# Toolbox: Inspiratie cyberpreventie

ibz Intérieur Binnenlandse Zaken

.be

In deze nieuwe versie van de cyberinspiratiebox krijgt u een niet-exhaustief overzicht van de belangrijkste soorten online oplichting, slachtofferadvies, enkele preventietips, de supralokale organisaties waarbij u terecht kan en enkele inspirerende lokale praktijken. Deze toolbox is in eerste instantie gericht op lokale overheden die weinig vertrouwd zijn met cyberpreventie, maar er wel alsmaar meer mee geconfronteerd worden. Het lokale niveau kan het verschil maken om een integrale aanpak tegen cybercriminaliteit mogelijk te maken.

We wensen u veel leesplezier.

## Belangrijkste soorten online oplichting

### Phishing

Phishing is online oplichting waarbij fraudeurs proberen de bankgegevens en de persoonlijke bankcodes van hun slachtoffers te bemachtigen. Dit doen ze door digitale berichten te sturen met hierin een link naar een valse website, een verdachte bijlage of de vraag om een app te downloaden.

Meer info: https://campagne.safeonweb.be/nl/phishing

### Helpdeskfraude

Vorm van oplichting waarbij fraudeurs doen alsof ze helpdeskmedewerkers van grote, bekende bedrijven zijn (bvb. banken en technologiebedrijven). Ze zeggen dat er zich een groot probleem voordoet en er dringend actie dient te worden ondernomen.

Meer info: https://safeonweb.be/nl/ik-word-opgebeld-door-een-onbekende-voor-een-pc-probleem

### Kluisrekeningfraude

Oplichters benaderen burgers hierbij meestal in twee stappen: ze sturen eerst een phishingbericht om persoonlijke bankcodes te ontfutselen. Zo proberen ze toegang te krijgen tot de bankrekening. Daarna bellen ze de persoon op. Ze doen zich dan voor als een bankmedewerker of Card Stop en vragen om geld over te schrijven naar een zogezegd nieuwe, veilige rekening. Daarbij gaan sommige oplichters zelfs zo ver dat ze bij het potentiële slachtoffer thuis langskomen om de nodige instructies te kunnen geven.

Meer info: https://www.febelfin.be/nl/artikel/kluisrekeningfraude-laat-je-niet-vangen

### Emofraude: Hulpvraagfraude

Fraudeurs geven zich uit voor een bekende/dierbare van hun slachtoffer. Ze vragen via e-mail, sms of appberichten om financiële hulp. Om het vertrouwen te winnen gebruikt men persoonlijke informatie over de bekende/dierbare die men heeft kunnen vinden of kopen (ook wel social engineering genaamd).

Meer info: https://www.febelfin.be/nl/press-room/febelfin-waarschuwt-voor-hulpvraagfraude-waarbij-dierbaren-dringend-financiele-hulp

**Emofraude: Vriendschapsfraude**

Oplichters leggen contact met hun potentiële slachtoffers, waarvan ze vermoeden dat deze eenzaam zijn of een grote nood aan vriendschap/liefde zoeken. In tegenstelling tot de meeste andere vormen van online fraude zal de dader veel tijd investeren om het vertrouwen van het slachtoffer te winnen, waarna men na verloop van tijd geld zal vragen. Daarbij zal een zogezegde noodsituatie vaak als excuus bij deze soort oplichting worden gebruikt.

Meer info: https://temooiomwaartezijn.be/fraude/vriendschapsfraude

**Aan- en verkoopfraude**

Bij aankoopfraude wordt geld overgemaakt naar een persoon of bedrijf zonder de dienst of het product te ontvangen waarvoor is betaald. Bij verkoopfraude worden goederen geleverd, maar betaalt de ontvanger daar niet voor. Tweedehandswebsites zijn daarbij een populaire plaats om deze misdrijven te plegen.

Meer info: https://www.safeonweb.be/nl/kijk-uit-voor-oplichters-op-online-verkoopsites

**CEO-fraude**

CEO fraude is een vorm van oplichting waarbij cybercriminelen een onderneming contacteren (telefonisch of per e-mail) met de vraag een belangrijke betaling uit te voeren naar hun bankrekening. De cybercriminelen nemen de identiteit aan van de CEO, CFO of een vertrouwde persoon en vragen een medewerker van de financiële dienst of boekhouding om een dringende betaling uit te voeren.

