



**Ne vous laissez pas berner.**

Déjouez les attaques d'ingénierie sociale

Bruxelles, juillet 2020

Bonjour et bienvenue à tous !

### Nouveau message [CONFIDENTIEL!]

Vous êtes contacté par votre patron qui vous fait savoir que les autorités mènent une enquête sur une possible fraude fiscale. Il faut d'urgence et en toute confidentialité effectuer un transfert de 60 000 euros. Flatterie, intimidation : votre interlocuteur vous parle de votre carrière exemplaire, de vos possibilités d'évolution... et de vos enfants. Sans votre coopération, les conséquences seront très graves...

*Vous marchez... ?*



Un scénario classique d'ingénierie sociale dans les entreprises et PME.




**Méfiez-vous !**

Une personne mal intentionnée veut abuser de votre confiance.

Une technique si bien rodée qu'on parle d'ingénierie sociale : le fraudeur a étudié votre profil en glanant des informations sur vous, sur le web ou les réseaux sociaux. Objectif ? Endormir votre vigilance avec un scénario plausible pour vous tirer les vers du nez ou vous pousser à agir.

## L'ingénierie sociale

est une technique très bien rôdée et particulièrement intrusive.



### L'ingénierie sociale, quésako ?

**L'ingénierie sociale :**

- Manipulation psychologique
- Sphère personnelle
- Usurpation d'identité
- E-mail, media sociaux, téléphone

**L'objectif :**

- Informations personnelles
- Données sensibles de l'entreprise
- Transfert d'argent

**Le modus operandi :**

- Collecte d'informations
- Scénario plausible
- Enquête, contrôle, opportunité

L'ingénierie sociale, ou **social engineering**, est une technique frauduleuse qui consiste à **abuser des gens en jouant sur des caractères typiquement humains** comme la confiance, la curiosité, la naïveté, la peur, la cupidité...

Le fraudeur se fait passer pour un **tiers de confiance** et exploite la la **sphère personnelle** de la victime afin de faire intrusion dans le **réseau de l'entreprise**.

Le plus souvent, il s'agit d'un **e-mail**, un message sur les **medias sociaux** ou d'un **coup de téléphone**.

#### Son but ?

- Récupérer des **informations personnelles** (identifiant, mot de passe, numéro de carte de crédit).
- Accéder à des **données sensibles** au sein de l'entreprise.
- Obtenir un **transfert d'argent**.

#### Comment ?


- Collecte minutieuse d'**informations publiques et personnelles** (réseaux sociaux), parfois sur plusieurs mois
- Elaboration d'un **scénario plausible**, bien rôdé
- Une **enquête**, un **contrôle**, une **opération** urgente, une **opportunité**

**1 société belge sur 2**  
est aujourd'hui confrontée à la cybercriminalité.

**Des chiffres qui en disent long...**

Les chiffres :

- 70 millions d'euros, pour une banque belge (CEO fraude).
- Plus de 10 milliards d'euros au niveau mondial (2018).

 CYBER SECURITY COALITION.be

5

En Belgique, **1 entreprise sur 2** est touchée par la cybercriminalité et des techniques d'ingénierie sociale.

Incroyable ! L'ingénierie sociale a déjà coûté **70 millions d'euros à une banque belge** via la technique dite de la « fraude du CEO ». Selon 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>) les responsables dans une organisation sont ciblés 10 fois plus que d'autres collaborateurs.

Au niveau mondial, les dommages liés au phénomène ont atteint **10 milliards d'euros**.  
(Source: FBI – 2018)



Dans cette **vidéo de Fébelfin** (<https://www.youtube.com/watch?v=F7pYHN9iC9I>), vous verrez comment opère un génie de l'ingénierie sociale pour tout savoir sur vous...

- Que diffusez-vous sur les réseaux sociaux ?
- Que peut-on deviner sur vous ?

Vous ne verrez plus jamais Internet de la même façon...

## Restez sur vos gardes.

Faites preuve de bon sens et d'esprit critique.



## Comment démasquer l'ingénierie sociale ?

### Les signaux :

- Interlocuteur inconnu
- Situation critique (Covid-19)
- Offre incroyable
- Urgent, secret
- Intimidation, flatterie

### Démasquez une attaque d'ingénierie sociale

- Vous ne **connaissez pas** votre interlocuteur.
- La situation est hautement **critique (cf. Covid-19)**
- Urgent, secret : vous devez **agir rapidement** et c'est **confidentiel**.
- Incroyable ! Une **offre trop belle** pour être vraie...
- Le ton est excessivement **intimidant ou flatteur**.

## Gardez la tête froide.

Prenez du recul et ne cédez pas à la panique.



## Que faire face à l'ingénierie sociale ?

### Les réflexes :

- Pas de réaction hâtive
- Identité de l'interlocuteur
- Informations claires
- Transaction inhabituelle
- Données sensibles

8

### Adoptez les bons réflexes contre l'ingénierie sociale

- Prenez un **temps de réflexion**, n'agissez pas dans l'urgence.
- Vérifiez l'**identité** de votre interlocuteur.
- Ne vous contentez pas d'**explications opaques** ou compliquées.
- N'effectuez **aucune transaction** inhabituelle sans l'accord d'un tiers.
- Ne fournissez pas de **données sensibles** ou internes.



## Pas d'impro.

Respectez les  
procédures internes  
de votre entreprise.



## Comment réagir en cas d'attaque ?

### Les dispositions :

- Personne responsable
- Respect des procédures
- Contact banque / fournisseur internet
- Mots de passe

9

### Réagissez en cas d'attaque par ingénierie sociale

- Prévenez la **personne responsable** au sein de votre entreprise.
- Respectez les **procédures** en place dans votre organisation.
- Contactez la **banque** en urgence si des fonds ont été volés. Contactez votre fournisseur internet
- Changez vos **mots de passe**, professionnels et privés.


## L'ingénierie sociale, on en parle !

Qu'en pensez-vous ?  
Des remarques ?  
Qu'avez-vous retenu ?  
Votre première action ?



10

Qu'en pensez-vous ?  
Avez-vous des remarques ?  
Qu'avez-vous retenu ?  
Quelle sera votre première action suite à cette présentation ?




**CYBER SECURITY  
COALITION**.be

**Une initiative  
de la Cyber Security Coalition**

Sa mission ? Renforcer la sécurité informatique en Belgique. Elle rassemble des experts du monde académique, public et privé pour mieux lutter contre le cyber-crime.

[www.cybersecuritycoalition.be](http://www.cybersecuritycoalition.be)



Tous droits réservés © 2020 Cyber Security Coalition

Merci de votre attention !