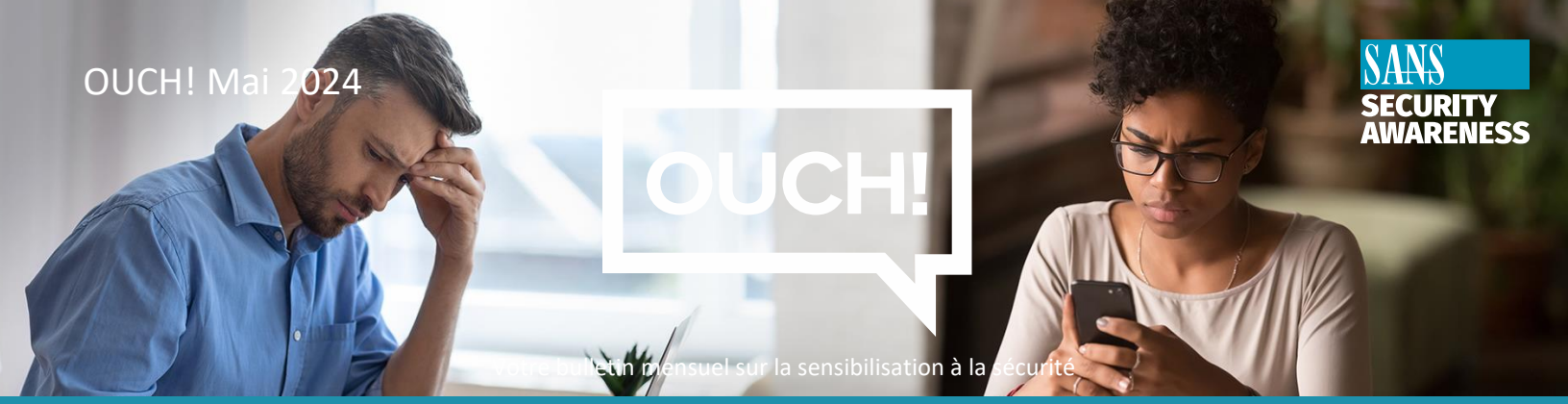

Les trois principaux moyens utilisés par les cyberattaquants pour vous piéger

Aperçu

Les attaques par ingénierie sociale, dans lesquelles les attaquants incitent les gens à faire quelque chose qu'ils ne devraient pas faire, sont l'une des méthodes les plus courantes utilisées par les cybercriminels pour cibler les gens. Ce concept est utilisé par les escrocs et les fraudeurs depuis des milliers d'années. Ce qui est nouveau, c'est qu'avec internet, il est très facile pour un cybercriminel, où qu'il se trouve dans le monde, de se faire passer pour qui il veut et de cibler qui il veut. Vous trouverez ci-dessous les trois types les plus courants de méthodes d'ingénierie sociale que les cyberattaquants utiliseront pour tenter de vous séduire et de vous tromper.

L'hameçonnage

L'hameçonnage est l'attaque d'ingénierie sociale la plus traditionnelle ; il s'agit de l'envoi par des cyber-attaquants d'un e-mail visant à vous inciter à entreprendre une action que vous n'auriez pas dû faire. À l'origine, on l'appelait hameçonnage parce qu'il s'agissait d'une pêche dans un lac : Vous lanciez une ligne et un hameçon, mais vous n'aviez aucune idée de ce que vous alliez attraper. La stratégie sous-jacente à cette tactique était que plus les cybercriminels envoyaient de courriels d'hameçonnage, plus le nombre de victimes augmentait. Les attaques par hameçonnage d'aujourd'hui sont devenues à la fois beaucoup plus sophistiquées et plus ciblées (parfois appelées spear phishing), et les cyberattaquants personnalisent souvent leurs emails d'hameçonnage avant de les envoyer.

