Février 2021 • Vol. 8 n° 2

PASSION AFFAIRES *et technologies*

ARS solutions affaires et technologies

NOUS AIDONS LES ENTREPRISES À TRANSFORMER LEURS TECHNOLOGIES EN LEVIER D'AFFAIRES

« Dans nos rencontres d'équipe, j'ai instauré *la minute informatique*, ce qui me permet de sensibiliser notre personnel à la sécurité informatique...

De nos jours, la cybercriminalité est une réalité et nous n'avons pas d'autre choix que de nous protéger.

Je consulte toutes les informations qu'ARS m'envoie, comme les bulletins et les rapports. Par la suite, je transmets aux employés les informations pertinentes pour les sensibiliser. Ils sont de plus en plus habiles à détecter les courriels frauduleux ou représentant un risque pour la sécurité de nos systèmes.

Ce sont de bonnes habitudes que nous n'avons plus le choix de combiner à une bonne protection antivirus et antipourriel ainsi qu'à une solution de sauvegarde et de relève robuste comme celle d'ARS. »

Louyse Trudel
Agente d'administration
à la direction générale
AQCS

Suivez-nous

Office 365 restera une cible de choix pour les tentatives d'hameçonnage en 2021

Affaires-TI

TEMPS DE LECTURE 1:50

Cette année, **Office 365 continue de présenter une cible de choix pour les malfaiteurs** avec les fraudeurs qui utilisent de nouvelles tactiques telles que le ***consent phishing***, un type de cyberattaques qui consiste à **tromper les victimes pour obtenir leur permission via une application malveillante afin d'accéder à des services légitimes dans le Cloud.**

En 2020, **les incidents d'hameçonnage ont augmenté de 220 %** par rapport à la moyenne annuelle au plus fort de la pandémie mondiale. Les fraudeurs ont rapidement semé la confusion et on a constaté des **pics importants d'activités d'hameçonnage coïncidant de près avec les règles de confinement et l'augmentation du travail à domicile.**

Les fraudeurs sont de plus en plus créatifs en ce qui concerne les noms et les lieux de leurs sites d'hameçonnage. En essayant de créer des adresses de sites Web toujours plus réalistes, **55 % des sites d'hameçonnage ont utilisé des noms de marques dans leur URL**. Il ne faut que **4 heures en moyenne après l'entrée des informations** de paiement par la victime sur un site Web frauduleux **avant que les cybercriminels commencent à les utiliser**.

Étant donné la croissance continue des attaques d'hameçonnage, les simulations d'hameçonnage et la formation continue de vos employés demeurent essentielles pour la combattre.

Comment repérer un courriel d'hameçonnage

TEMPS DE LECTURE 2:50

De **récentes cyberattaques par hameçonnage dans tous les secteurs géographiques** nous amènent à vous faire penser de redoubler de prudence. Un courriel d'hameçonnage est un **faux courriel qui est soigneusement conçu pour ressembler à une demande légitime (ou à un fichier joint) provenant d'un site en qui vous avez confiance dans le but de vous inciter à donner volontairement vos renseignements** de connexion à un site Web particulier ou à cliquer et télécharger un virus.

Souvent, ces courriels semblent légitimes et se présentent sous la forme d'un PDF (document numérisé) ou d'un numéro de suivi UPS ou FedEx, lettre bancaire, alerte Facebook, avis bancaire, etc. C'est ce qui les rend si dangereux - ils paraissent exactement comme un courriel légitime.

Alors, comment distinguer un courriel d'hameçonnage d'un courriel légitime? Voici quelques signes révélateurs...

Tout d'abord, **passez la souris sur l'URL du courriel (mais NE CLIQUEZ PAS!)** pour voir le site Web RÉEL vers lequel vous serez dirigé. S'il y a un lien URL suspect, supprimez immédiatement le courriel. En fait, c'est une bonne pratique **d'aller directement sur le site (en le tapant dans votre navigateur)** plutôt que de cliquer sur le lien pour accéder à un site particulier. **Un autre signe révélateur est une mauvaise grammaire et des fautes d'orthographe.** Le courriel peut également vous demander de "vérifier" ou de "valider" votre connexion ou des informations personnelles. Pourquoi votre banque aurait-elle besoin que vous vérifiiez votre numéro de compte? Ils devraient déjà avoir cette information. Et enfin, **si l'offre semble trop belle pour être vraie, elle l'est probablement.**

ATTENTION : certains cybercriminels vont tenter de tirer profit de l'actualité, comme c'est le cas avec la propagation du coronavirus. Selon la télémétrie d'IBM X-Force et de Kaspersky, une vague de courriels malveillants, pilotés par des robots, a pour thème le coronavirus. Les courriels prétendent avoir joint des avis concernant les mesures de prévention du virus alors qu'il ne s'agit que d'un prétexte pour en distribuer un autre.

L'objet des courriels contient la date du jour et un mot comme "notification" afin de donner un sentiment d'urgence. Le courriel invite le lecteur à consulter le document ci-joint. Il comporte également un pied de page avec une adresse postale, un numéro de téléphone et un numéro de fax légitimes de la santé publique, afin de donner un air d'authenticité. **Malheureusement, il est assez fréquent que les acteurs de la menace exploitent des émotions humaines comme la peur, surtout si un événement mondial a déjà provoqué la terreur et la panique...**

Webinaire pour les dirigeants

Ce n'est pas le temps pour votre entreprise de vivre tous les problèmes qu'engendre une cyberattaque. Éliminez le stress d'en être victime et restez concentré sur la croissance de votre entreprise!

