Nuttige websites:

Is je wachtwoord gelekt?
https://haveibeenpwned.com/

Cybertips Belgische overheid:
https://www.safeonweb.be/

Fraudetips Belgische overheid:
https://temooiomwaartezijn.be

Cybertips PZ Grens:
https://www.pzgrens.be/cybercrime

Een verdachte e-mail, SMS of Whatsapp ontvangen?

Stuur **verdachte mails** door naar:
verdacht@safeonweb.be

Maak van de **verdachte SMS** een schermafdruk en mail door naar verdacht@safeonweb.be

Ben je slachtoffer?

Licht je bank in en dien steeds klacht in bij je lokale politiebureau. Neem alle nuttige documenten mee:

- Bankafschriften
- E-mailberichten en e-mailheaders
- Schermafdrukken van verdachte sociale mediaprofielen
- Schermafdrukken van valse websites
- ...

Zorg zeker dat de adressenbalk er ook opstaat bij schermafdrukken.

Kantoren:

Kalmthout · Kapellensteenweg 32
Essen · Kapelstraat 9
Wuustwezel · Bredabaan 382

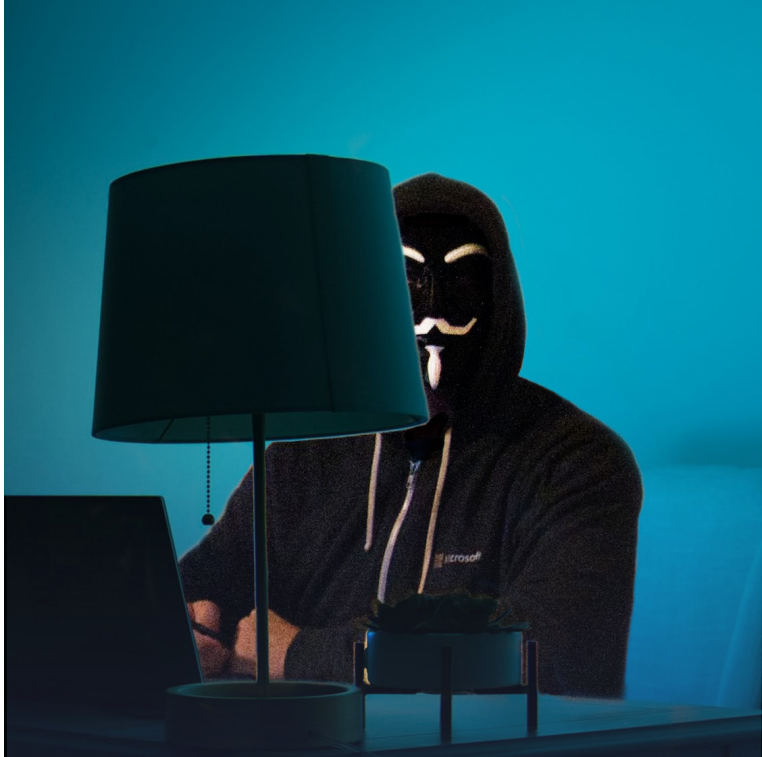
Centraal onthaal: 03/620.29.29
Dringende politiehulp: 101
Ziekenwagen/brandweer: 112

Algemeen:
pz.grens@police.belgium.eu

Cybercrime:
pz.grens.cybercrime@police.belgium.eu

PolitiezoneGrens
politiezonegrens
politiezonegrens

Deze brochure werd opgesteld door PZ Grens, Kapellensteenweg 32, 2920 Kalmthout.



CYBERCRIME

Informatiebrochure

POLITIEZONE
GRENS
Excellente Dienstverlening

Laat het ons eerst heel duidelijk maken: iedereen kan in de val trappen. Dagelijks ontvangt de politie aangiftes van slachtoffers die op een link geklikt hebben in een mail, sms of whatsapp. Ook worden er regelmatig betalingen uitgevoerd naar een verkoper van een tweedehands product waarvan het product nooit ontvangen wordt. Er wordt door onbekenden toegang verkregen tot Facebook waarna er allemaal berichten op verschijnen die niet door het slachtoffer gepost worden, ...

