Sensibilisation à la cybersécurité

Social Engineering

"Illusion is everything" - Bernz

Laurent Linard

Les objectifs de la sensibilisation

- Apprendre à appliquer les bonnes pratiques ;
- Savoir comment reconnaitre les menaces les plus courantes ;
- Le lien avec votre travail au quotidien ;
- Lever les interrogations par rapport à la sécurité de l'information et la cyber sécurité.

Avez-vous déjà été confronté à des tentatives de social engineering dans votre environnement de travail ?

1 Allez sur wooclap.com

2 Entrez le code d'événement dans le bandeau supérieur

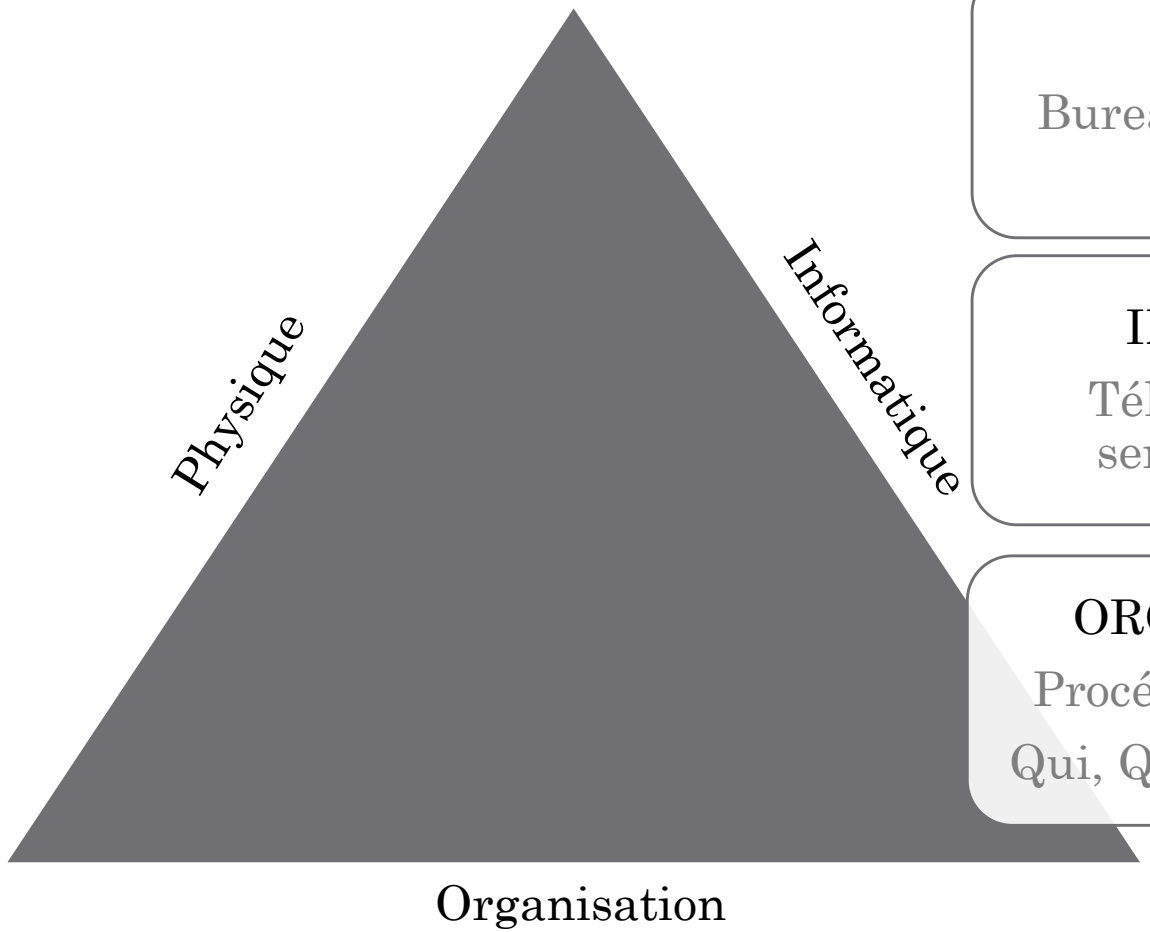
Code d'événement
CRF23

Les motivations principales

- **L'information**
  - Concurrents ;
  - Comptabilité ;
  - Liste des employés
  - Curiosité mal placée (interne) ;
  - …
- **Déstabilisation**
  - Destruction physique ou logique
  - Vol de données stratégiques
  - Vengeance
  - Blocage
  - Fuite d'information (Leaks)
  - …

- **Etatique**
  - Manipulation politique
  - Changement de régime ou gouvernement
  - Espionnage
  - …
- **Financière**
  - Attaques multiples > Phising/Hacking pour ransomwares et rançons
  - Revente de base de données illégalement
  - Transactions frauduleuses
  - Vol d'identité
  - …

1. Et pas que sur le net : Le triangle de la sécurité



PHYSIQUE:

Bureau, immeuble, voiture, armoires,…

INFORMATIQUE :

Téléphone, ordinateur, serveurs, accès wifi,…

ORGANISATIONNEL :

Procédures et Management

Qui, Quoi, Comment, Quand?

À votre avis, pourquoi y a-t-il une telle augmentation au niveau de ce type d'attaque ?

1 Allez sur wooclap.com

2 Entrez le code d'événement dans le bandeau supérieur

Code d'événement
CRF23

Pourquoi cette augmentation ?

Motivations des CyberCriminels

Des cibles de + en + nombreuses

* Transformation numérique globale (Entreprise et administration)
*Déploiement large des technologies dans le grand public
*Manque d'expert en sécurité et management de la cybersécurité

Expertise accessible

* Marché noir d'outils d'attaques
* Hack as a Service
* Outils automatiques plus faciles
* Prix Ddos : $20 à XX $ à qq centaines de $

Risques faibles pour les attaquants*

*Anonymisation / Absence de traces
*Peu de monitoring
*Réponse judiciaire complexe
*Crypto-monnaies
*Tor et machines fantômes

Profits importants

* Données cartes bancaires : 3 à $150 / Carte
* Données personnelles : 0,3 à 2$/personne
*Données médicales : 2$ à 50$/personne
*Fraude, espionnage

Facile → Si pas bien sécurisé

Efficace → Si correctement utilisé

Bon marché et facile à trouver si on sait où trouver

Quel est le pourcentage de cyberattaques qui relèvent de l'ingénierie sociale ?

1 Allez sur wooclap.com

2 Entrez le code d'événement dans le bandeau supérieur

Code d'événement
CRF23

L'ingénierie sociale en chiffres

+ 90 %

+ de 90 % des cyberattaques relèvent de l'ingénierie sociale

56 %

56 % des responsables informatiques déclarent que les attaques de phishing ciblées constituent leur plus grande menace pour la sécurité

66%

66 % des logiciels malveillants sont installés via des pièces jointes d'e-mails malveillants

2,4 million $

Le coût moyen d'une attaque de logiciel malveillant pour une organisation est de 2,4 millions de dollars.

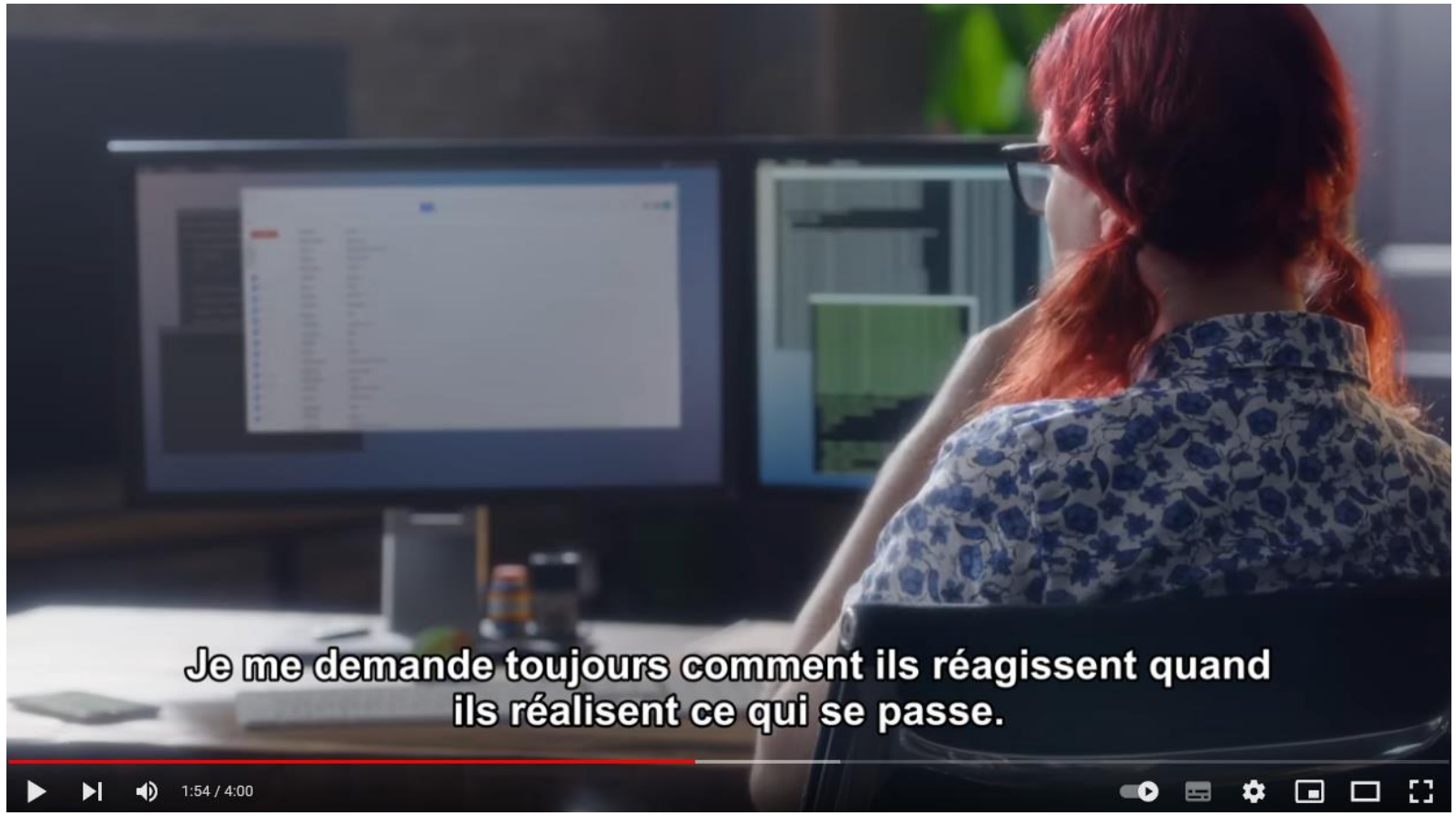
Nouveaux employés

Les nouveaux employés sont les plus sensibles aux attaques d'ingénierie sociale, 60 % des professionnels de l'informatique disent qu'ils sont à haut risque.

