



## Laat je niet voor de gek houden

Verijdel social engineering aanvallen

Brussel, mei 2020

Hallo en welkom allemaal!

### Nieuw bericht [VERTROUWELIJK!]

Je wordt gecontacteerd door je baas die je meedeelt dat de overheid onderzoek voert naar mogelijke fiscale fraude. Er moet snel en in alle vertrouwelijkheid 60.000 euro overgemaakt worden. Vleierij en intimidatie: je gesprekspartner heeft het over je lovenswaardige carrière, je doorgroeimogelijkheden... en over je kinderen. Zonder jouw medewerking zullen de gevolgen niet te overzien zijn...

*Tuin jij erin...?*



Een klassiek scenario van social engineering bij kmo's.



**Let op!**

Een persoon met slechte bedoelingen wil je vertrouwen schenden.

Het is zo'n gesmeerde techniek dat we spreken over 'social engineering': de fraudeur kent je profiel door informatie over jou te bestuderen op het web of de sociale netwerken. Doel? Je waakzaamheid omlaag halen aan de hand van een geloofwaardig scenario, om je de pieren uit de neus te halen of je aan te zetten om te handelen.

## Social engineering

is een heel gesmeerde en zeer opdringerige techniek



### Social engineering... wasda?

---

**Social engineering:**

- Psychologische manipulatie
- Persoonlijke sfeer
- Aannemen van andere identiteit
- E-mail, telefoon, social media

**Doel:**

- Persoonlijke informatie
- Gevoelige gegevens van de onderneming
- Geldtransfer

**Hoe?**

- Verzamelen van informatie
- Geloofwaardig scenario
- Onderzoek, controle, operatie: dringend!

Social engineering of **social hacking** is een frauduleuze techniek die erin bestaat **misbruik te maken van mensen, door in te spelen op typische karaktertrekken** zoals vertrouwen, nieuwsgierigheid, naïviteit, angst, hebzucht, ...

De fraudeur geeft zich uit voor een **vertrouwenspersoon** en gebruikt de **persoonlijke sfeer** van het slachtoffer om zo in het **netwerk van de onderneming** te kunnen inbreken.

Meestal gaat het om een **e-mail, social media** of een **telefoontje**.

#### Het doel?

- Op zoek gaan naar **persoonlijke informatie** (ID, wachtwoorden, kredietkaartnummer).
- Toegang tot **gevoelige gegevens** binnen de onderneming.
- Een **geldtransfer**.

#### Hoe?

- Het nauwkeurig verzamelen van **openbare en privéinformatie** (sociale netwerken), soms gedurende verschillende maanden.
- Opstellen van een goed gesmeerd en **plausibel scenario**.
- Een **onderzoek**, een **controle**, een dringende **operatie**, een **opportuniteit**.

**1 Belgische onderneming op 2**  
wordt vandaag geconfronteerd met cybercriminaliteit

**Cijfers liegen niet...**

De cijfers:

- 70 miljoen euro voor een Belgische bank (CEO-fraude)
- Meer dan 10 miljard euro op wereldschaal (2018)

CYBER SECURITY COALITION.be

5

In België wordt **1 op 2 ondernemingen** geraakt door cybercriminaliteit en technieken van social engineering.

Ongelooflijk! Social engineering kostte reeds **70 miljoen euro aan een Belgische bank**, via zogenaamde CEO-fraude. Volgens Verizon ([2019 Data Breach Report: https://www.helpnetsecurity.com/2019/05/09/verizon-2019-data-breach-investigations-report](https://www.helpnetsecurity.com/2019/05/09/verizon-2019-data-breach-investigations-report)) maken verantwoordelijken in organisaties 12 keer meer kans op een social engineering aanval dan andere medewerkers.

Op wereldschaal loopt de schade veroorzaakt door dit fenomeen op tot **10 miljard euro**. (Bron: FBI - 2018), een verdubbeling op 2 jaar tijd.

Kijk hoe het gebeurt!

Weet je wat men allemaal over jou te weten kan komen aan de hand van de informatie die je online verspreidt?

Bekijk de video

 CYBER SECURITY COALITION

6

In deze **video van Febelfin** (<https://www.youtube.com/watch?v=F7pYHN9iC9I>) zie je hoe een genie in social engineering te werk gaat om alles over jou te weten te komen...

- Wat verspreid jij op de sociale netwerken?
- Wat kan men hieruit afleiden over jou?

Je zal het internet nooit meer op dezelfde manier bekijken...