SMiShing

Le smishing est essentiellement un hameçonnage par SMS, dans lequel un message texte est envoyé au lieu d'un e-mail. Les cyberattaquants envoient des messages texte sur votre téléphone via des applications telles que iMessage, Google Messages ou WhatsApp. Plusieurs raisons expliquent la popularité du smishing. La première est qu'il est beaucoup plus difficile de filtrer les attaques par messagerie que par e-mail. Deuxièmement, les messages envoyés par les cyberattaquants sont souvent très courts, ce qui signifie qu'il y a très peu de contexte et qu'il est donc beaucoup plus difficile de déterminer si le message est légitime ou non. Troisièmement, le message est souvent plus informel et basé sur l'action, de sorte que les gens ont l'habitude de répondre rapidement aux messages ou d'agir en conséquence. Enfin, les gens repèrent de mieux en mieux les attaques d'hameçonnage par e-mail, de sorte que les cyberattaquants passent tout simplement à une nouvelle méthode, celle par messages.

Hameçonnage par téléphone

L'hameçonnage par téléphone est une tactique qui utilise un appel téléphonique ou un message vocal plutôt qu'un e-mail ou un message texte. Les attaques d'hameçonnage par téléphone prennent beaucoup plus de temps à exécuter pour l'attaquant, car elles s'adressent directement à la victime et interagissent avec elle. Cependant, ces types d'attaques sont également beaucoup plus efficaces, car il est beaucoup plus facile de créer des émotions fortes par téléphone, tel que le sentiment d'urgence. Une fois qu'un cyber-attaquant vous a au téléphone, il ne vous laissera pas raccrocher tant qu'il n'aura pas obtenu ce qu'il veut.

© SANS Institute 2023

Repérer et arrêter ces attaques

Heureusement, peu importe la méthode utilisée par les cyberattaquants, il existe des indices communs que vous pouvez repérer :

- **L'urgence** : tout message qui crée un énorme sentiment d'urgence dans lequel les attaquants essaient de vous pousser à agir rapidement et à commettre une erreur. Par exemple, un message prétendant provenir du gouvernement et vous indiquant que vos impôts sont en retard et que si vous ne payez pas immédiatement, vous finirez en prison.

- **La pression** : tout message incitant un employé à ignorer ou à contourner les politiques et procédures de sécurité de l'entreprise.

- **La curiosité** : tout message qui suscite une grande curiosité ou qui semble trop beau pour être vrai, tel qu'un colis UPS non livré ou un avis indiquant que vous allez recevoir un remboursement Amazon.

- **Le ton** : tout message semblant provenir d'une personne que vous connaissez, par exemple un collègue de travail, mais dont la formulation ne lui ressemble pas, ou dont le ton général ou la signature n'est pas le sien.

- **Les informations sensibles** : Tout message demandant des informations très sensibles, telles que votre mot de passe ou votre carte de crédit.

- **Générique** : un message provenant d'une organisation de confiance mais utilisant une salutation générique telle que "Cher client". Si Amazon a un colis pour vous ou si le service téléphonique a un problème de facturation, ils connaissent votre nom.

- **Adresse mail personnelle** : Tout e-mail qui semble provenir d'une organisation, d'un fournisseur ou d'un collègue légitime, mais qui utilise une adresse électronique personnelle comme @gmail.com ou @hotmail.com.

En recherchant ces indices fréquents, vous pouvez contribuer à votre protection.

Rédacteur Invité

Mary Jane Suarez Partain est directrice du programme Women in CyberSecurity (WiCyS). Son rôle consiste principalement à fournir des ressources, des initiatives et des programmes conçus pour recruter, retenir et faire progresser les femmes dans le domaine de la cybersécurité. Elle est passionnée par la création d'un environnement inclusif où tous se sentent valorisés, bienvenus et vus.

Ressources

Stop aux appels téléphoniques frauduleux : https://www.sans.org/newsletters/ouch/stop-phone-call-scams
Les attaques d'hameçonnage deviennent de plus en plus travaillées : https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier
Déclencheurs émotionnels - comment les cyber-attaquants vous piègent-ils ? : https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you
Je me suis fait hacker, et maintenant ? : https://www.sans.org/newsletters/ouch/im-hacked-now-what/

Traduit pour la communauté par : Juliette Busson

OUCH! Est publié par SANS Security Awareness et est distribué sous la licence Creative Commons BY-NC-ND 4.0. Vous êtes libre de partager ou de distribuer ce bulletin d'information, à condition de ne pas le vendre ou le modifier. Comité de rédaction : Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.