3 %

Seuls 3 % des utilisateurs ciblés signalent les e-mails malveillants à la direction

le social engineering en vidéo



Vidéo d'introduction

Reliez le mot à sa définition

1 Allez sur wooclap.com

2 Entrez le code d'événement dans le bandeau supérieur

Code d'événement
CRF23

Vishing, smishing et phishing — Connaissez-vous la différence ?

Vishing

Consiste à passer des appels téléphoniques et laisser des messages vocaux intimidants pour convaincre les victimes de partager des informations personnelles avant de les voler.

Smishing

Consiste à envoyer des messages textes pour dérober des informations et commettre d'autres cybercrimes.

Phishing

Utilise une grande variété de méthodes, y compris des e-mails, de faux sites Web et des SMS pour voler les victimes. Le smishing et le vishing sont deux types de phishing.

https://terranovasecurity.com/fr-fr/quest-ce-que-le-vishing/

L'ingénierie sociale : Le phishing

Qu'est-ce que le phishing?

- Le phishing vient du terme"fishing" (pêche) et est utilisé délibérément en raison de la manière dont il fonctionne : Le Hameçonnage.
- C'est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité via des messages "qui vous attirent" et qui tentent de vous faire "mordre à l'hameçon".
- Une fois que vous êtes "hameçonnés"… Vous avez des problèmes.

Le phishing
Les trois principaux types

1. **Le lien malveillant** qui vous conduit vers des sites Web factices qui volent vos informations ou infectent votre appareil avec des logiciels malveillants.

2. **La pièce jointe malveillante** qui compromet votre ordinateur.

3. **La demande de données sensibles par les pirates** qui vous invitent à saisir des identifiants, des mots de passe, des informations financières, etc. qui sont ensuite volés.

ING

Chère cliente, Cher client,

Lors de votre dernier opération bancaire, nous avons remarqué une activité inhabituelle sur votre compte.

Pour réactiver votre compte Vous devez mettre à jour vos informations, une fois ces dernières validées, le compte fonctionnera normalement.

L'ensemble du processus ne prendra que 5 minutes. Vous devez agir maintenant pour résoudre le problème le plus rapidement possible.

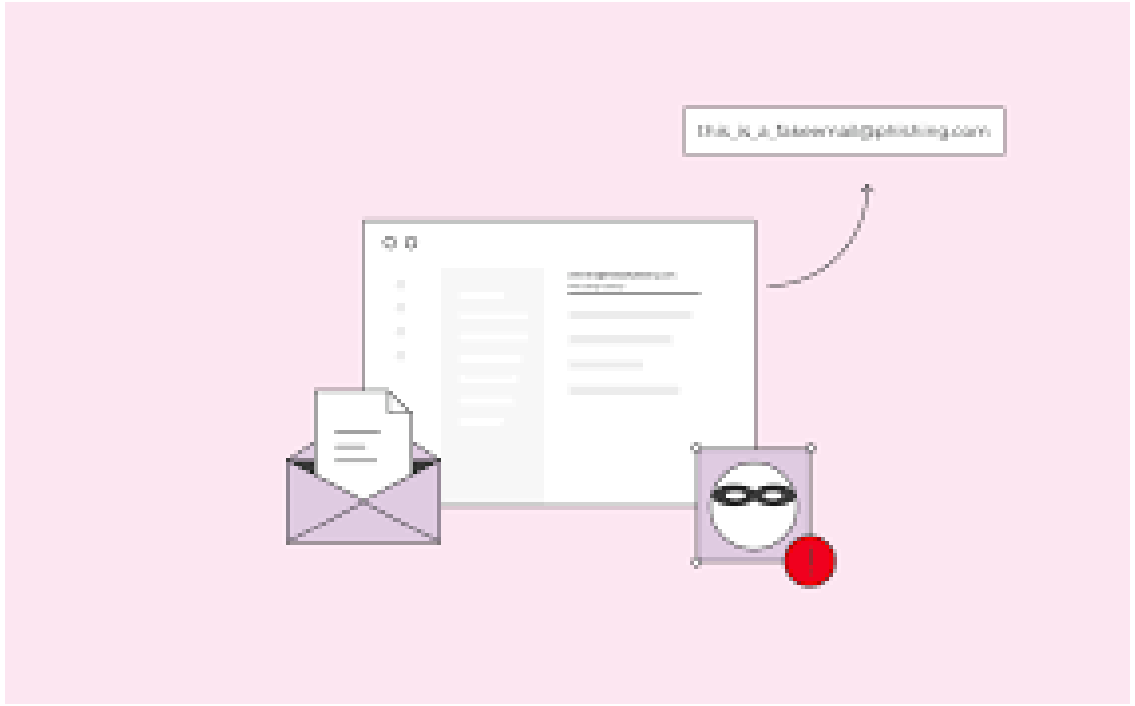
Suivez le lien ci-dessous pour finaliser le processus et régler l'état de votre compte

Accèder à votre espace sécurisé

Nous vous remercions de votre confiance

Cordialement,

Arnaud Le Roux
Direction Qualité



Le phishing
Exemple de phishing basé sur le lien

Aujourd'hui, la poste vous apporte un colis.

la poste <noreply@xyz542.be>
To YOU

4 septembre à 8 h 29

la poste

Bonjour,

BOLSY vous a envoyé un colis portant la référence 3232000179598199566320 40. La poste vous le livrera aujourd'hui entre 8 h et 17 h. Nous espérons que vous serez présent.

Vous pouvez consulter le statut de votre colis via notre application track & trace. Si vous ne parvenez pas à ouvrir le lien, veuillez télécharger notre outil pour suivre votre colis en direct.

Sincères salutations,
La poste.

Annexe à l'e-mail

Reply Reply to All Forward More

1 Allez sur wooclap.com
2 Entrez le code d'événement dans le bandeau supérieur

Code d'événement
CRF23

Safeonweb.be

Votre nouvelle carte bancaire – importance : élevée

Service clientèle QWT35 Bank <info@vnnabsbns.com>

Pas d'illustration dans cet e-mail ?
Dans ce cas, consultez-la en ligne.

QWT35 BANK

Votre nouvelle carte bancaire

Chère Cathy Jansens,

Notre service administratif nous informe que, malgré nos messages antérieurs, vous utilisez encore votre ancienne carte bancaire QWT35 Bank.

Les détenteurs d'un compte à vue QWT35 Bank ont jusqu'au 21 juillet 2017 pour commander gratuitement une nouvelle carte bancaire QWT35 Bank.

Les détenteurs d'un compte à vue ne profitant pas de cette action exclusive avant le 21 juillet 2017 recevront automatiquement une nouvelle carte bancaire QWT35 Bank. Les frais d'envoi automatique de la nouvelle carte s'élèvent à 17,95 € et sont automatiquement facturés. Les détenteurs d'un compte à vue en seront informés.*

Faites des économies et cliquez ici pour commander gratuitement votre nouvelle carte bancaire.

Avec nos plus cordiales salutations,

Votre équipe QWT35 Bank

QWT35 BANK

QWT35 Bank SA
Belgiëlei 2, 2018 Anvers
RPM Anvers, TVA BE 0404.453.579

QWT35 Bank Assurances SA
Belgiëlei 2, 2018 Anvers
RPM Anvers, TVA BE 0404.453.579
Code administratif : 0858 3539

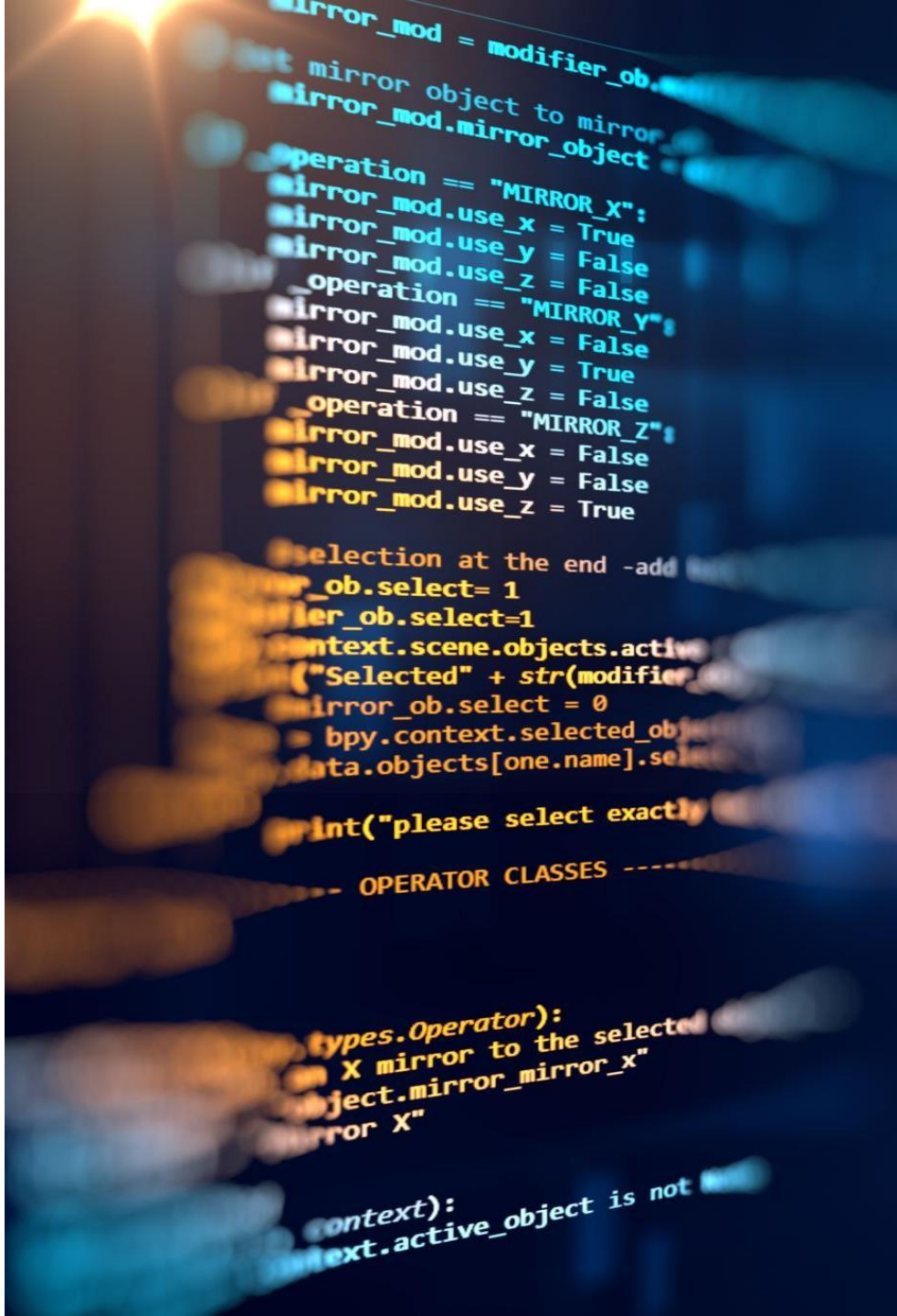
1 Allez sur wooclap.com
2 Entrez le code d'événement dans le bandeau supérieur

Code d'événement
CRF23

Safeonweb.be

Un lien peut en cacher un autre : test !

