

Oplichting via het internet

1. Wat is het?

Internetoplichting of internetfraude is de online variant van de klassieke oplichting: het ontfutselen van persoonlijke gegevens, geld of goederen aan nietsvermoedende personen met leugens, mooie woorden en voorstellen. Ook wanneer iemand daarvoor gebruikmaakt van het internet is er sprake van oplichting. Op www.besafe.be vind je een overzicht van de verschillende vormen van internetoplichting. De meest recent opkomende vorm is 'Microsoft fraude' waarbij slachtoffers worden opgebeld door zogenaamde Engelstalige of gebrekkig Nederlandstalige Microsoft-medewerkers met de smoes dat er (beveiligings)problemen zijn aan hun computer. Als je een bepaalde software download helpen ze vanop afstand. Zo nemen ze echter de computer over en begeleiden het slachtoffer door enkele betalingsschermen waardoor ze de bankkaartnummer en code te weten komen. Ook onder andere firmanamen wordt geopereerd Telenet, 2dehands.be,...

2. Komt het vaak voor?

Volgens cijfers van de Federale Politie steeg het aantal meldingen in Vlaams-Brabant van internetfraude met bijna 30% van 2017 tot 2018. De Veiligheidsmonitor van 2018 toont aan dat het werkelijke aantal feiten wellicht nog heel wat hoger ligt, want slechts 22% van de slachtoffers doet effectief aangifte.

3. Wat zijn de gevolgen?

Volgens de FOD Economie is er tussen januari 2017 en juni 2018 in het totaal 13,6 miljoen euro verloren aan internetoplichting.¹ Met dit geld financieren daders hun criminele organisaties. Slachtoffers van oplichting zijn vaak beschaamd. Ze vragen zich af hoe ze zich zo om de tuin hebben kunnen laten leiden. Ze zijn kwaad en worden wantrouwig.

4. Wat kan je doen?

Sensibiliseer het personeel om de burger steeds door te verwijzen naar www.safeonweb.be. Een websites met zeer duidelijke en nuttige tips. De richtlijnen van het centrum voor Cyber Security België zijn duidelijk. Wantrouw altijd telefoonoproepen van bedrijven die vragen om een aantal acties uit te voeren op je computer, laat je computer niet overnemen en voer geen betalingen uit, terwijl een onbekende je computer heeft overgenomen.

Sensibiliseer via uw website, sociale media en artikels in het gemeentelijk infoblad en organiseer initiatieven en activiteiten (presentaties, infomomenten, workshops ...) bij lokale clubs, verenigingen, handelaars en bedrijven

Stimuleer effectieve slachtoffers om aangifte te doen via de lokale politie. Gewoon iets verdacht melden kan via <https://meldpunt.belgie.be/meldpunt/>.

¹ VTM nieuws - 05/06/2018

5. Wat biedt de dienst maatschappelijke veiligheid?

- uitwisseling van goede praktijken uit andere gemeenten en politiezones;
- preventietips om te plaatsen in het lokale weekblad, op de website of op sociale media;
- opleidingen voor personeelsleden om hun kennis rond het thema te vergroten in samenwerking met het PIVO;
- zoeken naar of aanreiken van deskundigen die infosessies geven;
- presentaties, documentatie- en informatiemateriaal;
- sensibiliseringsmateriaal zoals brochures en gadgets (onder voorbehoud van beschikbaar budget).

Contactpersoon:

Marleen Piccard

Federale afdeling gouverneur Vlaams-Brabant, dienst maatschappelijke veiligheid

Provincieplein 1, 3010 Leuven

Telefoon: 016 26 78 42

E-mail: dmv.preventie@vlaamsbrabant.be

6. Interessante instanties en websites

Centrum voor Cyber Security België (CCB): www.safeonweb.be

Algemene website van de overheid over cyberveiligheid met informatie en campagnemateriaal. De site verzamelt actuele dreigingen, alsook een reeks tips om veilig te surfen.

Cybersimpel, een gezamenlijk initiatief: www.cybersimpel.be

Een nauwe samenwerking tussen Google en Test-Aankoop. Het promoot een veiliger internet en stimuleert consumenten om zich beter te wapenen tegen de risico's van het wereldwijde web.

Cyber Security Coalitie: www.cybersecuritycoalition.be

Een partnerschap van deskundigen uit de academische wereld, de lokale overheid en de private sector. Op de website kan je de Cyber security KIT downloaden die kleine en middelgrote organisaties helpt om intern te sensibiliseren over cyber security.

Febelfin vzw: www.safeinternetbanking.be

De Belgische federatie van de financiële sector heeft een website over veilig internetbankieren en de meest recente fraudetechnieken. Je vindt er leuke video's over phishing om de burger te sensibiliseren.

De Cyberfraude bewustwordingscampagne: www.cybersecuritycoalition.be

Een gezamenlijke inspanning van Europol, wetshandhavingsinstanties, de Europese Banken Federatie (EBF) en partners van de 'European Cyber Security Month'. Op de website kan je campagnemateriaal (video's en infographics) downloaden over internetfraude.

Te mooi om waar te zijn: www.temooiomwaartezijn.be

Deze website heeft als doel je te waarschuwen voor online oplichting en je te helpen om ze te vermijden. De gulden regel om niet misleid te worden: zorg ervoor dat je weet met wie je te doen hebt. De site werd ontwikkeld door de FOD Economie en ze behandelt onder andere vriendschapsfraude, beleggingsfraude, fraude met cryptomunten én heeft een uitgebreide FAQ ivm deze onderwerpen.

FOD Economie, KMO, Middenstand en Energie: www.economie.fgov.be

De FOD Economie heeft een brochure uitgegeven om de consument te waarschuwen en te sensibiliseren voor de meest voorkomende vormen van bedrog en oplichting. De brochure "Stop bedrog!" is samengesteld uit 36 fiches (vaak gelinkt aan cybercriminaliteit) die u kunt raadplegen en downloaden.