OUCH ! Mai 2025

OUCH!

SANS SECURITY AWARENESS

La lettre d'information mensuelle de sensibilisation à la sécurité pour vous

Comment les cybercriminels exploitent vos émotions

Un message qui coûte cher

Emma venait de quitter le supermarché, les bras pleins de sacs, lorsque son téléphone a sonné avec un message de sa fille.

"Maman ! J'ai perdu mon téléphone ! J'utilise celui d'un ami. J'ai besoin d'argent pour en acheter un nouveau. Envoie-moi 800€ maintenant s'il te plaît. Je t'explique plus tard !"

Son cœur a fait un bond. Sa fille, Angie, était partie à l'université et Emma savait à quel point son téléphone était important pour les cours, le travail et garder contact. L'imaginer seule sans téléphone l'a rendue anxieuse. Elle a rapidement répondu :

*"**Tu vas bien ? Qu'est-ce qui s'est passé ?"***

La réponse est arrivée presque aussitôt.

"Ça va, mais je ne peux pas parler. J'ai emprunté le téléphone d'un ami. Tu peux m'envoyer l'argent maintenant ? Il faut que j'en achète un nouveau très vite. Je t'appelle ce soir. Je t'aime !"

Emma a hésité un moment. Quelque chose lui paraissait étrange, mais son inquiétude a surpassé ses doutes. Elle a ouvert son application bancaire et a transféré 800€ au numéro de téléphone partagé dans les messages. Elle ne s'est même pas demandé pourquoi le virement n'était pas fait directement sur le compte de sa fille ; peut-être qu'Angie ne pouvait pas y accéder sans son téléphone.

Plus tard dans la soirée, elle a appelé le vrai numéro d'Angie, s'attendant à entendre du soulagement dans sa voix. Au lieu de cela, elle a répondu normalement.

"Coucou Maman ! Ça va ?"

Emme s'est figée

"Tu as reçu l'argent ?"

Angie avait l'air perdue.

"Quel argent ?"

Le ventre d'Emma s'est noué. Elle a ouvert les messages à nouveau, pour les lire avec un œil neuf. Le ton pressant, le manque de précisions et l'insistance sur le fait de payer immédiatement, tous ces éléments étaient des indices d'une **arnaque**. Un escroc s'était fait passer pour sa fille, conscient qu'une mère paniquée ne s'arrêterait pas pour vérifier.

© SANS Institute 2025

Malheureusement, elle n'est pas la seule personne à qui cela arrive. Chaque jour, les cybercriminels manipulent les émotions pour inciter les gens à commettre des erreurs coûteuses. Voici cinq déclencheurs émotionnels courants qu'ils exploitent et comment les repérer avant qu'il ne soit trop tard.

1. L'urgence : "Si vous n'agissez pas immédiatement, vous perdez quelque chose"

Les escrocs créent une pression temporelle artificielle pour vous pousser à commettre des erreurs.

Comment cela fonctionne :

"Votre compte bancaire a été compromis ! Vérifiez votre identité dans les deux heures, sinon votre compte sera bloqué."

- *"Votre paiement a été validé" (alors que vous n'avez rien acheté)*
- *"Votre mot de passe est sur le point d'expirer ! Mettez-le à jour immédiatement ici."*

Comment repérer cela :

- Contactez directement l'entreprise en utilisant les coordonnées officielles, par exemple en appelant un numéro de téléphone de confiance ou en utilisant l'application mobile de l'entreprise.
- Recherchez des détails vagues dans le message ; les entreprises légitimes fournissent des détails précis, mais ne menacent pas.

2. La peur : "Quelque chose de grave va se produire"

Les cybercriminels utilisent la peur pour créer la panique, poussant les victimes à agir sans réfléchir.

Comment cela fonctionne :

- *"Ici le gouvernement. Vous avez des arriérés d'impôts et vous devez les payer immédiatement, sinon vous serez arrêté."*
- *"Un virus a été détecté sur votre appareil ! Appelez ce numéro pour obtenir de l'aide."*
- *"Si vous ne payez pas cette rançon, vos photos privées seront divulguées."*

Comment repérer cela :

- Les agences gouvernementales ne profèrent pas de menaces par message ou par email.
- Les entreprises technologiques ne vous contactent pas pour réparer votre ordinateur.