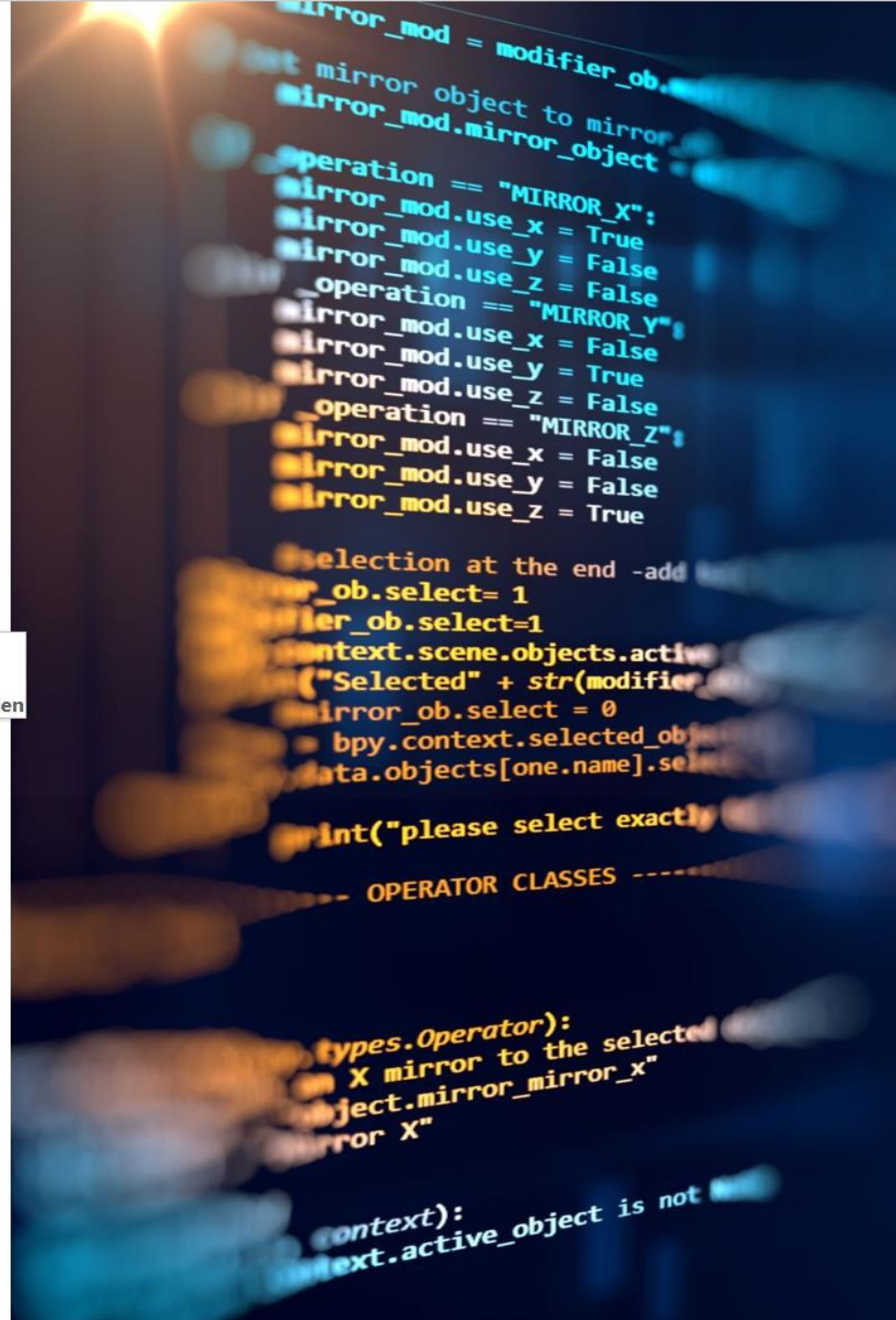
- Laurent.dupont@colissimo.com
- Laurent.dupont@collissimo.com
- Laurent.dupont@colissimo.com
- Laurent.dupont@colissimo.com
- Laurent.dupont@colissimo.com



Un lien peut en cacher un autre : test !

- Laurent.dupont@colissimo.com
- Laurent.dupont@collissimo.com
- Laurent.dupont@colissimo.com
- Laurent.dupont@colissimo
- Laurent.dupont@colissimo.com

mailto:robert.lehackeur@jetaibieneu.
be
Cliquer en maintenant le bouton Ctrl enfoncé pour suivre le lien



Le phishing
Exemple de demande d'informations sensibles

colissimo

Colissimo vous informe que l'envoi de votre colis est disponible.
Vous avez un délais de 48 heures sinon il sera retourn&eac ute; à l'expéditeur.
Pour confirmer l'envoi de votre commande:

-Envoyez un justificatif de domicile (**Facture Edf** , **avis d'imposition...**)valide de moins de 3 mois.

- Copie couleur **passeport** ou copie recto verso **pièce d'identité** à l'adresse suivante:

colisresponsable3616@gmail.com

NB: après avoir passé la confirmation avec succès, un e-mail vous sera envoyé avec toutes les informations nécessaires à propos de votre paquet(expéditeur, Date, bureau de poste le plus proche.)

Bien cordialement,
Service colissimo.fr

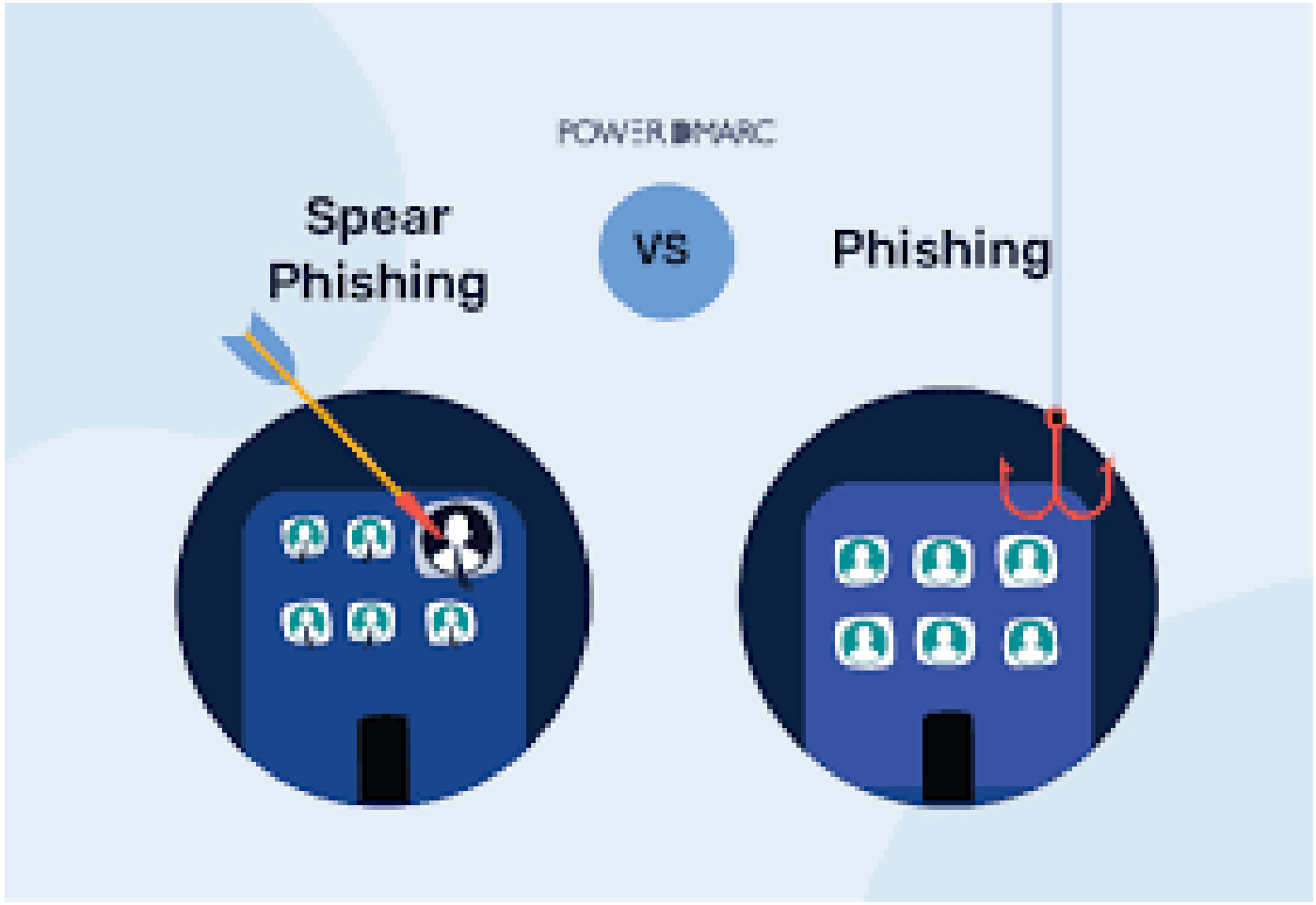
Le baiting (ou technique de l’appât)

- Cette variante est proche du phishing. Ce qui la rend différente, c'est la promesse d'un objet ou d'un produit que les attaquants utilisent pour séduire leurs victimes. Par exemple, ils utilisent l'offre de téléchargement gratuit de musiques ou de films.

https://www.nomios.fr/ressources/ingenierie-sociale/#:~:text=L'ing%C3%A9nierie%20sociale%20consiste%20%C3%A0,est%20une%20pratique%20de%20manipulation.

Pretexting (ou prétexte)

Cette attaque utilise un prétexte pour attirer l’attention et inciter la victime à fournir l’accès à des données sensibles ou des systèmes protégés. L'attaquant se fait généralement passer pour une personne d'autorité proposant son aide afin d'obtenir des données sensibles. Par exemple, se faire passer pour un employé d'une banque afin d'obtenir les coordonnées bancaires de la victime.



Spear Phishing et encore..... ... plus...

le Whaling

Le tailgating (ou talonnage)

Attaque de point d'eau *Watering Hole*

- L'attaque de point d'eau (Water-holing) cible un groupe d'utilisateurs ainsi que les sites Web qu'ils visitent fréquemment. Le cybercriminel explore ces sites Web à la recherche d'une faille de sécurité puis l'infecte avec un maliciel. L'un des membres du groupe ciblé est éventuellement contaminé par le maliciel. Cette technique d'ingénierie sociale est très spécifique et difficile à détecter.

https://terranovasecurity.com/fr/quest-ce-que-l-ingenierie-sociale/

Le maliciel ou Faux-semblant

- Le maliciel est utilisé pour amener les victimes à payer pour éliminer un maliciel, un virus ou un autre logiciel contaminé de leur ordinateur. On leur fait croire qu'il y a un virus ou un maliciel sur leur ordinateur et qu'il sera retiré en échange d'une somme d'argent. Selon l'arnaque, le criminel s'en tient à voler les informations de carte de crédit de la victime ou en profite pour installer également un vrai maliciel ou rançongiciel sur l'ordinateur.

