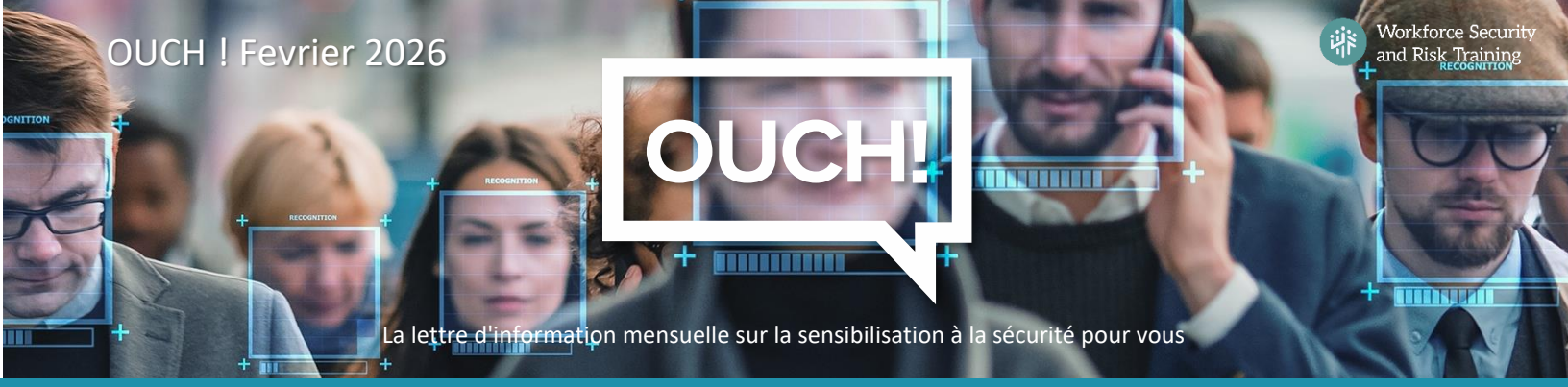

Se protéger dans un monde où la véritable confidentialité est impossible

Ce faux appel semblait trop réel

Tout a commencé avec un appel qui semblait ordinaire. "Allo, Mme Patel ? Ici Michael du département de lutte contre la fraude. Nous avons remarqué une activité inhabituelle sur votre compte. Avez-vous récemment fait un achat de 1,200$ dans un magasin éléctronique ? Mme Patel a commencé à paniquer. Elle n'avait rien acheté récemment.

Pour rendre son appel plus convaincant, "Michael" a confirmé son adresse et sa date de naissance, des informations qu'elle pensait que seule sa banque pouvait connaître. Il lui a expliqué que pour être remboursée, elle devait vérifier son identité en fournissant sa carte de crédit et ses identifiants et mot de passe bancaires. Elle s'est exécutée. Son interlocuteur l'a remerciée et lui a assuré que le problème serait réglé. Mais quelques heures plus tard, Mme Patel ne pouvait plus se connecter à son compte bancaire. Puis elle a commencé à recevoir des notifications indiquant que des milliers de dollars avaient été transférés à l'étranger depuis son compte.

Ce que Mme Patel n'avait pas compris était que l'arnaqueur avait obtenu ses informations personnelles grâce à une faille précédente et l'avait utilisée pour rendre son appel crédible. Tout dans cet appel était faux. Elle venait de s'être fait arnaquer.

Nos données sont partout

Dans le monde connecté d'aujourd'hui, la confidentialité est devenue l'une des choses les plus difficiles à protéger. Chaque fois que nous achetons en ligne, regardons un film, utilisons notre carde de crédit, conduisons sur l'autoroute ou utilisons une application mobile, nos données sont collectées, analysées et partagées. De plus, la plupart de nos données personnelles peuvent être accessibles au public, stockées dans les bases de données gouvernementales d'inscription sur les listes électorales, les dossiers fiscaux ou les données relatives à l'achat d'une maison. Même marcher dans un parking peut être filmé par les caméras de sécurité installées dans la plupart des voitures modernes.

