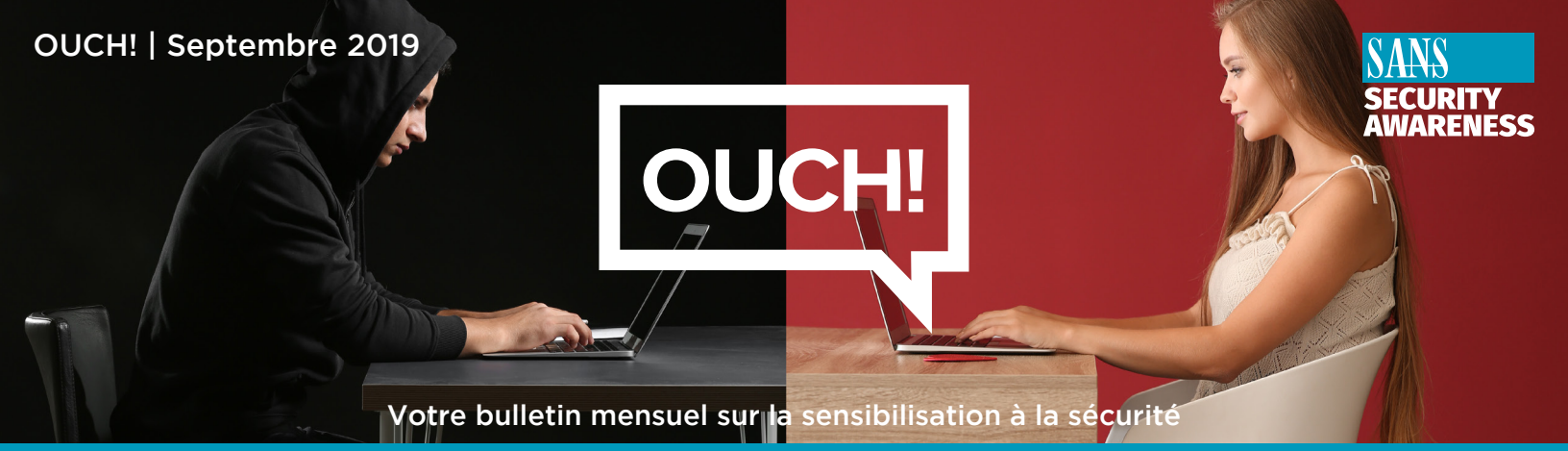
OUCH! | Septembre 2019



Votre bulletin mensuel sur la sensibilisation à la sécurité

L'escroquerie par les réseaux sociaux

Aperçu

Nous sommes nombreux à avoir subi des attaques par hameçonnage, au travail comme à la maison. Ce sont des e-mails qui semblent légitimes, comme de notre banque, patron ou magasin en ligne. Ce sont cependant bien des attaques, tentant de nous amener à faire des erreurs, comme ouvrir une pièce jointe infectée, partager un mot de passe ou transférer de l'argent. Le défi, c'est que plus nous devenons avertis et sachons stopper ces attaques, plus les cybercriminels essaient de nouvelles techniques pour escroquer les personnes.

Des tentatives d'escroquerie peuvent survenir par presque tous les moyens de communication, de Skype, WhatsApp et Slack à Twitter, Facebook, Snapchat, Instagram et même les applications de jeux. La communication à travers ces plateformes peut paraître plus informelle ou sûre. C'est pour cela que les criminels les utilisent pour nous berner. De plus, grâce aux nouvelles technologies, il est de plus en plus facile pour un criminel de prétendre être quelque chose ou quelqu'un qu'il n'est pas, et ce de n'importe où dans le monde. Il est important de se rappeler qu'à travers n'importe quelle moyen de communication, l'interlocuteur n'est pas forcément celui qu'il prétend être.

Points importants

Voici les indices les plus fréquents indiquant que le message reçu ou le poste lu est peut être une attaque.

L'urgence : un message à caractère urgent qui requiert de prendre une « action immédiate » avant que quelque chose de négatif n'arrive, comme la fermeture de votre compte bancaire ou votre arrestation. Le criminel veut vous pousser à faire une erreur.

La pression : vous pousser à contourner ou ignorer les procédures au travail.

La curiosité : un fort sentiment de curiosité ou quelque chose de trop beau pour être vrai. Non, vous n'avez pas gagné au Loto.

La confidentialité : une requête pour des données sensibles, comme votre numéro de carte bancaire, votre mot de passe ou autres informations sensibles.

Les messages officiels : Le message se dit officiel, mais contient des fautes d'orthographe ou de grammaire. La plupart des organisations gouvernementales ne vont pas utiliser les réseaux sociaux pour communiquer avec vous. Si vous doutez de la légitimité d'un message, appelez l'organisation directement en utilisant un numéro sûr, comme celui figurant sur leur site web.

L'usurpation d'identité : vous recevez un message d'un ami ou collègue, mais le ton ou les mots utilisés ne leur ressemblent pas. Si vous êtes suspicieux, appelez-les directement pour vérifier. Il est facile pour un cybercriminel de créer des messages semblant provenir de quelqu'un que vous connaissez. Dans certains cas, ils peuvent pirater le compte d'un ami et prétendre être celui-ci pour vous contacter. Prenez particulièrement garde aux messages courts, comme sur Twitter ou autres, où il est plus difficile de reconnaître la personalité de l'expéditeur.

Vous êtes la meilleure défense contre de telles escroqueries ou attaques. Si un poste ou un message paraît étrange ou suspicieux, ignorez-le ou effacez-le. S'il provient de quelqu'un que vous connaissez, appelez-les pour confirmer qu'ils vous l'ont bien envoyé.

Rédacteur Invité

Dr Jessica Barker *(@drjessicabarker) est la leader du côté humain de la cybersécurité. Elle est PDG à Cygenta, où elle poursuit sa passion d'influencer positivement la sensibilisation, les comportements et la culture autour de la cybersécurité. Elle siège au ClubCISO et est une conférencière principale connue.*

Ressources

Ingénierie sociale:	https://www.sans.org/u/Uz6
Escroquerie par téléphone:	https://www.sans.org/u/Uzb
Arrêter l'hameçonnage:	https://www.sans.org/u/Uzg
Attaques personnalisées:	https://www.sans.org/u/Uzl