3. La curiosité : "Vous n'allez pas en revenir !"

Les escrocs exploitent la curiosité en utilisant des messages choquants ou séduisants.

Comment cela fonctionne :

- *"C'est une vidéo de toi ? 😲" (avec un lien infecté)*
- *"Dernières nouvelles ! Énorme scandale de célébrité. Cliquez ici pour voir."*
- *"Ton ami t'a identifié dans une publication incroyable !"*

Comment repérer cela :

- Méfiez-vous des messages sensationnels.
- Vérifiez auprès de l'expéditeur avant de cliquer sur quoi que ce soit.

© SANS Institute 2025

4. La confiance et l'autorité : "C'est quelqu'un que vous connaissez"

Les cybercriminels se font passer pour des personnes de confiance : patrons, banques ou même proches.

Comment cela fonctionne :

- *"Coucou Maman, c'est moi ! J'ai perdu mon téléphone. Tu peux m'envoyer de l'argent ?"*
- *"Ici votre patron. J'ai besoin que vous achetiez des cartes-cadeaux pour un événement de bureau."*
- *"Nous avons détecté une activité suspecte sur votre compte. Cliquez ici pour le sécuriser."*

Comment repérer cela :

- Créez une phrase secrète avec les membres de votre famille pour vérifier l'identité de chacun.
- Cherchez les détails vagues : les escrocs ne connaissent souvent pas votre nom ou votre adresse postale.
- Méfiez-vous des demandes inhabituelles, en particulier celles qui concernent de l'argent ou des informations sensibles.

5. L'excitation et la cupidité - "Vous avez gagné quelque chose d'extraordinaire !"

Les escroqueries "trop belles pour être vraies" s'appuient sur le désir de récompenses ou d'attention des gens.

Comment cela fonctionne :

- *"Félicitations ! Vous avez gagné un iPhone gratuit ! Réclamez-le maintenant !*
- *"Vous semblez être une personne merveilleuse, parlez-moi un peu de vous."*
- *"Vous avez été sélectionné pour une opportunité d'investissement exclusive."*

Comment repérer cela :

- Si vous n'avez pas participé, vous n'avez pas gagné. Les entreprises légitimes ne demandent pas de frais pour réclamer les prix.
- Méfiez-vous des étrangers qui persistent à vous proposer quelque chose de "trop beau pour être vrai" ou qui expriment trop rapidement des sentiments romantiques.
- Méfiez-vous des offres "exclusives" envoyées au hasard.

La prochaine fois que vous recevrez un message ou un appel urgent, faites une pause, réfléchissez et vérifiez avant d'agir. Ne laissez pas les émotions être votre faiblesse !

Rédacteur invité

Teressa Gehrke est la fondatrice de PopCykol, une société de sensibilisation à la sécurité en ligne. Elle a plus de 10 ans d'expérience dans l'industrie en tant que rédactrice technique, conceptrice UX et chef de projet. Elle est membre du conseil d'administration de WiCyS Colorado. Teressa est une musicienne primée. Linktree

Ressources

Les escroqueries à l'investissement fondées sur le romantisme : https://www.sans.org/newsletters/ouch/sweet-talk-empty-wallet-romance-fueled-investment-scams/
Se défendre contre les attaques de clonage vocal : https://www.sans.org/newsletters/ouch/phantom-voices-defend-against-voice-cloning-attacks/
Attaques par SMS : Une saga de smishing : https://www.sans.org/newsletters/ouch/text-messaging-attacks-smishing-saga/

Traduit pour la communauté par : Juliette Busson
OUCH ! Est publié par SANS Security Awareness et distribué sous la licence Creative Commons BY-NC-ND 4.0. Vous êtes libre de partager ou de distribuer cette lettre d'information tant que vous ne la vendez pas ou ne la modifiez pas. Comité de rédaction : Phil Hoffman, Leslie Ridout, Princess Young.