Meer info: https://ccb.belgium.be/nl/document/ceo-fraude-beter-voorkomen-dan-betalen

**Investeringsfraude**

Investeringsfraude is de illegale of vermeende verkoop van financiële producten. Typische beleggingsfraude wordt gekenmerkt door fake aanbiedingen van beleggingen met weinig of geen risico, gegarandeerde opbrengsten, overdreven consistente opbrengsten, complexe strategieën of niet-geregistreerde effecten. Daarbij worden potentiële slachtoffers vaak onder enorme druk gezet om snel te beslissen.

Meer info: https://febelfin.be/nl/themas/fraude-veiligheid/online-fraudevormen/beleggingsfraude

**Piramidefraude**

Bij piramidefraude belooft de initiatiefnemer van de piramide de beleggers investeringen met een buitengewoon hoog rendement.

De fraudeur neemt de eerste stortingen in ontvangst van beleggers die zich hebben laten verblinden door de voorgespiegelde winst. Maar in tegenstelling tot wat hen is voorgehouden, belegt hij hun geld niet. Het piramidesysteem houdt in dat de deelnemers zelf nieuwe beleggers moeten aanbrengen, waardoor ze nog meer winst kunnen behalen. Nieuwe beleggers die in het systeem stappen, brengen geld binnen dat alweer niet wordt belegd, maar deels wordt gebruikt om de eerste deelnemers te vergoeden.

Alle beleggers samen vormen zo een piramide. Hoe hoger je in de piramide staat, hoe groter de kans dat je geld verdient. De fraudeurs vallen door de mand als er te weinig nieuwe beleggers bijkomen.

Meer info: https://www.fsma.be/nl/piramidefraude

## Geldezel

Criminelen kunnen gestolen geld niet zomaar op hun eigen rekening laten storten. Dus vragen ze om het eerst op de rekening van een zogenaamde geldezel te zetten, waarna het wordt doorgesluisd.

Geldezels zijn dus mensen die gebruikt worden als tussenpersoon om oplichtingsgeld door te storten. In veel gevallen gaat het om jongeren die snel geld willen verdienen, door hun rekening door derden te laten gebruiken.

Als geldezel ben je strafbaar, want je bent medeplichtig aan fraude en witwaspraktijken. De kans dat je wordt gepakt is zeer groot. De bankrekening is namelijk gekoppeld aan een uniek nummer en de naam van de persoon in kwestie.

Meer info: https://febelfin.be/nl/themas/fraude-veiligheid/geldezels/wat-zijn-geldezels

## Slachtoffers bijstaan

In het geval daders toegang hebben kunnen krijgen tot de bankrekening van het slachtoffer dient deze de volgende instanties te contacteren, in deze volgorde:

1) **Card Stop (078 170 170):**
   - Is 24/7 gratis bereikbaar
   - Bankkaart blokkeren

2) **Bank**
   - Overige betaalmiddelen blokkeren
   - Verkrijgen bewijsmateriaal, in het bijzonder rekeninguittreksels
   - Toegang tot bankapplicatie laten blokkeren: https://cardstop.be/nl/home/ik-wil-blokkeren/Blokkeer-via-uitgever.html
3) **Lokale politie**
   - Om klacht in te dienen, met bewijsmateriaal.
     - Slachtoffers aanraden zoveel mogelijk screenshots te maken.

In het geval er andere persoonlijke gegevens (bvb. gegevens identiteitskaart, paspoort, rijbewijs) in handen van oplichters zijn terechtgekomen, is het essentieel dat slachtoffers hiervan zo snel mogelijk een aangifte doen bij de politie. Daarbij dient bij identiteitsdocumenten Doc Stop (00800 2123 2123 of +32 2 518 2123) gecontacteerd te worden door het slachtoffer.

Meer info: https://www.checkdoc.be/CheckDoc/docstop.do?language=nl

DOC STOP 24/24 00800 2123 2123 +32 2 518 2123

CARD 078 170 170 STOP 24/24

## Belangrijkste preventietips

### Algemeen

Online fraudepogingen zijn alsmaar moeilijker te herkennen. Bij de meeste vormen van online oplichting gebruiken daders een gelijkaardige werkwijze, maar is het vaak verpakt op een andere manier. Door artificiële intelligentie (AI) zijn valse berichten alsmaar moeilijker te herkennen.