Au cours de ce webinaire, vous découvrirez :

- Stratégies à mettre en place
- Rôles et responsabilités des dirigeants
- Les rapports de gouvernance à utiliser
- Les indicateurs clés à valider

Intéressé à y participer ? Contactez-nous pour obtenir les détails - info@ars-solutions.ca • 418 872-4744 #233

Méfiez-vous de l'hameçonnage vocal

TEMPS DE LECTURE 2:50

Les fraudeurs utilisent le téléphone pour demander aux victimes peu méfiantes des informations personnelles ou financières. Cette technique d'hameçonnage vocal est plus communément appelée "vishing".

À quoi faut-il faire attention?

Sentiment d'urgence

En ingénierie sociale, on tente souvent d'ajouter un sentiment d'urgence. C'est d'ailleurs l'indice le plus criant. Par exemple, l'appel à l'action rapide peut être émise par un objet de courriel contenant la date du jour et le mot "notification".

Données personnelles

Elles peuvent être collectées sur les profils de médias sociaux, fournissant des informations confidentielles aux criminels, ce qui rend les attaques plus crédibles.

Tactiques d'intimidation

Les fraudeurs utilisent des tactiques d'intimidation, en vous faisant croire que votre argent est en danger et que vous devez donc agir rapidement.

Des tactiques de persuasion par téléphone

Les tactiques qui semblent trop bonnes pour être vraies sont en général un signe d'activités criminelles. Par exemple, le numéro suivant : Phoenix, AZ 555-555-5555. Les fraudeurs modifient leur numéro de téléphone ou leur identification pour masquer l'origine réelle de leurs appels.

Les fraudeurs appellent en tant qu'agents officiels du service des impôts

Un rapport du département des impôts montre que 2 013 896 000 personnes ont été contactées par des fraudeurs se faisant passer pour des agents officiels du service des impôts. **5 000 DE CES VICTIMES ONT PAYÉ UN TOTAL DE PLUS DE 26.5 MILLIONS DE DOLLARS.**

N'oublions pas de faire la fête au travail

3:00 TEMPS DE LECTURE

Notre monde a basculé le 13 mars 2020 avec le début officiel du confinement relié à la pandémie. Ce qui se faisait auparavant en face à face se fait désormais de la maison ou avec le plus de distanciation possible. Le télétravail et la distanciation physique sont désormais la norme, une réalité qui perdurera tant que le virus de la COVID-19 sera présent. Tout au long de la dernière année, s'il y a une chose que la pandémie nous a confirmée de façon incontestable, c'est que l'humain est bel et bien un être fondamentalement social.

Vouloir faire partie d'un groupe et sentir qu'on y a sa place est un sentiment fort, mais la crise actuelle nous oblige à **trouver de nouveaux moyens pour échanger les uns avec les autres.** Si certaines personnes en télétravail à la maison apprécient les horaires plus souples et s'acclimatent bien à devoir travailler seules, d'autres se sentent isolées et sont plus anxieuses qu'avant.

On remarque que les **discussions virtuelles tendent à être plus brèves et plutôt axées sur le travail,** et non sur la dimension humaine. Les nouvelles structures organisationnelles tendent aussi à isoler la personne de ses collègues ou patrons. Cela peut se traduire par **moins de soutien émotionnel,** comme l'écoute, le respect et l'empathie, ou de soutien opérationnel, comme l'aide dans l'accomplissement de tâches et le partage des responsabilités. Un faible soutien social des collègues peut aussi se traduire par moins de travail d'équipe et de partage d'informations.

Bien qu'il ne soit plus à démontrer que de nourrir ce qui fait du bien et d'encourager le soutien social soient des facteurs de protection puissants pour la santé mentale, plusieurs milieux de travail ont été grandement éprouvés au cours des derniers mois et ont oublié l'importance de ces actions.

Pourtant, plus le soutien social est élevé, **plus le niveau de détresse psychologique tend à diminuer.** La preuve : une étude de l'Université Laval menée au printemps dernier **montre que la détresse psychologique a atteint 55 % chez les travailleuses et 41 % chez les travailleurs pendant le confinement au printemps dernier. Malgré ces chiffres alarmants, on remarque que ceux et celles qui ont bénéficié du soutien de leurs collègues pendant le confinement ont vécu 14 % moins de détresse psychologique.** Les données recueillies démontrent aussi que les milieux de travail bienveillants s'en sortent beaucoup mieux. Dans les entreprises où l'on encourage le dialogue sur la santé mentale, on constate 24 % moins de détresse psychologique comparativement aux entreprises où la santé mentale n'est pas priorisée par la direction.

Pourtant, **miser sur le soutien social,** qu'il soit en personne ou à distance, comme moyen de prévention en santé mentale peut rapporter beaucoup. C'est pourquoi mettre en place des initiatives ludiques, **comme participer à un 5 à 7 virtuel via Zoom,** peut être un évènement qui exige peu d'investissement et qui permet de maintenir et de développer des liens, d'avoir du plaisir et d'apprendre à mieux connaître ses collègues.

Prendre le temps de se rencontrer au-delà des tâches, rire, s'amuser n'est pas du temps perdu. C'est du temps pour protéger une richesse individuelle, collective et sociale, qu'est la santé mentale.

Tchin virtuel et à votre santé mentale à tous!

Sources : Le Club PVRH, La Presse, par Renée Ouimet, Directrice Mouvement Santé Mentale Québec.

ARS Solutions
6655, boul. Pierre-Bertrand, bureau 301, Québec (Québec) G2K 1M1
www.ars-solutions.ca | info@ars-solutions.ca | 418 872-4744