## Blijf op je hoede

Gebruik je gezond  
verstand en je  
kritische geest



## Hoe ontmasker je social engineering?

### De signalen:

- Onbekende gesprekspartner
- Kritieke situatie (Covid-19)
- Ongelooflijke aanbieding
- Dringend, geheim
- Intimidatie, vleierij

### Ontmasker een aanval van social engineering

- Je **kent** je gesprekspartner **niet**.
- De situatie is heel **kritiek** (bv. context Covid-19)
- Dringend, geheim: je moet **snel handelen** en het is **vertrouwelijk**.
- Ongelooflijk! Een aanbod dat **te mooi** is **om waar te zijn**...
- De toon is uiterst **intimiderend of vleierend**.

## Hou het hoofd koel

Neem afstand en  
geef niet toe aan  
paniek



## Wat doe je tegen social engineering?

### Goede reflexen:

- Geen gehaaste reactie
- Controleer identiteit gesprekspartner
- Vraag door naar duidelijke informatie
- Voer geen ongewone transactie uit
- Geef geen gevoelige info door

8

### Neem de juiste reflexen aan tegen social engineering

- Neem de **tijd om na te denken**, handel niet in zeven haasten.
- Controleer de **identiteit** van je gesprekspartner.
- Stel je niet tevreden met een **vage of ingewikkelde uitleg**.
- Voer **geen ongewone transactie** uit zonder het akkoord van een derde.
- Geef geen **gevoelige of interne gegevens** door.



## Improviseer niet

Respecteer de  
interne procedures  
van je onderneming



## Hoe reageer je bij een aanval?

### De middelen:

- Waarschuw de verantwoordelijke
- Respecteer procedures
- Contacteer je bank / je internetprovider
- Wijzig je wachtwoorden

9

### Hoe reageren bij een aanval van social engineering

- Waarschuw de **verantwoordelijke** binnen je onderneming.
- Respecteer de **procedures** die gelden binnen de onderneming.
- Contacteer de **bank** onmiddellijk om na te gaan of er geld verduisterd werd. Contacteer ook je internetprovider.
- Wijzig je professionele en privé**wachtwoorden**.

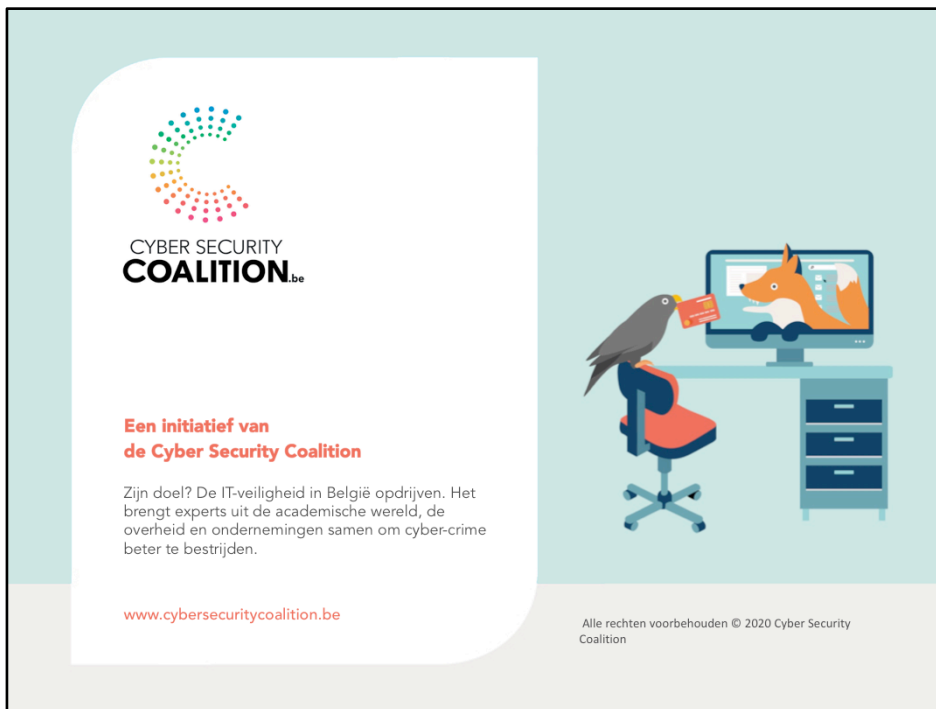
## Social engineering: praat erover!

Wat is jouw mening?  
Heb je opmerkingen?  
Wat heb je  
onthouden?  
Je eerste actie?



10

Wat is jouw mening?  
Heb je opmerkingen?  
Wat heb je onthouden?  
Wat zal de eerste actie zijn die je onderneemt na deze presentatie?



Bedankt voor je aandacht!