De volgende tips van SafeOnWeb kunnen aan burgers worden meegedeeld om verdachte berichten te ontmaskeren:

- **Is het onverwacht?**
  Je krijgt zonder reden een bericht van deze afzender: je kocht niets, had lang geen contact, enz. Controleer zeker verder.
- **Is het dringend?**
  Hou je hoofd koel: kreeg je echt een eerste aanmaning tot betaling? Ken je die 'vriend in nood' wel echt?
- **Ken je de afzender?**
  Controleer het e-mailadres, ook op spellingsfouten. Maar let op: een legitiem e-mailadres is geen garantie.
- **Vind je de vraag vreemd?**
  Een officiële instantie zal je nooit via e-mail, sms of telefoon vragen om je wachtwoord, bankgegevens of persoonlijke gegevens.
- **Naar waar leidt de link waar je moet op klikken?**
  Zweef met je muis over de link. Is de domeinnaam, het woord voor .be, .com, .eu, .org, … en voor de allereerste slash “/”, ook echt de naam van de organisatie?
- **Word je persoonlijk aangesproken?**
  Berichten met algemene en vage aanspreektitels, die wantrouw je beter.
- **Bevat het bericht veel taalfouten?**
  Ook al zorgen doorgewinterde cybercriminelen voor correcte taal: taalfouten of een vreemde taal kunnen wijzen op een verdacht bericht.
- **Zit het bericht in je Spam/Junk folder?**
  Indien ja, wees extra voorzichtig. Je kan ook zelf verdachte berichten markeren als Spam of Junk en zo anderen waarschuwen.
- **Probeert iemand je nieuwsgierig te maken?**
  Iedereen zou nieuwsgierig worden bij berichten met een link zoals "Kijk wat ik over jou las..." of "Ben jij dit op deze foto?", maar laat je niet vangen.

### App

Daarnaast kan ook de SafeOnWeb-app worden gedownload. Deze bezorgt burgers op een laagdrempelige manier preventietips en informeert burgers over actuele dreigingen, zodat ze verdachte berichten sneller leren herkennen. Meer info:
https://www.safeonweb.be/nl/safeonweb-app

***Blijft er twijfel?*** Contacteer de betrokken instanties of organisaties langs de officiële kanalen. Bij twijfel: spreek mensen in jouw omgeving aan en stel de betaling uit tot je volledige zekerheid hebt.

## Verdacht bericht ontvangen

Alsmaar meer burgers zijn alert voor online oplichting en herkennen vele valse berichten. In dit geval kunnen ze worden aangemoedigd om het volgende te doen:

- **Het bericht doorsturen naar verdacht@safeonweb.be**
- Bij twijfel? Niet op linken of bijlages in de e-mail klikken.
- Het bericht niet doorsturen naar andere contacten, tenzij via een screenshot om mensen te sensibiliseren.
- Geef geen persoonlijke gegevens door.
- In het geval een oplichter zich voordoet als een organisatie/bedrijf, raden we aan om de officiële organisatie op de hoogte te brengen. Op die manier kunnen zij hun klanten waarschuwen.

## Emofraude

In tegenstelling tot de meeste vormen van online oplichting, is de werkwijze van digitale emotiefraudeurs enigszins anders. Eerst gaan ze een grondige research van het potentiële slachtoffer doen: dit gebeurt vooral via informatie die men kan terugvinden op sociale netwerken, om voldoende persoonlijke informatie over die persoon te kunnen verkrijgen. Op die manier kunnen ze het slachtoffer op een zeer geloofwaardige manier benaderen.

### Hoe herken je vriendschapsfraude?

Bij vriendschapsfraude gaan de daders vaak veel tijd investeren in online berichten met het slachtoffer. Het doel is om een vertrouwensband op te bouwen met het slachtoffer, omdat de dader vermoed dat het beoogde slachtoffer nood heeft aan vriendschap en/of liefde.