Logiciel alarmant (scareware)

- Également considéré comme une forme de logiciel malveillant, le logiciel alarmant ou scareware utilise la peur pour inciter les utilisateurs à partager des informations confidentielles ou à télécharger des logiciels malveillants. Ils prennent souvent la forme d'un faux avis des forces de l'ordre accusant la personne d'un délit, ou d'un faux message d'assistance technique avertissant l'utilisateur de la présence d'un logiciel malveillant sur son appareil.

https://www.ibm.com/fr-fr/topics/social-engineering#:~:text=L'ing%C3%A9nierie%20sociale%20manipule%20les,commettre%20d'autres%20erreurs%20qui

ARNAQUE AU PRÉSIDENT

- Extrêmement redouté par les entreprises, ce type d'attaque peut engendrer des dommages financiers importants. Souvent lié aux attaques de phishing, les escrocs se font passer pour le président de l'entreprise pour demander à un employé d'effectuer un virement important et urgent à l'étranger.

- **La clé USB**
- Offert comme un cadeau, une clé USB infectée et utilisée sur un appareil peut permettre d'en prendre le contrôle. Une fois connecté, le logiciel malveillant contenu sur la clé permettra à son auteur de prendre le contrôle de la machine à distance. Ce virus peut s'étendre à tous les autres appareils reliés au même réseau.

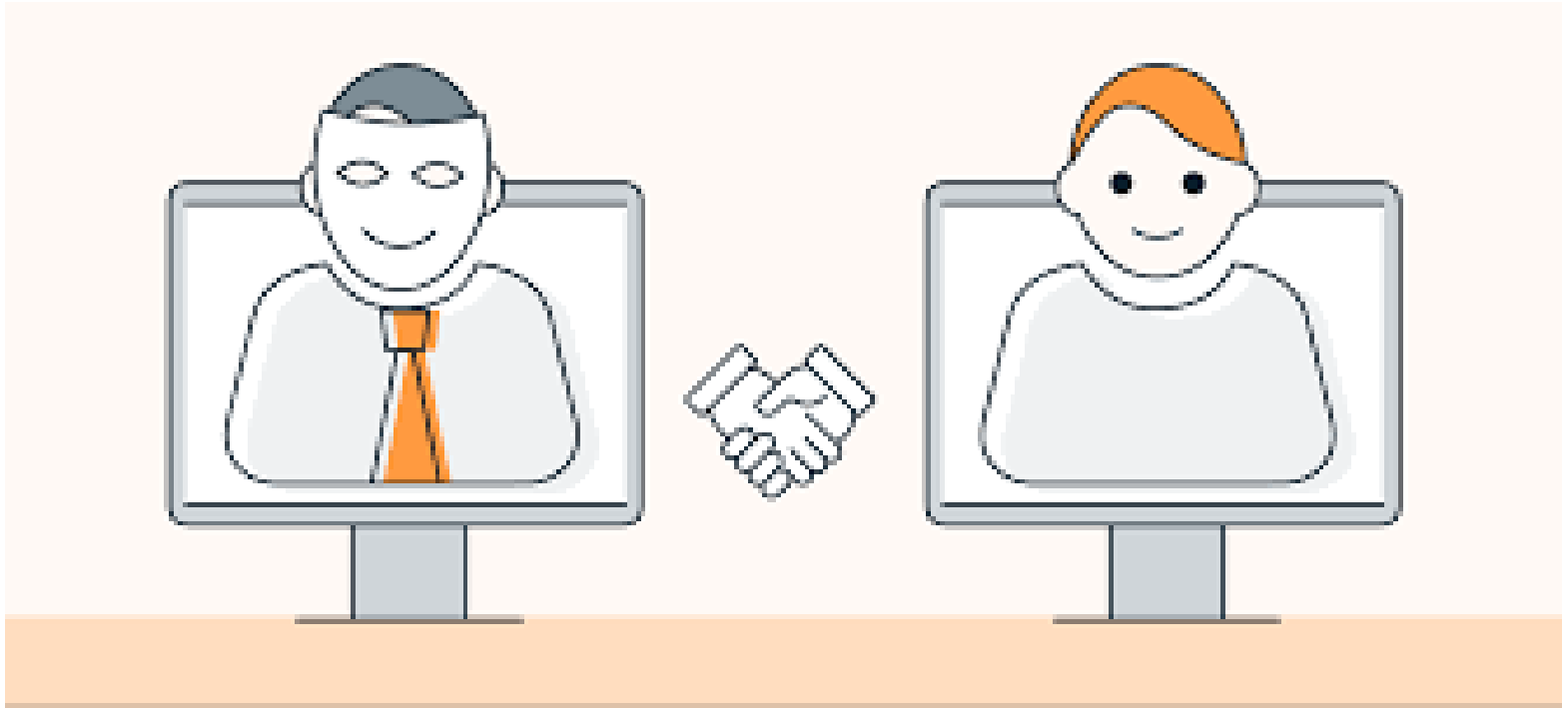
Quid pro quo :

- Des employés mécontents peuvent être amenés à fournir des informations sensibles à un pirate en échange d'argent ou d'autres promesses.

Ingénierie sociale en personne :

- Ingénierie sociale en personne : Les attaquants peuvent se faire passer pour des employés, des techniciens ou des visiteurs légitimes pour infiltrer des locaux sécurisés et obtenir un accès non autorisé à des informations ou à des systèmes.

https://www.human-station.com/sequences/le-piratage-psychologique-definition



Usurpation d'identité

- Les attaquants peuvent utiliser des informations personnelles volées ou publiques pour se faire passer pour quelqu'un d'autre, tels que des employés, des partenaires commerciaux ou des amis, afin de gagner la confiance des victimes et obtenir des informations sensibles.

https://www.avg.com/fr/signal/what-is-social-engineering

Ingénierie sociale téléphonique :

- Les escrocs/hackers compétents ont tout mis en place pour paraître légitimes :
- **Les bonnes informations**
- **L'urgence**
- **L'expertise téléphonique**
- **Une ambiance professionnelle**

https://blog.mailfence.com/fr/le-vishing-ingenierie-sociale/

- Le vishing (hameçonnage vocal ou VoIP) est un cybercrime qui consiste à passer des appels téléphoniques dans le but d'obtenir les renseignements personnels et confidentiels d'une victime. Les cybercriminels utilisent des tactiques d'ingénierie sociale pour convaincre leurs victimes de partager des informations privées comme les données d'accès à un compte bancaire.

- Un exemple en image :https://www.youtube.com/watch?v=lc7scxvKQOo&t=1s

1. La numérotation de guerre (wardialing)

Le cybercriminel utilise un logiciel pour appeler un indicatif régional spécifique et laisse un message semblant provenir d'une organisation locale, comme une banque, un service public ou une entreprise. Lorsqu'une personne répond, un message automatique démarre lui demandant de fournir des informations personnelles telles que : nom complet, renseignement de carte de crédit,

exemple que ces

pas été compromis.

2. La voix sur IP (VoIP)

Grâce à la voix sur IP, il est très facile pour les cybercriminels de créer un faux numéro de téléphone. Ces types de numéros sont difficiles à retracer et peuvent être utilisés pour créer des numéros de téléphone qui paraissent locaux ou qui présentent un préfixe 1-800. Certains cybercriminels créent des numéros VoIP qui semblent provenir d'un ministère, d'un hôpital local ou d'un service public.

3. Le spoofing téléphonique ou l'usurpation de numéro

Tout comme dans le cas du vishing, le cybercriminel se cache derrière un faux numéro de téléphone. Une des principales stratégies de spoofing consiste à masquer l'identité de l'appelant et à faire apparaître la mention « Inconnu » sur l'afficheur du destinataire. Il est également possible d'indiquer sur l'afficheur que l'appel semble provenir du gouvernement, d'un service public ou d'une banque. Le cybercriminel peut ainsi se faire passer pour une organisation légitime.

4. Le dumpster diving ou la fouille des poubelles

Une méthode simple et populaire pour recueillir des numéros de téléphone valides consiste à littéralement fouiller les poubelles en particulier celles situées derrière les bureaux des entreprises. Souvent, les criminels trouvent suffisamment d'information pour lancer une attaque de spear phishing (harponnage) contre la victime.

De qui faut-il se méfier ?

1. Représentant du gouvernement

L'auteur de l'appel prétend téléphoner au nom du gouvernement afin de valider des données d'identification personnelle. Il peut menacer de suspendre le paiement d'un remboursement d'impôt ou d'un programme de sécurité sociale si la victime ne fournit pas les informations demandées pour confirmer son compte et son identité.

2. Fraude du soutien technique

Dance cette situation, le cybercriminel prétend être un représentant du soutien technique de Microsoft, Amazon ou d'un fournisseur de service en ligne. Il affirme avoir remarqué une activité inhabituelle dans le compte de la victime et souhaite confirmer qu'il possède les informations exactes du compte. En outre, le cybercriminel peut demander à la victime de lui transmettre son adresse courriel pour qu'il puisse lui envoyer la mise à jour d'un logiciel, soi-disant pour protéger son ordinateur des cybercriminels. Bien entendu, son installation permettra plutôt l'installation d'un malware.

