V.U.: Dirk Van Aerschot,
politiezone Geel-Laakdal-Meerhout
Stelenseweg 92 - 2440 Geel

OPLICHTING VIA INTERNET & PHISHING

PROBLEEM

Je werd online opgelicht d.m.v. een valse e-mail, website of bericht.
Je werd online opgelicht via een zoekertjessite.
Jouw bankkaartgegevens werden door derden achterhaald en misbruikt.

PREVENTIEF

1. Wees niet naïef, wat te mooi lijkt om waar te zijn, is dat meestal ook.
2. Handel de verkoop niet af buiten de zoekertjessite.
3. Betaal niet via een pakjes- of transportbedrijf.
4. Stuur nooit identiteitsdocumenten via e-mail door aan onbekenden.
5. Opteer voor afhaling ter plaatse i.p.v. verzending.
6. Vermijd betalingen via geldtransferagentschappen (Western Union, Moneygram).
7. Verwijder verdachte e- mails of berichten van onbekende afzenders.
8. Neem in geval van twijfel telefonisch contact op met je bank.
9. Klik nooit zomaar op verdachte links en bijlagen.
10. Doe aankopen via betrouwbare websites (let op het slotje in de adresbalk).
11. Geef nooit betaalkaartgegevens en/of pincodes door via e-mail.
12. Geef nooit de pincode van jouw betaal– of kredietkaart in op een website.

WAT TE DOEN

- Contacteer je bank zo snel mogelijk om de transactie te blokkeren.
- Bel onmiddellijk CARD STOP: 078 170 170. Probeer een terugbetaling te bekomen via de bank.
- Contacteer de helpdesk van de zoekertjessite zelf.
- Maak melding van de (internet)fraude op: https://meldpunt.belgie.be

SCAMMING

PROBLEEM

Oplichters nemen telefonisch contact met je op en doen zich voor als technici van een computerfirma (Microsoft, Apple, ...). Ze vragen om op je computer bepaalde handelingen uit te voeren en/of je bankgegevens door te geven.

PREVENTIEF

1. Wantrouw telefoons van computerbedrijven die vertrouwelijke informatie of pincodes opvragen.
2. Deel geen identiteits– en/of bankgegevens met onbekenden.

WAT TE DOEN

- Bel onmiddellijk CARD STOP: 078 170 170.
- Neem zo snel mogelijk contact op met je bank.
- Probeer een terugbetaling te bekomen via de bank.
- Bewaar zoveel mogelijk bewijsmateriaal (e-mails, telefoonnummers, betalingsbewijs, ...).

HACKING ACCOUNT

PROBLEEM

Je account werd gehackt waarbij er zonder je medeweten berichten worden verstuurd naar je contactpersonen, berichten of foto's op je account worden geplaatst, ...

PREVENTIEF

1. Gebruik een sterk wachtwoord. Gebruik verificatie in 2 stappen (2FA).
2. Gebruik voor elke account een ander wachtwoord.
3. Deel een wachtwoord nooit met derden.
4. Klik nooit zomaar op verdachte links en bijlagen.
5. Verwijder e-mails of berichten van onbekende afzenders.

WAT TE DOEN

- Verander onmiddellijk je wachtwoord als je nog toegang hebt tot je account.
- Contacteer de helpdesk van de website zelf indien je geen toegang meer hebt.
- Koppel het gehackte systeem los van het internet.

MISBRUIK BETAALKAARTEN & SKIMMING

PROBLEEM

Je pincode wordt achterhaald en vervolgens wordt je bankkaart misbruikt.
Je bankkaartgegevens worden gekopieerd en misbruikt.

PREVENTIEF

1. Bewaar geen pincode bij je betaalkaarten. Controleer regelmatig je rekeninguittreksels.
2. Banken vragen nooit via e-mail vertrouwelijke informatie of pincodes op.
3. Opteer voor een geldautomaat binnen i.p.v. een buitenautomaat.
4. Let op voor verdachte voorwerpen rond de geldautomaat.
5. Scherm altijd je pincode af met de hand.
6. Laat je niet afleiden tijdens de geldtransactie. Meer informatie op https://www.safeinternetbanking.be.

WAT TE DOEN

- Bel onmiddellijk CARD STOP: 078 170 170.
- Neem zo snel mogelijk contact op met je bank.
- Betwist de geldtransactie(s) op: https://www.mijnkaart.be
- Probeer een terugbetaling te bekomen via de bank.