### Hoe herken je hulpvraagfraude?

De daders zullen in dit geval de familie en sociale omgeving van het potentiële slachtoffer onderzoeken om bepaalde informatie te verkrijgen. Deze informatie wordt gebruikt om het vertrouwen van het slachtoffer te winnen. Informatie die men bijvoorbeeld kan nagaan: hoeveel kinderen heeft de persoon? Zijn ze op reis? Hoe heten de huisdieren?

### Volgende preventietips kunnen helpen om emofraude tegen te gaan:

- Wees steeds kritisch bij online contacten en ga zeker niet in op betaalverzoeken, zonder deze persoon in het echt (veilig) te hebben ontmoet.
- Als er iemand in de directe omgeving online vraagt om dringend geld over te schrijven, kan als controlemiddel een videocall worden aangeraden (als fysiek contact onmogelijk is). Schrijf bij grote betalingen nooit over vooraleer deze controle te hebben gedaan, hoe echt het gesprek ook lijkt.
- Om hulpvraagfraude te vermijden kan daarnaast ook worden aangeraden om een vraag te stellen, waarvan het antwoord enkel gekend is door het nauwe contact. Daarbij dient er op gelet te worden dat deze informatie niet op internet te vinden is. Dit is vaak moeilijk, gezien de hoeveelheid informatie die circuleert op sociale media.
- Bij de minste twijfel, schrijf geen geld over.

# Inspirerende lokale praktijken

Het afsluiten van deze inspiratiebox doen we met enkele praktijken die op lokaal niveau kunnen toegepast worden. Van enkele daarvan zijn ondertussen ook al in België initiatieven opgestart.

## Cybervrijwilligers

- Hierbij worden burgers als vrijwilligers ingezet om andere burgers laagdrempelig te sensibiliseren tegen online oplichting. Daarbij is het aangeraden om elke burger in aanmerking te laten komen als cybervrijwilliger. Op die manier kan de informatie op een begrijpbare manier tussen burgers onderling worden meegedeeld.
- Cybervrijwilligers kunnen op verschillende manieren ingezet worden: luisteren naar slachtoffers, infosessies aan scholen/verenigingen en proactief sensibiliseren van kwetsbare personen in de omgeving. Het is daarbij essentieel dat er een kader wordt gemaakt door de lokale overheid, waarin enkele afspraken worden vastgelegd. Zodat de cybervrijwilliger weet wat diens mogelijkheden zijn, maar de lokale overheid ook kan optreden indien er misbruiken zouden voorkomen.
- De vorming tot cybervrijwilliger kan daarbij gegeven worden door de lokale overheden, waarbij een goede afstemming tussen de politiezone en gemeente sterk wordt aanbevolen. De coördinatie van de vrijwilligers gebeurt door de organiserende gemeente/politiezone. Op die manier hebben burgers een officieel aanspreekpunt bij eventuele vragen.
- Op vlak van opleidingsmateriaal kan in eerste instantie verwezen worden naar het materiaal dat reeds door het CCB wordt aangeboden: https://ccb.belgium.be/nl/lesgeven-over-cyberveiligheid . Daarnaast kan u ook op de website van Febelfin ( https://www.febelfin.be/nl ) terecht. Ook kan u de informatie gebruiken die vanuit ADVP (www.besafe.be) wordt aangereikt. Al deze informatie kan tijdens de vormingen gratis gebruikt worden.
- Het is sterk aanbevolen om hierbij beroep te doen op de BuurtInformatieNetwerken (BIN) die in uw gemeente actief zijn. Dit kan een basis zijn om het werken met cybervrijwilligers op te bouwen. Indien dit toch niet mogelijk is, kan gewerkt worden met lokale verenigingen die een interesse hebben om hieraan mee te werken.
    - Voor vragen hieromtrent kan contact worden opgenomen met BIN-Kenniscentrum, die mee de lead hebben van dit project.
- Stimuleer ook jongeren om zich in te zetten als cybervrijwilliger. Maak het aantrekkelijk voor hen. Hierbij kan worden samengewerkt met de diensten en verenigingen die nauw in contact met jongeren staan.
- Bij dit alles is het belangrijk dat de lokale overheid het overzicht kan houden wie er officieel actief is als cybervrijwilliger. Het is daarbij namelijk de bedoeling dat burgers enkel gesensibiliseerd worden. Manipulaties aan toestellen zijn daarbij dus niet aan de orde.