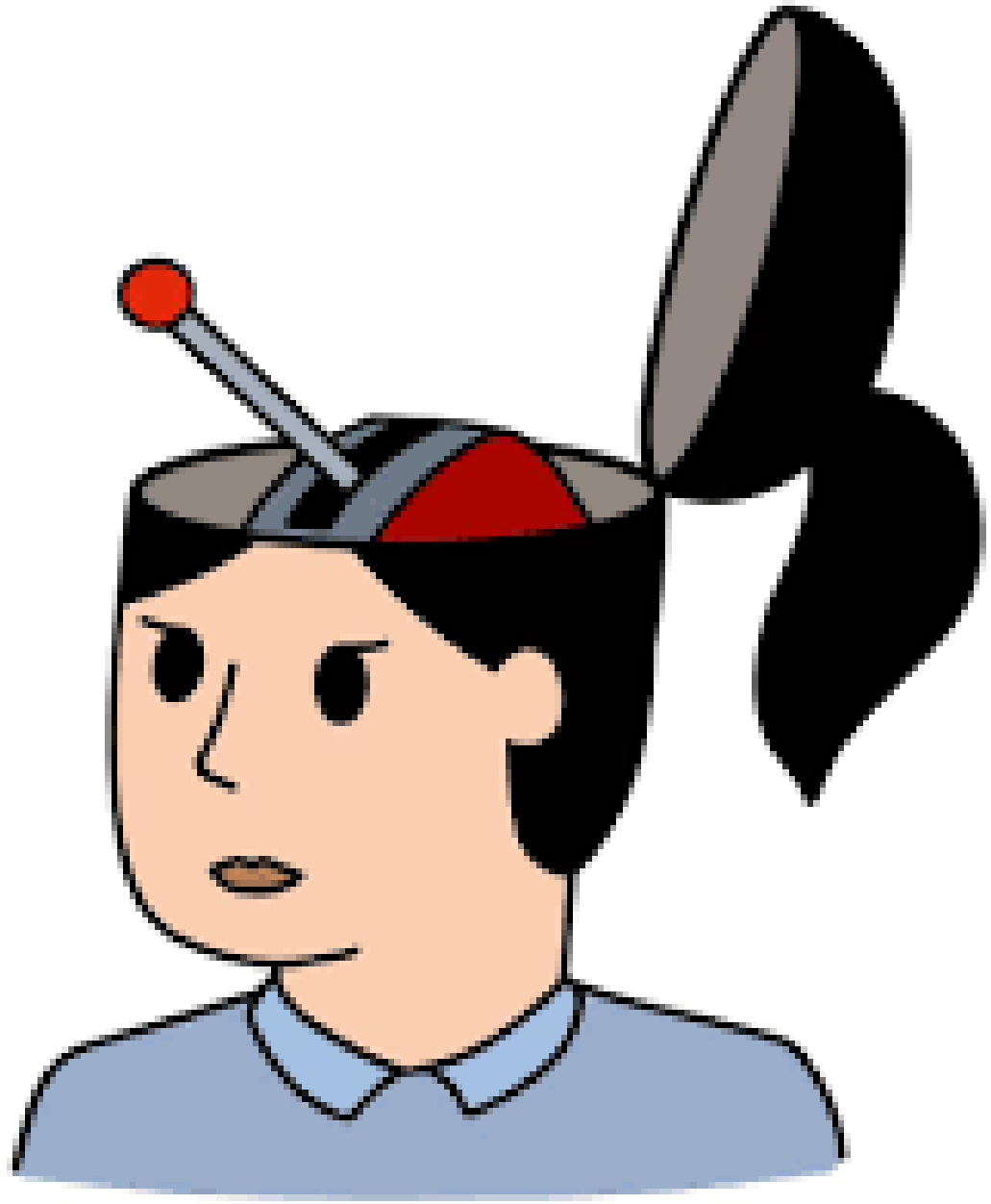
3. Fausse banque

En utilisant un faux numéro de téléphone et une fausse identité, le cybercriminel prétend téléphoner au nom de la banque de la victime. Il affirme qu'une activité inhabituelle a été détectée dans son compte et qu'il doit confirmer ses détails bancaires, y compris son adresse postale, comme preuve d'identification. Cette information peut ensuite être utilisée pour commettre un vol d'identité.

4. Attaque de télémarketing

Tout le monde aime gagner des cadeaux et les cybercriminels le savent bien. Ils profitent de cette situation pour amener des victimes sans méfiance à partager des informations confidentielles pour confirmer la réception du prix et l'acheminer à la victime.

Les Leviers Psychologiques



À votre avis, quels sont les leviers psychologiques sur lesquels les hackers agissent pour vous manipuler ?

1 Allez sur wooclap.com

2 Entrez le code d'événement dans le bandeau supérieur

Code d'événement
CRF23

10 techniques de manipulation mentale à repérer et à fuir

- La manipulation mentale vise à **contrôler ou influencer** les émotions, les pensées, le **comportement d'autrui** de façon positive ou négative et de manière consciente ou inconsciente chez le sujet.
- Nous utilisons tous la **manipulation** au quotidien pour obtenir quelque chose d'autrui.

- Recourir au chantage émotionnel
- Faire culpabiliser l'autre
- Menacer et intimider
- Jouer sur les insécurités de l'autre
- Dénigrer, critiquer et se moquer constamment
- Renier l'existence de l'autre
- Être ambivalent sur ses attentes
- Séduire par des compliments excessifs
- Utiliser la projection mentale pour manipuler
- Utiliser la technique du gaslighting pour rendre l'autre fou

https://www.la-clinique-e-sante.com/blog/relations-toxiques/techniques-manipulation-mentalev

Le futur de l'ingénierie sociale

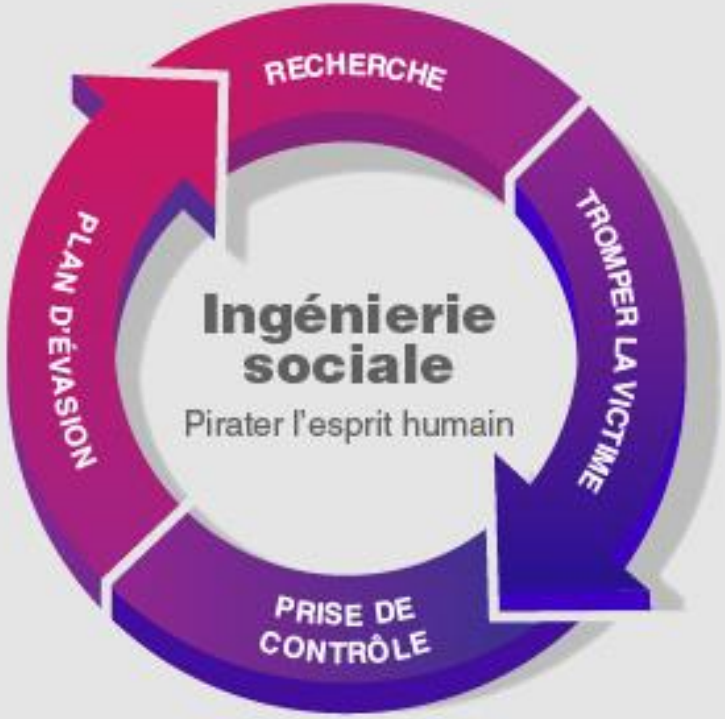
Avec le Deepfake ou le Deepvoice, la supercherie des ingénieurs sociaux sera encore plus dure à déceler. Le Deepfake permet de remplacer son visage par celui de sa victime, le Deepvoice permet de remplacer sa voix par celle de sa victime. Si la victime est un chef d'entreprise, alors il est facile, et à peu de frais de se faire passer pour lui.

Autrement dit, même un contact en video ne permet pas de savoir si la personne est véritablement la bonne.

Le Deepfake et le Deepvoice sont donc deux technologies pouvant être mises à profit par les cybercriminels dans le cadre d'une attaque par ingénierie sociale.

En résumé le cercle vicieux

- La victime est identifiée par l'attaquant
- Des informations sur la victime sont collectées
- Les attaquants élaborent la meilleure stratégie afin de pirater la victime



- Se retirer après l'intrusion sans susciter le doute
- Suppression du programme malveillant
- Effacer ses traces

- Présenter de fausses informations à la victime
- Concevoir une histoire trompeuse
- Attirer la victime dans le piège

- Investir du temps et des ressources afin de gagner la confiance de la victime
- Lancement de l'attaque
- Obtenir les données recherchées

https://fr.safetydetectives.com/blog/quest-ce-que-lingenierie-sociale-et-pourquoi-represente-t-elle-une-menace/

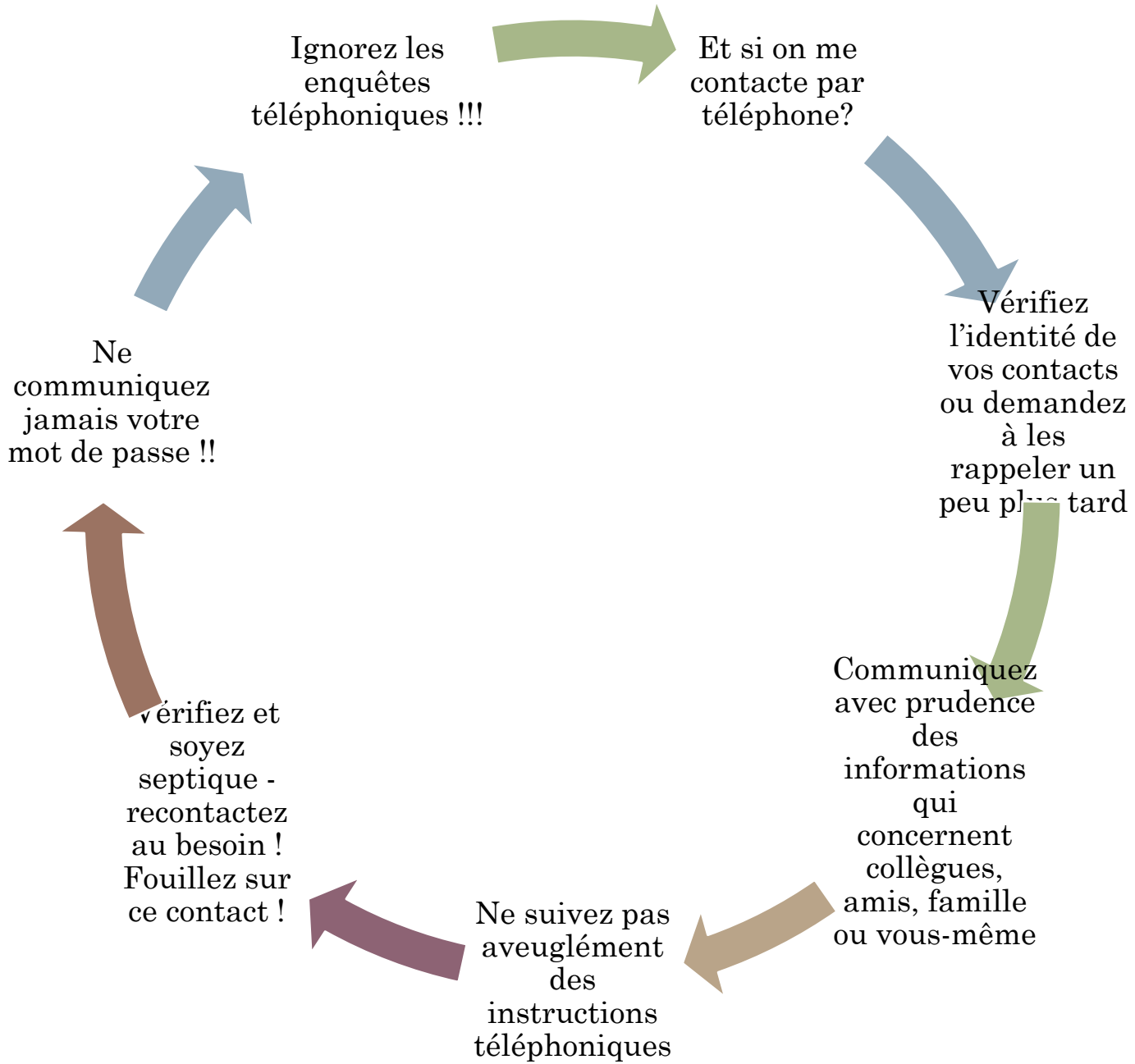
Ce qui doit vous alerter

- Fautes d'orthographe, de grammaire et de language ;
  - Attention pour les jeunes ☺
- Adresses mails suspectes ;
- Nom d'interlocuteur inconnu ;
- Url inhabituel, lien hypertexte qui ne correspond pas au site réel ;
- Présence de pièces jointes (*.exe ; *.bat ; …) ;
- Demande d'informations personnelles (sensibles) ;
- Exemple: mot de passe, adresse, numéro de téléphone, numéro de carte bancaire ;
- Demande de recontacter un numéro de type 08XX ;
- …

Phishing

Ingénierie sociale

Ce qu'il faut retenir



Un dernier bon réflexe à adopter : VPN

- Sécuriser la connexion
- Chiffrement
- Données non lisibles par des tiers
- Connexion anonyme (ou presque)
- Votre adresse ip est modifiée
- Vous avez accès au monde entier

Un doute ???? Signaler !!!!!