CYBERSTALKING & CYBERPESTEN

PROBLEEM

Je wordt herhaaldelijk via elektronische weg (e-mails, sms, foto's, commentaren, ...) bedreigd, vernederd of lastiggevallen.

PREVENTIEF

1. Deel geen persoonlijke gegevens met onbekenden.
2. Houd je account zo privé mogelijk.
3. Blijf steeds beleefd in je communicatie.
4. Wees voorzichtig met het gebruik van webcams.
5. Negeer vriendschapsverzoeken van onbekenden.

WAT TE DOEN

- Bewaar zoveel mogelijk bewijsmateriaal (e-mails, schermafdrukken, accountnaam, mailheaders, ...).
- Maak melding bij de beheerder van de website.

SABOTAGE & VIRUSBESMETTING

PROBLEEM

Je computer wordt geblokkeerd en je hebt geen toegang meer tot je bestanden.

PREVENTIEF

1. Update regelmatig je software. Installeer antivirus– en firewallsoftware.
2. Maak regelmatig een back-up van je bestanden.
3. Gebruik een sterk wachtwoord.
4. Gebruik verificatie in 2 stappen (2FA).

WAT TE DOEN

- Koppel het besmette systeem los van het internet.
- Installeer een virusscanner en zet deze onmiddellijk aan.
- Zoek antivirussoftware op: https://www.safeonweb.be/ nl/heb-je-een-virus.
- Contacteer een gespecialiseerde computerzaak voor hulp.

VALS PROFIEL

PROBLEEM

Er wordt zonder jouw toestemming een profiel aangemaakt met je identiteitsgegevens en/of je persoonlijke afbeelding.

PREVENTIEF

1. Geef geen identiteitsdocumenten aan onbekenden.
2. Let op met het verspreiden van persoonlijke gegevens via sociale media.
3. Gebruik een sterk wachtwoord.
4. Verspreid geen persoonlijke gegevens via internet.
5. Deel een wachtwoord nooit met derden.

WAT TE DOEN

- Maak melding bij de beheerder van de website.
- Bewaar zoveel mogelijk bewijsmateriaal (accountnaam, afbeeldingen, schermafdrukken, ...).

SEXTORTION & SEXTORTIONSCAM

PROBLEEM

Afpersing waarbij oplichters ermee dreigen om intieme beelden van jezelf te verspreiden indien je geen geldsom betaalt.
Afpersing waarbij oplichters een e-mail sturen waarin wordt beweerd dat ze over intieme beelden van je beschikken die zullen worden verspreid indien je geen geldsom betaalt.

PREVENTIEF

1. Negeer vriendschapsverzoeken van onbekenden.
2. Deel geen seksueel getinte foto's of video's van jezelf.
3. Negeer berichten waarin je wordt afgeperst (hacking / intieme beelden).
4. Scherm je webcam af

WAT TE DOEN

- Ga niet in op de vraag om geld te betalen. Antwoord niet op de e-mail.
- Bewaar zoveel mogelijk bewijsmateriaal (e-mails, berichten, schermafdrukken, ...).
- Markeer het bericht als spam of ongewenst.
- Blokkeer de afzender.

RANSOMWARE

PROBLEEM

Je computer, mobiele apparaten of digitale bestanden worden vergrendeld en er wordt losgeld gevraagd om deze terug te ontgrendelen.

PREVENTIEF

1. Update regelmatig je software. Installeer antivirus– en firewallsoftware.
2. Maak regelmatig een back-up van je bestanden.
3. Verwijder verdachte e-mails of berichten van onbekende afzenders.

WAT TE DOEN

- Koppel het gehackte systeem los van het internet.
- Koppel alle andere toestellen los (USB-sticks, externe harde schijven, ...)
- Bewaar zoveel mogelijk bewijsmateriaal (e-mails, schermafdrukken, ...).
- Ga niet in op de vraag om geld te betalen.
- Zoek gratis de cryptiesleutels op: https:// www.nomoreransom.org/.
- Laat je toestel helemaal opnieuw installeren indien de cryptie niet mogelijk is.

CONTACTGEGEVENS

Politiezone Geel-Laakdal-Meerhout

Stelenseweg 92
2440 Geel

014 56 47 00

pz.glm.preventie@police.belgium.eu

www.pzglm.be

@pzglm en @preventiepzglm

politiezone_glm

Deze brochure is een uitgave van het Team Preventie & Participatie

Veiligheid, een gedeelde zorg
Politie
Geel - Laakdal - Meerhout