Cybercrime is dus een brede term om uit te drukken dat er een misdrijf is gepleegd met behulp van één of meerdere ICT systemen. Dit kan een computer zijn, een telefoon, een bankkaart, ...

Criminelen weten ook dat bijna iedereen gebruik maakt van het internet om online aankopen te verrichten. De cijfers duiden dat fysieke inbraken en diefstallen in een woning minder vaak plaatsvinden dan online diefstallen en inbraken.

We mogen echter niet bang worden van het internet. Een beetje gezond verstand helpt je vaak om de criminelen te doorgronden en te beseffen dat er iets niet klopt. Is het te mooi om waar te zijn, dan is het te mooi om waar te zijn! Twijfel je toch? Neem dan contact op met een kennis, je bank of zelfs met de politie van je eigen woonplaats.

In deze folder vind je een aantal tips en tricks terug om zelf te achterhalen of je met een online oplichter te maken hebt.

PZ Grens – het cybercrime team

Nuttige tips:

- Geloof niet in (internet) sprookjes!
- Laat je niet opjagen. Denk rustig na en gun jezelf tijd om te evalueren.
- **Open niet elke link/bijlage** in een e-mailbericht. Analyseer eerst het bericht, daarna de bijlage.
- Gebruik steeds **een zoekmachine** zoals Google om namen, adressen, websites, ... te controleren.
- **Gebruik favorieten** voor de websites die je regelmatig bezoekt.
- Stuur nooit foto's van identiteitskaarten, rijbewijzen, bank- of kredietkaarten door naar anderen.
- Hou Windows **up-to-date** en installeer een (gratis) **virusscanner**.
- Wil je aan de slag met **cryptomunten**? Vraag raad aan vrienden of kennissen voor je begint!
- Word je gebeld door je bank en klopt het oproepnummer niet? **Blijf achterdochtig**, geef geen codes en schrijf niet snel geld over. Beëindig het gesprek en bel zelf je eigen kantoor op het door jouw gekende nummer.
- Geef nooit aan iemand je wachtwoord/M1/M2 digipass code, niet via e-mail noch via telefoon. Een bankmedewerker zal hier ook nooit om vragen.
- **Gebruik paswoordzinnen**, zoals bv:"ikGaOpVakant1eMetFacebook" of "ikGaOpVakant1eMetInstagram".
- Heb je een **verdachte e-mail of SMS** herkend? Stuur hem door naar **verdacht@safeonweb.be**.

Doorloop steeds volgende stappen:

1. Tijdsdruk? Zo ja, afbreken!
2. Controleer afzender en "antwoord aan".
3. Controleer het webadres voor je klikt!

Hoe bepaal je het juiste domein van een website?

Je klikt best nooit meteen op een link in een e-mail. Zweef eerst een keer met je muisaanwijzer over de link, op deze manier wordt het echte internetadres zichtbaar.

Laten we het uitleggen met volgend voorbeeld:

- Door te zweven over de link ontdek je dat deze je niet naar mijnburgerprofiel.be brengt. Nee, het brengt je zogezegd naar de website van Politiezone Grens: **https://www.pzgrens.be.nmbvma.me/cybercrime/**
- Check op volgende manier of dit echt de website van de politie is.
  1. Verwijder "http(s)://": **www.pzgrens.be.nmbvma.me/cybercrime/**
  2. Verwijder alles na de eerste "/": **www.pzgrens.be.nmbvma.me**
  3. Behoud enkel datgene voor en na het laatste punt: **nmbvma.me**
  4. nmbvma.me is **niet de originele website** van PZ Grens, **je opent deze link dus beter niet**. Zoek bij twijfel de gewenste site via een zoekmachine zoals Google, Bing,...je zou bijvoorbeeld "website Politiezone Grens" kunnen zoeken op deze manier. Je komt dan uit op: https://www.pzgrens.be. Dit matched niet met het webadres achter de link. **Conclusie: je opent de link best niet!**