CYBERCRIME
SLACHTOFFER

VERDACHTE MAILS?

stuur ze naar:

verdacht@safeonweb.be

NUTTIGE LINKS

www.safeonweb.be
www.cert.be
www.besafe.be/nl/veiligheidsthemas/cyberveiligheid
www.politie.be
https://meldpunt.belgie.be
https://ccb.belgium.be
www.clicksafe.be
www.cybersimpel.be
https://temooiomwaartezijn.be/
www.veiligonline.be

SLACHTOFFER?

Contacteer ons:
Politiezone Zennevallei
Pepingensesteenweg 250
1600 Sint-Pieters-Leeuw

website:
www.lokalepolitie.be/5905

e-mail:
info@politiezennevallei.be

RANSOMWARE

PROBLEEM:

- Uw computer, mobiele apparaten of digitale bestanden werden vergrendeld en er wordt losgeld gevraagd om deze terug te ontgrendelen.

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 decryptiesleutels op: https://www.nomoreransom.org/
- Laat uw toestel helemaal opnieuw installeren indien decryptie niet mogelijk is.

OPLICHTING VIA INTERNET & PHISHING

PROBLEEM:

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

WAT TE DOEN?

- Contacteer uw bank zo snel mogelijk om de transactie te laten blokkeren.
- Bel onmiddellijk CARD STOP: 070/344 344. 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

SEXTORTION & SEXTORTIONSCAM

PROBLEEM:

- U werd overtuigd om intieme beelden van uzelf door te sturen en u wordt nu afgeperst om geld of bitcoins te betalen om verspreiding ervan te voorkomen.
- U ontvangt een e-mail waarin oplichters beweren dat ze intieme beelden van u bezitten en deze zullen verspreiden tenzij u geld of bitcoins betaalt.

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.

SABOTAGE & VIRUSBESMETTING

PROBLEEM:

- U kreeg een melding van een virus op uw computer.
- Uw computer werd geblokkeerd en u heeft geen toegang meer tot uw bestanden.

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.

MISBRUIK BETAALKAARTEN & SKIMMING

PROBLEEM:

- Uw pincode werd achterhaald en vervolgens werd uw bankkaart misbruikt.
- Uw bankkaartgegevens werden gekopieerd en misbruikt.

WAT TE DOEN?

- Bel onmiddellijk CARD STOP: 070/344 344.
- Neem zo snel mogelijk contact op met uw bank.
- Betwist de geldtransactie(s) op: https://www.mijnkaart.be
- Probeer een terugbetaling te bekomen via de bank.

VALS PROFIEL

PROBLEEM:

- Er werd een vals profiel aangemaakt met uw identiteitsgegevens en/of uw persoonlijke afbeelding.

WAT TE DOEN?

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

CYBERSTALKING & CYBERPESTEN

PROBLEEM:

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

WAT TE DOEN?

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

SCAMMING

PROBLEEM:

- U werd opgebeld door oplichters die zich voordeden als technici van een computerfirma Microsoft, Apple ...) en zij vroegen u om bepaalde handelingen uit te voeren en/of uw bankkaartgegevens door te geven.

WAT TE DOEN?

- Bel onmiddellijk CARD STOP: 070/344 344.
- Neem zo snel mogelijk contact op met uw bank.
- Probeer een terugbetaling te bekomen via de bank.
- Bewaar zoveel mogelijk bewijsmateriaal (e-mails, telefoonnummer, betalingsbewijs ...).

HACKING ACCOUNT

PROBLEEM:

- Uw account werd gehackt waarbij er zonder uw medeweten berichten werden verstuurd naar uw contactpersonen, berichten of foto's op uw account werden geplaatst ...

WAT TE DOEN?

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

Dienst Maatschappelijke Veiligheid
Provincieplein 1
3010 Leuven
VLAAMS-BRABANT

Met dank aan de politiezone K-L-M