

# CYBERCRIME PREVENTIE

## VERDACHTE MAILS?

stuur ze naar:

[verdacht@safeonweb.be](mailto:verdacht@safeonweb.be)



## NUTTIGE LINKS

[www.safeonweb.be](http://www.safeonweb.be)  
[www.cert.be](http://www.cert.be)  
[www.besafe.be/nl/veiligheidstemas/  
cyberveiligheid](http://www.besafe.be/nl/veiligheidstemas/cyberveiligheid)  
<https://meldpunt.belgie.be>  
<https://ccb.belgium.be>  
[www.clicksafe.be](http://www.clicksafe.be)  
[www.cybersimpel.be](http://www.cybersimpel.be)  
<https://temooiomwaartezijn.be/>  
[www.veiligonline.be](http://www.veiligonline.be)

## SLACHTOFFER?

Contacteer ons  
Stationsstraat 292  
1700 Dilbeek

☎ 02 464 12 00

[pz.dilbeek@police.belgium.eu](mailto:pz.dilbeek@police.belgium.eu)

[www.politie.be/5406](http://www.politie.be/5406)



## CYBERSTALKING & CYBERPESTEN

### PROBLEEM:

- Iemand herhaaldelijk lastigvallen, bedreigen of vernederen via elektronische weg (e-mails, sms'en, foto's, commentaren ...).

### PREVENTIEF?

- Deel geen persoonlijke gegevens met onbekenden. Hou uw account zo privé mogelijk.
- Blijf steeds beleefd in uw communicatie. Wees voorzichtig met het gebruik van webcams.
- Negeer vriendschapsverzoeken van onbekenden.

## SABOTAGE & VIRUSBESMETTING

### PROBLEEM:

- Uw computer wordt geblokkeerd en u heeft geen toegang meer tot uw bestanden.

### PREVENTIEF?

- Update regelmatig uw software. Installeer antivirus- en firewallsoftware.
- Maak regelmatig een back-up van uw bestanden.
- Gebruik een sterk paswoord. Gebruik verificatie in 2 stappen (2FA).

## RANSOMWARE

### PROBLEEM:

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

### PREVENTIEF?

- Update regelmatig uw software. Installeer antivirus- en firewallsoftware.
- Maak regelmatig een back-up van uw bestanden.
- Verwijder verdachte e-mails of berichten van onbekende afzenders.

## SEXTORTION & SEXTORTIONSCAM

### PROBLEEM:

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

### PREVENTIEF?

- Negeer vriendschapsverzoeken van onbekenden.
- Deel geen seksueel getinte foto's of video's van uzelf.
- Negeer berichten waarin u wordt afgeperst (hacking/intieme beelden).
- Scherm uw webcam af.

## MISBRUIK BETAALKAARTEN & SKIMMING

### PROBLEEM:

- Uw pincode wordt achterhaald en vervolgens wordt uw bankkaart misbruikt.
- Uw bankkaartgegevens worden gekopieerd en misbruikt.

### PREVENTIEF?

- Bewaar geen pincode bij uw betaalkaarten. Controleer regelmatig uw rekeninguittrekels. Banken vragen nooit via e-mail vertrouwelijke informatie of pincodes op. Opteer voor een geldautomaat binnen i.p.v. een buitenautomaat. Let op voor verdachte voorwerpen rond de geldautomaat.
- Scherm steeds uw pincode af met de hand. Laat u niet afleiden tijdens de geldtransactie. Meer informatie op <https://www.safeinternetbanking.be>.

## OPLICHTING VIA INTERNET & PHISHING

### PROBLEEM:

- Online oplichting via valse e-mails, websites of berichten.
- Online oplichting via een zoekertjessite.
- Oplichting waarbij uw bankkaartgegevens worden achterhaald en misbruikt.

### PREVENTIEF?

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

## VALS PROFIEL

### PROBLEEM:

- Er wordt zonder uw toestemming een profiel aangemaakt met uw identiteitsgegevens en/of uw persoonlijke afbeelding.

### PREVENTIEF?

- Gebruik een sterk paswoord. Verspreid geen persoonlijke gegevens via internet. Deel een paswoord nooit met derden.
- Geef geen identiteitsdocumenten aan onbekenden. Let op met het verspreiden van persoonlijke gegevens via sociale media.

## SCAMMING

### PROBLEEM:

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

### PREVENTIEF?

- Wantrouw telefoons van computerbedrijven die vertrouwelijke informatie of pincodes opvragen.
- Deel geen identiteits- en/of bankkaartgegevens met onbekenden.

## HACKING ACCOUNT

### PROBLEEM:

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

### PREVENTIEF?

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



Dienst Maatschappelijke Veiligheid

Provincieplein 1  
3010 Leuven

Met dank aan de politiezone K-L-M