

Hebt u online een product of dienst gekocht en niet ontvangen waar u voor betaald hebt, ondanks uw herinneringen? Zoek niet verder, u bent helaas het slachtoffer van oplichting.

De definitie van oplichting en de gevolgen ervan zijn opgenomen in artikel 496 van het Strafwetboek.

## Wat moet u doen als u slachtoffer bent geworden?

Dien een klacht in bij een politiecommissariaat, liefst met de volgende informatie:

- referentie van de verrichte overschrijving(en);
- e-mailadres, telefoonnummer en alias gebruikt door de oplichter(s);
- kopieën van uitgewisselde e-mails en/of sms-berichten;
- alle andere informatie die de oplichter(s) zou kunnen identificeren.

Als u uw bankgegevens hebt doorgegeven, breng uw bank dan zo snel mogelijk op de hoogte om de frauduleuze transactie(s) te blokkeren.

**U kunt dit ook doen via Card Stop.**



## Nuttige telefoonnummers

Commissariaten **24u/24, 7d/7** geopend

### Directie Proximiteit en Interventie CENTRUM

Kolenmarkt 30, 1000 Brussel  
02/279.77.11

### LAKEN

Emile Bockstaellaan 246, 1020 Laken  
02/279.88.10

### ELSENE - LOUIZA

Collegestraat 1, 1050 Elsene  
02/279.84.16

### NEDER-OVER-HEEMBEEK/HAREN

Versailleslaan 130, 1120 Neder-Over-Heembeek  
02/279.81.10 & 02/279.89.10

## Nuttige links

**Politie Brussel HOOFDSTAD Elsene**  
[www.polbru.be](http://www.polbru.be)

**Federale Overheidsdienst Binnenlandse Zaken -  
Veiligheid en preventie**  
[www.besafe.be/nl](http://www.besafe.be/nl)

**Safeonweb.be**  
[www.safeonweb.be/nl](http://www.safeonweb.be/nl)

**Jezelf online beschermen is cybersimpel!**  
[www.cybersimple.be/nl](http://www.cybersimple.be/nl)

**Contactpunt voor fraude, bedrog, misleiding en oplichting**  
<https://meldpunt.belgie.be>

# CYBER- CRIMINALITEIT



## Preventie



# Politie

Brussel HOOFDSTAD Elsene

## Enkele tips om u te beschermen



### Antivirus

Installeer antivirussoftware op uw computer.

### Updaten

Werk uw besturingssysteem en antivirussoftware regelmatig bij.

### Back-up

Maak regelmatig back-ups van uw gegevens op een externe schijf.

### Programma's

Installeer alleen programma's of toepassingen die door een officiële website worden verspreid.

### Verdachte bijlagen: niet openen!

### Verdachte links: niet op klikken!

### Privacy

Geef nooit uw persoonlijke gegevens (identiteit, bankgegevens, codes, enz.) aan onbekenden.

### Wachtwoorden

Kies ingewikkelde wachtwoorden met symbolen, cijfers, hoofdletters en kleine letters. Gebruik een wachtwoordbeheerder om ze gemakkelijker te onthouden.

### Bankieren

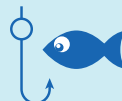
Gebruik de beveiligde browser die beschikbaar is bij uw antivirussoftware. Controleer uw bankafschriften en kredietkaartafschriften regelmatig op frauduleuze transacties.

### Sociale netwerken

Configureer uw privacy-instellingen om uw inhoud te beschermen. Wees ook op uw hoede voor "vriendschapsverzoeken" van onbekenden.

## Enkele voorbeelden van oplichting

### Phishing



Pogingen om toegang te krijgen tot uw vertrouwelijke gegevens door zich voor te doen als een bank of administratie.

### Sextortion of afpersing met gebruik van afbeeldingen met een seksuele inhoud



Oplichters overtuigen u om intieme foto's door te sturen en dreigen dan om ze te verspreiden als u hun geen geld stort. Deel geen intieme foto's op het internet en op sociale netwerken, en zeker niet met onbekenden.

### Misleiding door sextortion



Oplichters beweren dat ze uw computer hebben gehackt en compromitterende foto's van u hebben genomen terwijl u naar een pornofilm kijkt. Ze dreigen ermee deze te verspreiden tenzij u een bepaald bedrag betaalt.

### Ransomware



Schadelijk programma dat wordt gebruikt om losgeld van het slachtoffer te verkrijgen door zijn/haar persoonlijke gegevens achter te houden.

### Cyberstalking



Belaging op het internet of op sociale netwerken die verschillende vormen kan aannemen, zoals het aanmaken van valse profielen, het verspreiden van valse geruchten, beledigende of kwaadaardige berichten.

### Spam



Reclameboodschap die een risico kan inhouden, zoals diefstal van uw vertrouwelijke gegevens (zie phishing), besmetting van uw computer met spyware die in het bericht voorkomt, enz.

### Hacking



Ongeoorloofde toegang tot uw computersysteem voor frauduleuze doeleinden.

### Computerfraude



Bestaat erin goederen of geld van u te verkrijgen door middel van mooie beloften, woorden of voorstellen. Meestal gaat het erom dat het slachtoffer een bedrag betaalt voor iets dat niet bestaat (financiële transacties, loterijen of kansspelen, kopen en verkopen op internet, enz.).

Bepaalde sites zoals 2dehands.be, Facebook Marketplace, enz. zijn favoriete plaatsen geworden voor oplichters.

Meer informatie over oplichting vindt u op de website van de federale politie:

[www.politie.be/5998/nl/nieuws/internetfraude](http://www.politie.be/5998/nl/nieuws/internetfraude)