Peu importe les personnes qui collectent ces informations ou leurs motivations, le résultat est le même : une quantité considérable de données personnelles est stockée dans des bases de données à travers le monde, sur lesquelles vous n'avez aucun contrôle. Et une fois que ces informations existent, elles peuvent être volées, vendues, partagées ou utilisées à mauvais escient. Il est pratiquement impossible d'atteindre une véritable confidentialité.

Ce n'est pas parce qu'ils vous connaissent qu'ils sont légitimes

Les attaquants utilisent souvent toutes ces informations accessibles vous concernant pour rendre leurs arnaques plus crédibles. Par exemple :

1. Un escroc pourrait vous appeler en se faisant passer pour un employé de votre banque et vous demander de confirmer votre adresse avant de vous demander votre identifiant et votre numéro de compte.
2. Un email peut inclure votre nom complet, votre numéro de téléphone et une date de naissance pour paraître légitime.
3. Un SMS peut sembler provenir d'un service de garantie automobile, avec des détails sur la marque, le modèle et l'année de l'une de vos voitures.

En réalité, le fait de détenir des informations personnelles vous concernant ne rend pas quelqu'un digne de confiance, cela le rend seulement plus convaincant. Soyez toujours méfiant face aux messages, appels et courriels inattendus, même si l'expéditeur semble "bien vous connaître" ou que le message semble urgent. N'hésitez pas à raccorcher et appeler l'institution sur un numéro de téléphone fiable.

Surveillez votre argent. C'est là que l'arnaque commence

Comme vous ne pouvez pas protéger toutes vos informations, la meilleure défense est la **détection précoce**. Surveiller vos comptes financiers vous offre un avantage décisif : vous pouvez détecter toute activité suspecte avant qu'elle ne cause de réels dommages. Plus vite vous remarquez une transaction frauduleuse, plus il est facile de l'annuler et d'éviter d'autres pertes. Voici quelques mesures simples que tout le monde peut prendre :

- **Configurez des alertes :** la plupart des banques, des cartes de crédit et des services d'investissement vous permettent de recevoir des SMS instantanés pour chaque transaction, retrait ou tentative de connexion.
- **Vérifiez régulièrement vos comptes :** même si vous recevez des alertes, prenez quelques minutes chaque semaine pour vérifier vos comptes et vos activités récentes afin de détecter toute anomalie. Ou configurez vos comptes pour recevoir des rapports quotidiens ou hebdomadaires par email.
- **Gelez votre crédit :** selon votre pays, vous pouvez geler votre crédit afin que personne ne puisse contracter un prêt ou obtenir une carte de crédit à votre nom. Vous pouvez également accéder à des relevés gratuits ou à faible coût auprès des agences d'évaluation du crédit. Recherchez les comptes ou les demandes inhabituels.

Dans le monde actuel, il n'est plus possible d'avoir une vie privée parfaite. N'oubliez jamais que le simple fait qu'une personne détienne des informations vous concernant ne la rend pas légitime. Vous n'avez pas besoin d'être un expert en cybersécurité pour rester en sécurité : il suffit d'être vigilant, de poser des questions et de surveiller vos comptes.

Rédacteur invité

Le Dr Litany Lineberry, secrétaire de la filiale Éducation et formation de WiCyS, est titulaire d'un doctorat en ingénierie avec une spécialisation en cybersécurité. Elle enseigne les technologies des systèmes d'information au Hinds Community College, campus d'Utica, et soutient la mission de WiCyS qui consiste à recruter, retenir et promouvoir les femmes dans le domaine de la cybersécurité dans tous les secteurs. https://www.linkedin.com/in/litany-lineberry

Ressources

Comment les cyber-criminels exploitent vos émotions : https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
Comment les cybercriminels volent vos mots de passe : https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
Verrouiller vos comptes bancaires : https://www.sans.org/newsletters/ouch/dont-let-cybercriminals-swipe-your-savings-lock-down-your-financial-accounts/

Traduit pour la communauté par : Juliette Busson

Vous pouvez trouver plus de contenu OUCH! Sur le lien suivant : https://www.sans.org/newsletters/ouch