weinig. Dat is een van de belangrijkste conclusies van het onderzoek naar internetveiligheid van de KULeuven en de UGent.

Als steeds, voorkomen is zoveel beter dan genezen. Eenvoudige maatregelen zoals bewustwording en preventie kunnen echt wel adequaat zijn om oplichting te vermijden. Deze brochure helpt u daarbij. Nuttige websites en telefoonnummers maken u wegwijs in de problematiek en belangrijker nog, ze bieden u een betrouwbare houvast voor het geval het ook u overkomt.
Maximaal op onze hoede zijn voor oplichters; hun werkwijze herkennen en zo fenomenen als hacking, skimming, cyberstalking maar ook laster en eerroof op het internet maximaal voorkomen, is een opdracht van ieder van ons. Neem dus voldoende tijd om de handige tips en adviezen uit deze brochure aandachtig te lezen en ze, waar en indien nodig, toe te passen. Kortom, informeer u goed en wees alert als u zich op het internet begeeft.

Cathy Berx
Gouverneur
Provincie Antwerpen

Anne-Marie Gepts
Procureur des Konings
Antwerpen

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

V.U.: de procureur des Konings Antwerpen,Bolivarplaats 20 bus 2, 2000 Antwerpen

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 (*www.eccbelgie.be*)
- *www.politie.be* - *www.infoshopping.be*

REMEDIËRING

- Klacht indienen bij FOD Economie (*www.economie.fgov.be/nl/geschillen*)
- Consumentenlijn: **0800/120.33**
- 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 rekeninguittreksels
- 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 FOD Economie (*www.economie.fgov.be/nl/geschillen*)
- Bel CARD STOP: **070/344 344**
- Neem contact op met uw bank + bezorg hen ook het proces-verbaal van aangifte.

SABOTAGE + VIRUSBESMETTING

PREVENTIEF

- Verschillende open bronnen analyseren uw bestanden op virussen (v.b. *www.virustotal.com*, …)
- Maak regelmatig een back-up van uw gegevens
- Zorg voor een goed paswoord (zie v.b. *www.cert.be*)
- Zorg voor een goede anti-virus, firewall en anti-spyware (v.b. *www.mcafee.com* - *www.norton.com* - *www.bitdefender.nl* - *www.avg.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 (v.b. *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, mailheader, ID, 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.

SKIMMING

PREVENTIEF

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