- **Vous avez fait face à une situation suspecte ?**
- Pour le privé :
- Envoyez-le à l'adresse **suspect@safeonweb.be** et supprimez-le ensuite.
- Dans votre entreprise :
- Prévenez le **service IT** avec une capture d'écran > Démo !
- ***Ne pas le transférer !***
- ***Ne pas ouvrir la pièce jointe !!***
- ***Ne PAS cliquer !!!***

Incidents de sécurité : solutions

Si vous êtes victimes

- Débranchez la machine du réseau (Coupez WIFI et Cable réseau sans les ciseaux ☺)
- Signalez les faits (essayez de noter sur un carnet papier)
- Alertez votre service IT
- Alertez votre direction
- Ne pas transférer des éléments douteux
- Conservez les preuves (ex: captures d'écran) > COMMENT FAIRE ?
- Déposez plainte à la POLICE si vous êtes directement concerné ;
- Identifiez la source afin de ne plus reproduire (Pas tjs facile) ;

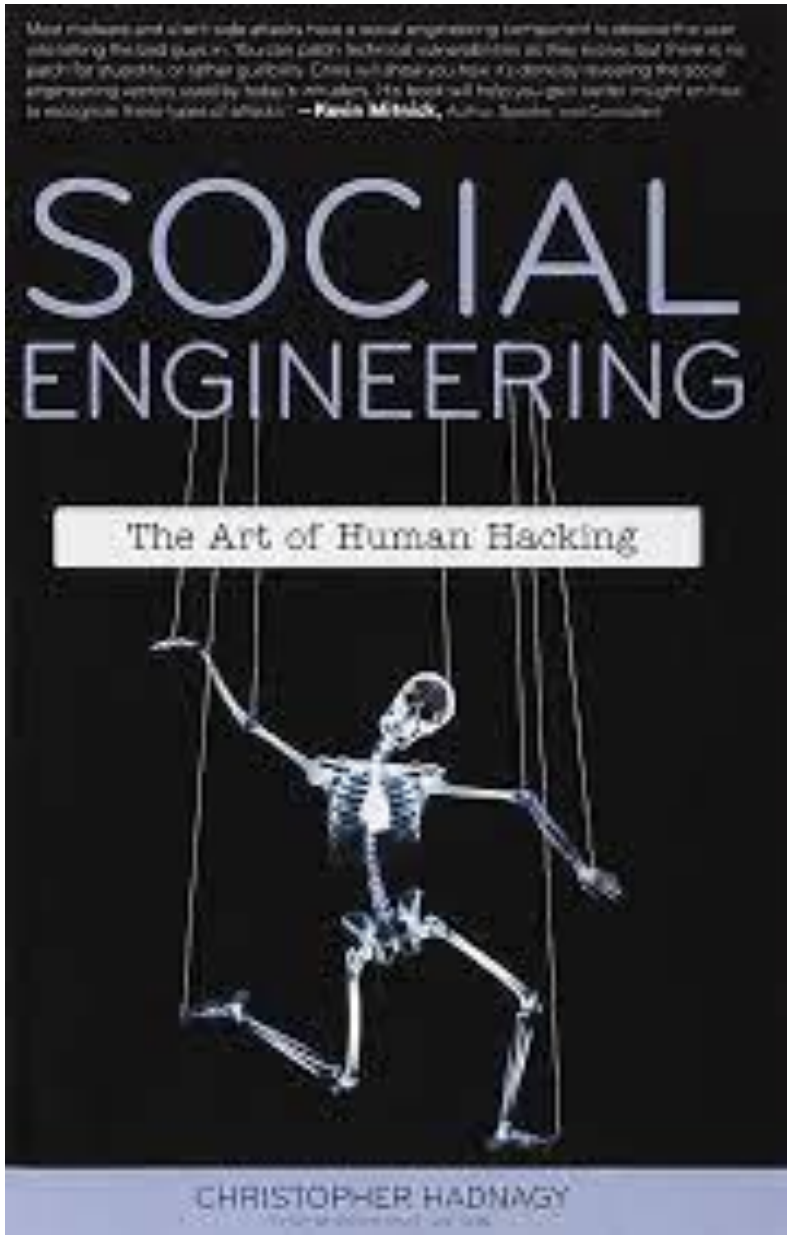
- Lorsque vous êtes face à un incident de sécurité de type propagation de virus, ransowmare, n'éteignez pas votre pc !

Enquête de satisfaction

1 Allez sur wooclap.com

2 Entrez le code d'événement dans le bandeau supérieur

Code d'événement
CRF23



Envie d'exemple ?

https://www.tessian.com/blog/examples-of-social-engineering-attacks/

1. $100 Million Google and Facebook Spear Phishing Scam

The biggest social engineering attack of all time (as far as we know) was perpetrated by Lithuanian national, Evaldas Rimasauskas, against two of the world's biggest companies: Google and Facebook. Rimasauskas and his team set up a fake company, pretending to be a computer manufacturer that worked with Google and Facebook. Rimsauskas also set up bank accounts in the company's name.

The scammers then sent phishing emails to specific Google and Facebook employees, invoicing them for goods and services that the manufacturer had genuinely provided — but directing them to deposit money into their fraudulent accounts. Between 2013 and 2015, Rimasauskas and his associates cheated the two tech giants out of over $100 million.

2. Persuasive email phishing attack imitates US Department of Labor

In January 2022, Bleeping Computer described a sophisticated phishing attack designed to steal Office 365 credentials in which the attackers imitated the US Department of Labor (DoL). The scam is a noteworthy example of how convincing phishing attempts are becoming.

The attack used two methods to impersonate the DoL's email address—spoofing the actual DoL email domain (reply@dol[.]gov) and buying up look-a-like domains, including "dol-gov[.]com" and "dol-gov[.]us". Using these domains, the phishing emails sailed through the target organizations' security gateways.

The emails used official DoL branding and were professionally written and invited recipients to bid on a government project. The supposed bidding instructions were included in a three-page PDF with a "Bid Now" button embedded.

On clicking the link, targets were redirected to a phishing site that looked identical to the actual DoL site, hosted at a URL such as bid-dolgov[.]us. The fake bidding site instructed users to enter their Office 365 credentials. The site even displayed an "error" message after the first input, ensuring the target would enter their credentials twice and thus reducing the possibility of mistyped credentials.

It's easy to see how even a relatively scrupulous employee could fall for an attack like this—but the problem would not have arisen if the target organization had better email security measures in place.

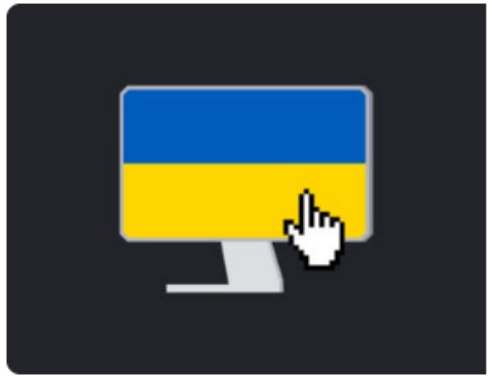
3. Russian hacking group targets Ukraine with spear phishing

As world leaders debate the best response to the increasingly tense situation between Russia and Ukraine, Microsoft warned in February 2022 of a new spear phishing campaign by a Russian hacking group targeting Ukrainian government agencies and NGOs.

The group—known as Gamaredon and tracked by Microsoft as ACTINIUM—has allegedly been targeting "organizations critical to emergency response and ensuring the security of Ukrainian territory" since 2021.

The initial phase of Gamaredon's attack relies on spear phishing emails containing malware. The emails also contain a tracking pixel that informs the cybercriminals whether it has been opened.

The case is an important reminder of how cybersecurity plays an increasingly central role in international conflicts—and how all organizations should be taking steps to improve their security posture and protect against social engineering attacks.



THREAT STORIES, ADVANCED EMAIL THREATS

Phishing Campaigns Pick-Up in the Wake of the Ukraine Invasion

by Charles Brook • Tuesday, April 5th, 2022

4. Deepfake Attack on UK Energy Company

In March 2019, the CEO of a UK energy provider received a phone call from someone who sounded *exactly like* his boss. The call was *so* convincing that the CEO ended up transferring $243,000 to a "Hungarian supplier" — a bank account that actually belonged to a scammer.

This "cyber-assisted" attack might sound like something from a sci-fi movie, but, according to Nina Schick, Author of "*Deep Fakes and the Infocalypse: What You Urgently Need to Know*", "This is not an emerging threat. This threat is here. Now."

To learn more about how hackers use AI to mimic speech patterns, watch Nina's discussion about deepfakes with Elvis Chan, Supervisory Special Agent at the FBI.

ADVANCED EMAIL THREATS

What are Deepfakes? Are They a Security Threat?

Sunday, December 26th, 2021

5. $60 Million CEO Fraud Lands CEO In Court

Chinese plane parts manufacturer FACC lost nearly $60 million in a so-called "CEO fraud scam" where scammers impersonated high-level executives and tricked employees into transferring funds. After the incident, FACC then spent *more* money trying to sue its CEO and finance chief, alleging that they had failed to implement adequate internal security controls.

While the case failed, it's an important reminder: cybersecurity is business-critical and *everyone's* responsibility. In fact, Gartner predicts that by 2024, CEOs could be personally liable for breaches.

ADVANCED EMAIL THREATS

CEO Fraud Prevention: 3 Effective Solutions

Wednesday, October 20th, 2021

6. Microsoft 365 phishing scam steals user credentials

In April 2021, security researchers discovered a Business Email Compromise (BEC) scam that tricks the recipient into installing malicious code on their device. Here's how the attack works, and it's actually pretty clever.

The target receives a blank email with a subject line about a "price revision." The email contains an attachment that looks like an Excel spreadsheet file (.xlsx). However, the "spreadsheet" is actually a .html file in disguise.

Upon opening the (disguised) .html file, the target is directed to a website containing malicious code. The code triggers a pop-up notification, telling the user they've been logged out of Microsoft 365, and inviting them to re-enter their login credentials.

You can guess what happens next—the fraudulent web form sends the user's credentials off to the cybercriminals running the scam.

This type of phishing—which relies on human error combined with weak defenses—has thrived during the pandemic. Phishing rates doubled in 2020, according to the latest FBI data.

7. Singapore bank phishing saga like ‘fighting a war’

Customers of the Oversea-Chinese Banking Corporation (OCBC) were hit by a string of phishing attacks and malicious transactions in 2021, leading to around $8.5 million of losses across approximately 470 customers.

The bank’s CEO Helen Wong described her company’s battle against the phishing attacks and subsequent fraudulent transfers as like “fighting a war.”

OCBC customers were duped into giving up their account details after receiving phishing emails in December 2021. The situation escalated quickly despite the bank shutting down fraudulent domains and alerting customers of the scam.