## Lokale samenwerkingen opzetten

Elke lokale overheid beschikt over vele diensten en verenigingen in het grondgebied. Afhankelijk van de organisatie kunnen deze ook ingezet worden bij cyberpreventie.

- Bvb. infosessie in samenwerking met scholen, verenigingen en sociale diensten.
- Bvb. bij de jeugdverenigingen op eigenzinnige wijze aandacht voor online risico's, gekoppeld aan een spel.
- Bvb. beroep doen op een diefstalpreventieadviseur. Deze bijscholingen laten volgen zodat deze tijdens huisbezoeken verdachte berichten herkent en weet wat de burger kan ondernemen als deze slachtoffer is geworden.
- Bvb. de lokale informatiekanalen inzetten om mensen te sensibiliseren.

## Infosessies

- Organiseer een infosessie rond online oplichting in jouw lokale overheid. Dit zal in vele gevallen personen kunnen bereiken die over minder digitale vaardigheden beschikken. Tegelijkertijd zorgt het voor sociale cohesie in de gemeente, doordat inwoners elkaar ook tijdens die avond kunnen leren kennen.
- Zorg voor laagdrempelige informatie, waarvoor geen bijzondere technische voorkennis nodig is. Maak het toegankelijk voor iedereen en zo praktisch mogelijk. Durf daarbij ook in interactie te gaan met het publiek. Dit zal veel informatie opleveren en jou helpen bij het organiseren van toekomstige infosessies.
- Op vlak van informatie kan het opleidingsmateriaal gebruikt worden dat het CCB ter beschikking stelt: https://ccb.belgium.be/nl/lesgeven-over-cyberveiligheid . Daarnaast kan u ook op de website van Febelfin ( https://www.febelfin.be/nl ) terecht. Ook kan u de informatie gebruiken die vanuit ADVP (www.besafe.be) wordt aangereikt.

## Sensibilisering op markt

- Een markt kan een ideale gelegenheid zijn om personen te bereiken die digitaal moeilijk bereikbaar zijn voor lokale overheden.
- Er kunnen daarbij op diverse manieren acties worden opgezet om personen te sensibiliseren rond online oplichting. Daarbij kan er ook gebruik worden gemaakt van flyers/folders, met tips hoe men pogingen tot online oplichtingen kan herkennen en wat men kan doen als men het slachtoffer is.

## Boodschappenzakje met preventietips

- Personen met beperkte digitale vaardigheden bereiken rond cyberpreventie is online niet eenvoudig. Vaak helpen daarbij fysieke acties, zoals een broodzak met preventietips tegen online oplichting. Door samenwerkingen met lokale bakkers kan het doelpubliek beter worden bereikt, de lokale economie worden versterkt en kunnen lokale ondernemers ook hun sociale rol aantonen.
- Combineer zulke actie wel bij voorkeur met andere acties. Op die manier zal meer een sensibiliserend effect mogelijk zijn.

## Educatieve media

- Er zijn alsmaar meer educatieve games op de markt. Dit kan ook zeer nuttig zijn om jongeren te sensibiliseren en hen te bereiken, ook rond online risico's. Zij blijken namelijk ook vatbaar voor verschillende vormen van online oplichting en geweld.
- Ook kan er gebruik gemaakt worden van educatieve tv/video's. Daarbij wordt ingespeeld op de leefwereld van jongeren, maar tegelijkertijd wel met een educatieve boodschap.

## Escape room

- Op maat van jongeren en personen die zeer vertrouwd zijn met het internet.
- Om hun digitale vaardigheden verder aan te scherpen en hen bewust te maken van de impact die online risico's ook op hun leven kunnen hebben. Daarbij dienen tegelijkertijd ook tips gegeven te worden waar men in de online wereld op dient te letten, zonder al te belerend te zijn. Focus daarbij ook steeds op de rol die (online) omstaanders kunnen spelen, leg de verantwoordelijkheid bij de dader(s) en beperk zoveel als mogelijk victim blaming.

Quiz

- Een quiz opstellen waarbij digitale vaardigheden worden aangescherpt. Zo kan er onder meer getraind worden op het herkennen van frauduleuze e-mails.
- Daarbij is het wel belangrijk dat er ook duidelijk wordt gemaakt welke acties de persoon in kwestie wél moet ondernemen als hij te maken krijgt met online oplichters.