Wong described how, once the phishing campaign had taken hold, the fraudsters had set up “mule” accounts to receive stolen funds. No matter how quickly the bank’s security team managed to shut down a mule account, the scammers would soon find another to take its place.

The CEO described her dilemma after getting the phishing campaign under control: reimbursing customers felt like the right thing to do, but Wong feared it could incentivize further attacks. So far over 200 customers have been compensated.

8. Ransomware gang hijacks victim's email account

In April 2021, several employees of U.K. rail operator Merseyrail received an unusual email from their boss's email account with the subject line "Lockbit Ransomware Attack and Data Theft." Journalists from several newspapers and tech sites were also copied in.

The email—sent by a fraudster impersonating Merseyrail's director—revealed that the company had been hacked and had tried to downplay the incident. The email also included an image of a Merseyrail employee's personal data.

It's not clear how Merseyrail's email system got compromised (although security experts suspect a spear phishing attack)—but the "double extortion" involved makes this attack particularly brutal.

The "Lockbit" gang not only exfiltrated Merseyrail's personal data and demanded a ransom to release it—the scammers used their access to the company's systems to launch an embarrassing publicity campaign on behalf of its director.

9. Phishing scam uses HTML tables to evade traditional email security

Criminals are always looking for new ways to evade email security software. One BEC attack, discovered in April 2021, involves a particularly devious way of sneaking through traditional email security software like Secure Email Gateways (SEGs) and rule-based Data Loss Prevention (DLP).

BEC attacks often rely on impersonating official emails from respected companies. This means embedding the company's logos and branding into the email as image files.

Some "rule-based" email security software automatically treats image files as suspicious. If a phishing email contains a .png file of the Microsoft Windows logo, the email is more likely to be detected—but without that distinctive branding, the email won't look like it came from Microsoft.

But once again, cyber criminals have found a way to exploit the rule-based security approach.

To imitate Microsoft's branding, this attack uses a table instead of an image file—simply a four-square grid, colored to look like the Windows logo. The average employee is unlikely to closely inspect the logo and will automatically trust the contents of the email.

This isn't the first time fraudsters have used tables to evade rule-based DLP software. For example, some email security filters are set up to detect certain words, like "bitcoin." One way around this is to create a borderless table and split the word across the columns: "bi | tc | oin."

10. Sacramento phishing attack exposes health information

Five employees at Sacramento County revealed their login credentials to cybercriminals after receiving phishing emails on June 22, 2021.

The attack was discovered five months later, after an internal audit of workers' email inboxes.

The breach occurred after employees received phishing emails containing a link to a malicious website. The targets entered their usernames and passwords into a fake login page which were then harvested by cybercriminals.

The attack resulted in a data breach exposing 2,096 records of health information and 816 records of "personal identification information." The county notified the victims by email and offered free credit monitoring and identity theft services.

It remains to be seen whether this proposed resolution by the county will be enough. Protection of health information is particularly tightly regulated in the US, under the Health Insurance Portability and Accountability Act (HIPAA), and data breaches involving health data have led to some hefty lawsuits in the past.

11. Google Drive collaboration scam

In late 2020, a novel but simple social engineering scam emerged that exploited Google Drive's notification system.

The fraud begins with the creation of **a document containing malicious links to a phishing site**. The scammer then tags their target in a comment on the document, asking the person to collaborate.

Once tagged, the target receives a legitimate email notification from Google containing the comment's text and a link to the relevant document.

If the scam works, the victim will view the document, read the comments, and feel flattered at they're being asked to collaborate. Then, **the victim will click one of the malicious links**, visit the phishing site, and enter their login credentials or other personal data.

This scam is particularly clever because it exploits Google's email notification system for added legitimacy. Such notifications come straight from Google and are unlikely to trigger a spam filter.

But like all social engineering attacks, **the Google Drive collaboration scam plays on the victim's emotions**: in this case, the pride and generosity we might feel when called upon for help.

Want to see a screenshot of a similar attack? We breakdown a spear phishing attack in which the attacker impersonates Microsoft Teams. Check it out here.

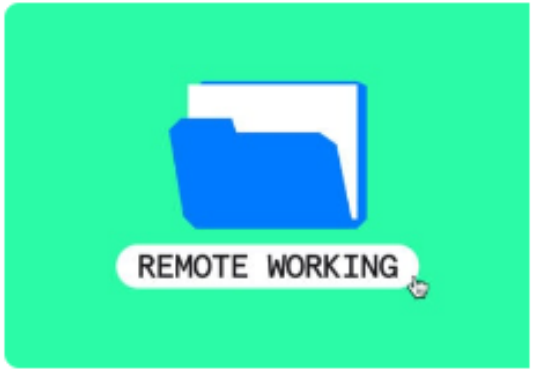
12. Sharepoint phishing fraud targets home workers

April 2021 saw yet another phishing attack emerge that appears **specifically designed to target remote workers using cloud-based software.**

The attack begins when the target receives an email—written in the urgent tone favored by phishing scammers—requesting their signature on a document hosted in Microsoft Sharepoint.

The email looks legitimate. It includes the Sharepoint logo and branding familiar to many office workers. But **the link leads to a phishing site designed to siphon off users' credentials.**

Phishing attacks increasingly aim to exploit remote collaboration software—Microsoft research suggests nearly half of IT professionals cited the need for new collaboration tools as a major security vulnerability during the shift to working from home.



REMOTE WORKING

The Ultimate Guide to Security for Remote Working

by Andrew Webb • Friday, January 28th, 2022

14. High-Profile Twitters Users' Accounts Compromised After Vishing Scam

In July 2020, Twitter lost control of 130 Twitter accounts, including those of some of the world's most famous people — Barack Obama, Joe Biden, and Kanye West.

The hackers downloaded some users' Twitter data, accessed DMs, and made Tweets requesting donations to a Bitcoin wallet. Within minutes — before Twitter could remove the tweets — the perpetrator had earned around $110,000 in Bitcoin across more than 320 transactions.

Twitter has described the incident as a "phone spear phishing" attack (also known as a "vishing" attack). The calls' details remain unclear, but somehow Twitter employees were tricked into revealing account credentials that allowed access to the compromised accounts.

Following the hack, the FBI launched an investigation into Twitter's security procedures. The scandal saw Twitter's share price plummet by 7% in pre-market trading the following day.

15. Texas Attorney-General Warns of Delivery Company Smishing Scam

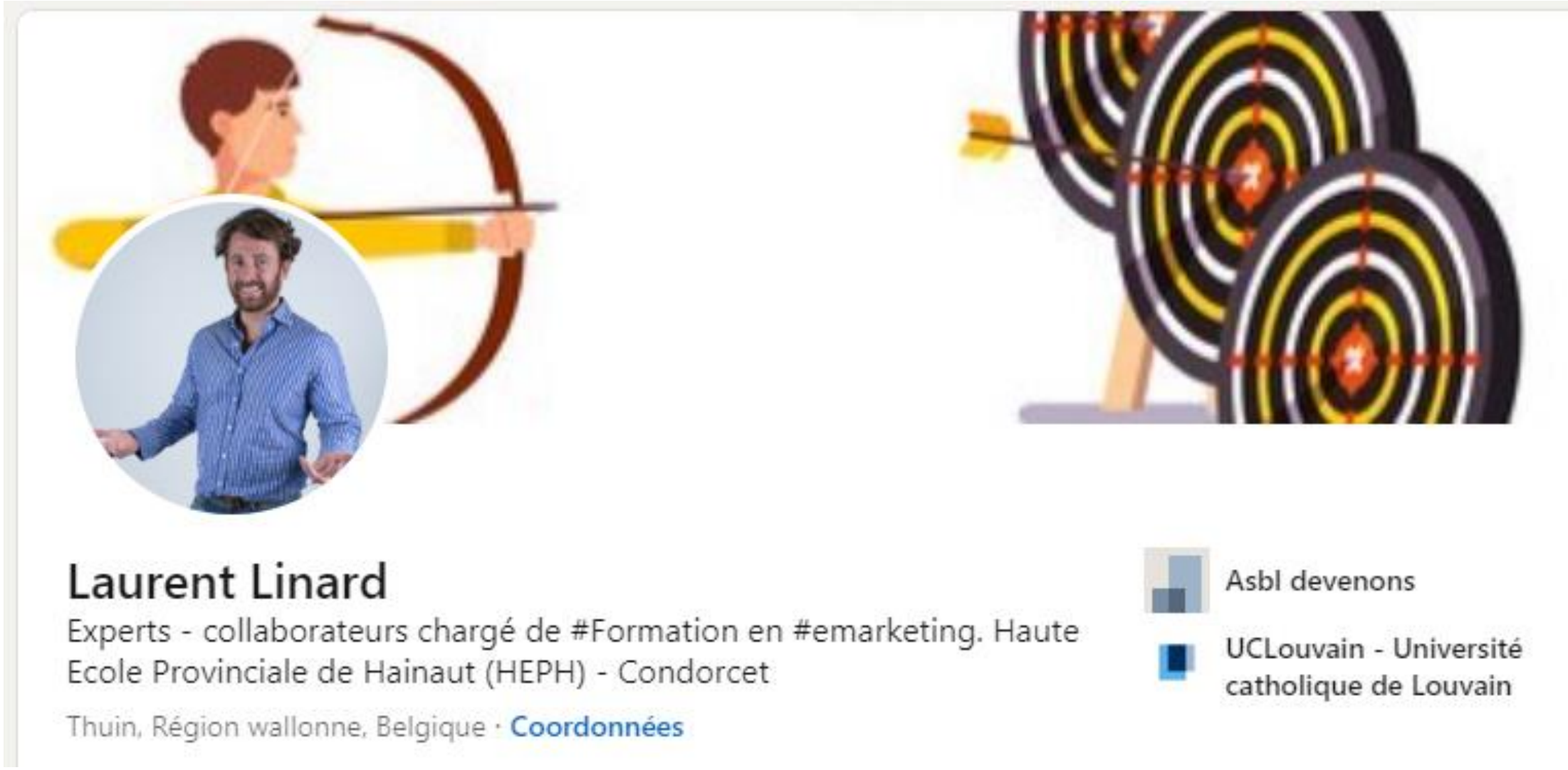
Nearly everyone gets the occasional text message that looks like it could be a potential scam. But in September 2020, one smishing (SMS phishing) attack became so widespread that the Texas Attorney-General put out a press release warning residents about it.

Victims of this scam received a fraudulent text message purporting to be from a delivery company such as DHL, UPS, or FedEx. The SMS invited the target to click a link and "claim ownership" of an undelivered package. After following the link, the target was asked to provide personal information and credit card details.

The Texas Attorney-General warned all Texans not to follow the link. He stated that delivery companies do not communicate with customers in this way, and urged anyone receiving the text message to report it to the Office of the Attorney General or the Federal Trade Commission.

Top tip: Never to respond to any suspicious message, click links within SMS messages, or reveal personal or company information via SMS.

Merci pour votre attention ;)

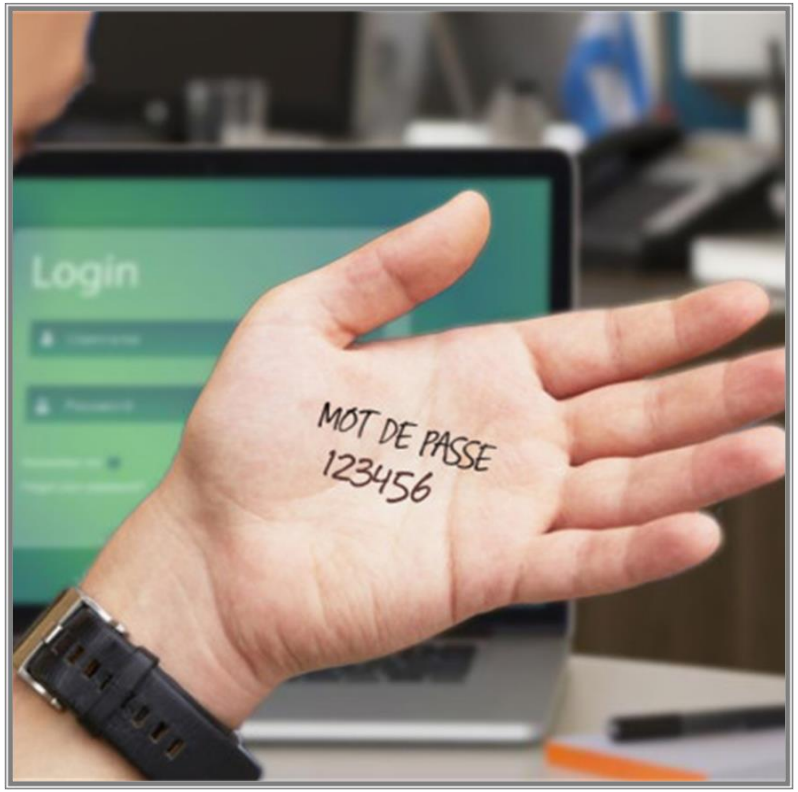


Pour aller un peu plus loin

https://www.ipe.fr/politique-securite-informatique-entreprise/

Les bons réflexes à adopter

Définition d'un mot de passe

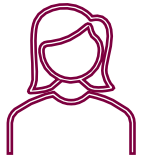


Pas sur la main ! En dessous du clavier ou un post-it

- Pas facile à deviner
  - Mot de passe fort
    - Minimum une autre authentification ;
  - Mot de passe faible (Login/Pass) ;
- Changez régulièrement (OUI et NON) ;
- Un pass différent pour chaque compte ;
- Evitez de l'écrire (post-it) ou en dessous du clavier ou dans votre portefeuille ;
- Ne pas activer la sauvegarde automatique des navigateurs et éventuellement (OS) ;
- Effacez l'historique de navigation de temps en temps ;
- Evitez de le confier à des tiers (Inconnue, Ami, Collègue ou même votre responsable) ;
- Activez la double authentification lorsque c'est possible > **? La M?F?A?**
- Trouvez-vous une formule magique.

L'utilité d'un mot de passe « fort »....

- L'authentification consiste à vérifier l'identité d'un utilisateur.
- Réduire la vulnérabilité



Identifiant
Mot de passe

Matériels

Applications

Données

Documents

Un mot de passe fort est un mot de passe qui est difficile à découvrir par un attaquant dans un temps raisonnable

Ne pas confondre avec authentification forte !

Les bons réflexes à adopter

Résistance d'un mot de passe

- Quelle est la force d'un mot de passe ?
- Ex: Michael (Jackson)

Pas une bonne idée d'utiliser des noms connus … même long.

Mot de passe	Time to crack (2012) – (1)	2018 (2)	2018 (3)	2020 (4)	2022 GO !
michael	2 Sec	0.22 s	- 0 sec	- 0 sec	
MichaeL	6 min et 2 sec	18 h 58 min	- 0 sec	- 25 sec	
M1chaeL	20 min et 40 sec	2 J 16 h 59 m	0.01 sec	1 min	
M1ch@eL	6 h et 20 min	1 M 1 S 5 D 21 H	0.01 sec	6 min	
jatl|Dd@M	2 ans et 4 mois	Infinity	5 ans	2 mois	
jatl|Dd@MJ	198 ans et 26 jours	Infinity	391 ans	17 ans	
:Jemangedesbananas	490978540809316900 ?	Infinity	800 ans	1 quadrillion	

DITES : Phrases PASS

(1) https://random-ize.com/how-long-to-hack-pass

(2) https://www.betterbuys.com/estimating-password-cracking-times/

(3) https://www.my1login.com/resources/password-strength-test/

(4) : https://www.security.org/how-secure-is-my-password

Construction d'un mot de passe

- **Caractères spéciaux** $^ù*!:à) -> 28 éléments
- **Lettres majuscules** ABC… -> 26 éléments

Lettres minuscules abc… -> 26 éléments

Chiffres 123… -> 10 éléments

Et l'Espace ?

- **$#3j~Zw?sYZ5**

- 12 caractères

:C'Est1000FoisFacileàRetenir

28 caractères → THE BEST : La Phrase Passe

Les bons réflexes à adopter

Les mots de passe les + utilisés **A éviter !!!!!!**

Construction d'une authentification FORTE

- **UNE PHRASE PASSE ou une FORMULE**
- Utilisez >16 à 20 caractères au minimum ;
- Adoptez les recommandations vues avant ! ☺
- **(1) LA FORMULE ou La Phrase Passe (+IchMange100ApplesEt2Bananas)**
  - TRUC : Mélangez les langues… + Inscrivez les chiffres au milieu
- **(2) CONFIGUREZ le MFA***
  - Téléchargez une APPS sécure
  - SCANNEZ le QR Code en fonction du compte
  - RISQUES du MFA ?
    - IMPRIMEZ les CODES de Récupération !!!
    - Cachez les ☺
  - Utilisez le multi-facteur un maximum (Exemples)

***SINCE 1990 ☺**

Commandement 1

1

Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez

Commandements 2

2

Ne mélangez pas votre messagerie professionnelle et personnelle

Commandements 3

3

Ayez une utilisation responsable d’internet au travail

Commandements 4

4

Maitrisez la confidentialité de vos informations sur les réseaux sociaux

Commandements 5

5

N’utilisez pas de service de stockage en ligne personnel à des fins professionnels

Commandements 6

6

Faites les mises à jour de sécurité de vos équipements et mises à jour applicatives (ne les reportez pas)

Commandements 7

7

Utilisez une solution de sécurité contre les virus et autres attaques

Commandements 8

8

Installez sur votre smartphone que des applications connues (vérifiez les commentaires) et cherchez des exemples de failles.

TAPEZ le nom du logiciel +Faille dans le moteur de recherche

Commandements 9

9

Méfiez-vous des supports USB

Commandements 10

10

Evitez les réseaux Wi-Fi publics ou inconnus

l’environnement de travail: La sécurité de votre espace de travail

- Ne laissez pas votre appareil sans surveillance !
- Verrouillez votre session quand vous quittez votre poste de travail.
- Rangez votre bureau (ne pas laisser des documents importants à vue !!!).
- Effacez le tableau blanc … s’il contient des informations confidentielles.

La sécurité sur les réseaux sociaux

- Ne communiquez pas vos données personnelles (date de naissance, adresse, N° téléphone)
- **Vérifiez vos paramètres de confidentialité**
  - Configurez les !
  - Renseignez-vous
- **Maitrisez vos publications**
- Faites attention à qui vous parlez ou chattez
- Contrôlez les applications (trop intrusives)
- Supprimez votre compte si vous ne l'utilisez plus

Wifi lieux publics / Pirates inspirants

https://www.youtube.com/watch?v=LiRVDHC3skA

https://www.youtube.com/watch?v=N_WH3rQCPi8

A vous de jouer à la pêche

Êtes-vous aguerri ou tombez-vous facilement
dans le panneau du phishing ?
Faites le test : ligne

Vidéos intéressantes à voir et revoir

- Ransonware part 1 : https://www.youtube.com/watch?v=K3ctVjz4NvU
- Ransonware part 2 : https://www.youtube.com/watch?v=pooeMsv9qJ0
  - Ca parle des mots de passe, conseil , double authentification
- RGPD c'est quoi ? https://www.youtube.com/watch?v=hYwHaZj57zQ
- Télétravail : Attention chez vous : https://www.youtube.com/watch?v=w6AbMNCyoTE

- Vos métadonnées sous surveillance : https://www.youtube.com/watch?v=kz3Zb_Y_wJw
- Les 5 pirates qui glacent le sang ! https://www.youtube.com/watch?v=N_WH3rQCPi8
- Piraté un WIFI gratuit > Facile: https://www.youtube.com/watch?v=LiRVDHC3skA
- Mot de passe fort : https://www.youtube.com/shorts/rcuemQFAP_U
- Cliquez pas sur tout ce qui bouge :https://www.youtube.com/watch?v=lfoe5Ldn-AI
- Média sociaux : se protéger : https://www.youtube.com/watch?v=i007ntqNOGQ

Lecture et vidéo !

SafeOnWeb c’est du Belge

- **Au secours! J'ai cliqué sur un faux lien**
- https://www.safeonweb.be/index.php/fr/au-secours-jai-clique-sur-un-faux-lien
- **Soyez malin. Déjouez le phishing.**
- https://campagne.safeonweb.be/fr/phishing
- **Les mots de passe, c’est dépassé**
- https://campagne.safeonweb.be/fr/authentification-a-2-facteurs
- **Savez-vous à quoi vous devez être attentif(ve) en cas de messages suspects ?**
- https://www.safeonweb.be/fr/quiz/test-du-phishing
- **Ne vous laissez pas prendre en otage !**
- https://www.youtube.com/watch?v=g8mI58jtqJM
- **Récupérons internet - 15sec spot**
- https://www.youtube.com/watch?v=0Ti_M5I7edw
- Protection des données et RGPD (1/2)
- https://www.youtube.com/watch?v=RDqi3u4A1lg
- Protection des données et RGPD (2/2)
- https://www.youtube.com/watch?v=ymePTcFh0T4
- Protégez vos employés - Phishing
- https://www.youtube.com/watch?v=sIwpybDGjpE

Lecture et vidéo !

SafeOnWeb c'est du Belge

- Identifiez-vous les faux messages à temps ? :
- https://www.youtube.com/watch?v=quDdky4m-G4
- Allez les belges, boostez votre santé digitale!
- https://www.youtube.com/watch?v=yQHtN8EvvXk
- Protégez vos employés avec des bons Mots de passe
- https://www.youtube.com/watch?v=l6Qmmvm-620
- Incident response: Comment ce préparer à une cyberattaque
- https://www.youtube.com/watch?v=ETtBwTZWsm4
- Incident response: Que faire après une cyberattaque?
- https://www.youtube.com/watch?v=UbMMWqKzHQ0
- Incident Response - Arrêter l'attaque
- https://www.youtube.com/watch?v=yHkmUxpvrgI

Sensibilisation à la sécurité de l'information

- Merci pour votre participation !