DÉCEMBRE 2022 - JANVIER 2023 • VOL. 10 N° 1

ARS SOLUTIONS

PASSION AFFAIRES et technologies

Édition spéciale

TOP 3 des articles qui vous ont le plus intéressés en 2022

#1 Outil de collaboration : une porte d'entrée pour les criminels

#2 Tentative d'hameçonnage provenant d'un client piraté

#3 Augmentation de 800 % des attaques d'hameçonnage dues au conflit en Russie

JOYEUX NOËL & BONNE ANNÉE

à tous nos clients et partenaires!

Toute l'équipe d'ARS Solutions vous souhaite un joyeux temps des Fêtes avec vos proches ainsi qu'une bonne et heureuse année couronnée de succès!

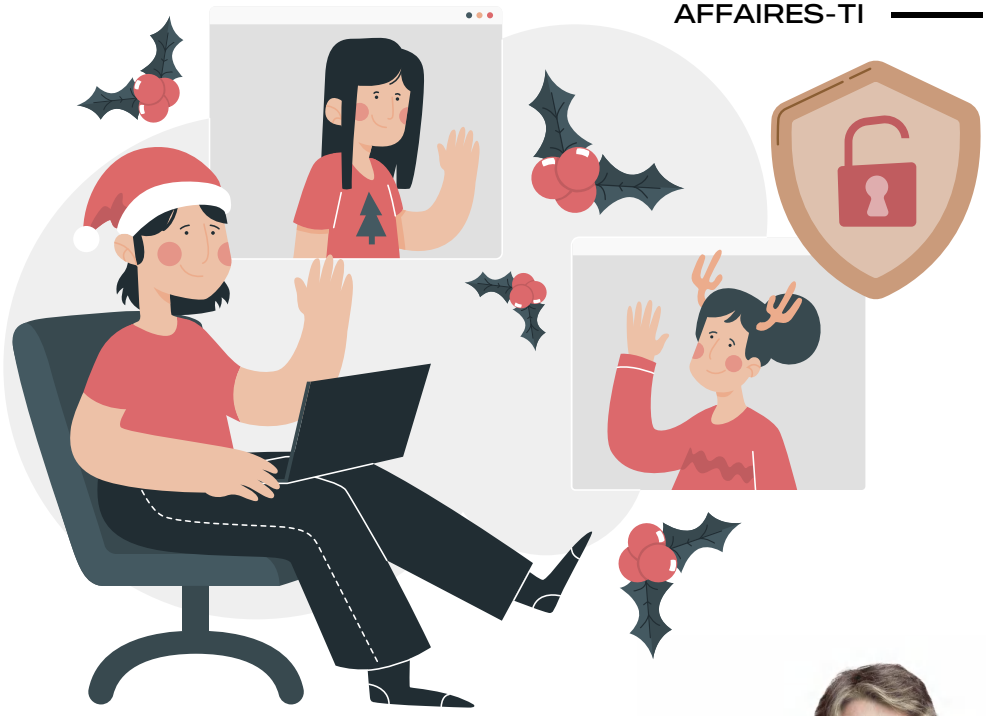
Que cette nouvelle année soit pour vous riche en moments inspirants. Qu'elle soit également une opportunité de dépassement de soi et de fierté.

Merci de votre confiance depuis toutes ces années, profitez bien de cette période de réjouissances et au plaisir de vous revoir en 2023!

SUIVEZ-NOUS SUR NOS RÉSEAUX SOCIAUX

- ARS Solutions Affaires-TI et Cybersécurité
- ARS Solutions Affaires et Technologies
- ARS Solutions
- arssolutions89

AFFAIRES-TI

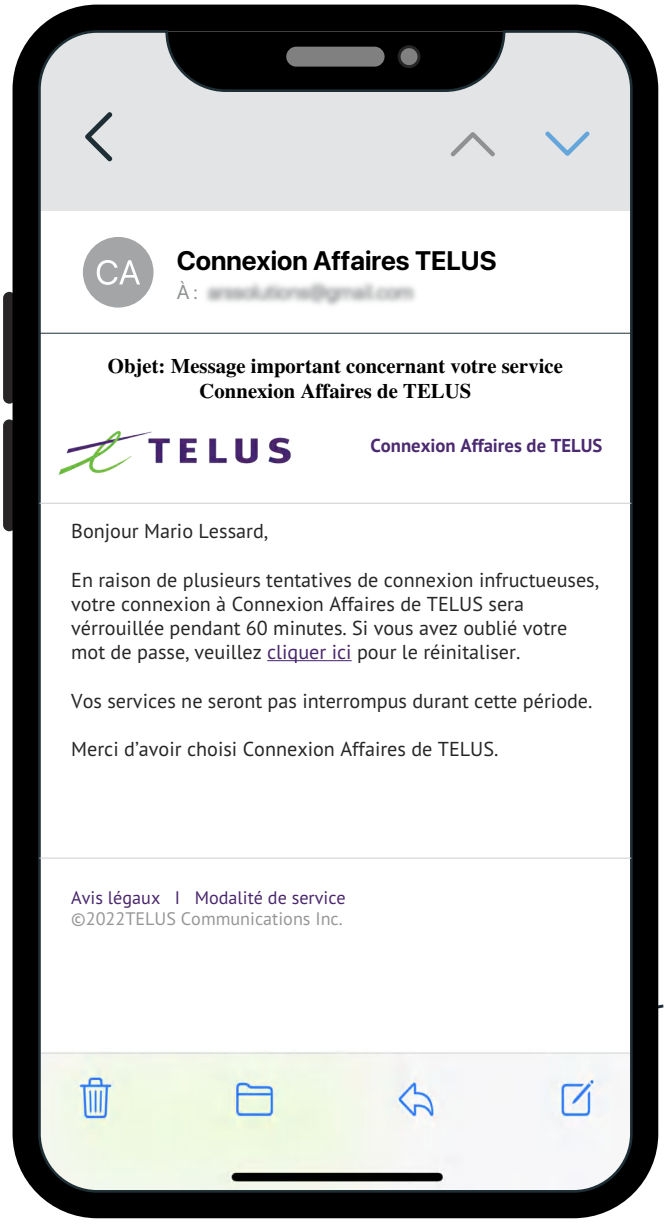


#1

OUTIL DE COLLABORATION : UNE PORTE D'ENTRÉE POUR LES CRIMINELS

Depuis que le télétravail s'est normalisé, les outils de collaboration sont également devenus la norme au sein des entreprises. Il s'agit toutefois d'une porte d'entrée supplémentaire pour les cybercriminels...

SUITE PAGE 2

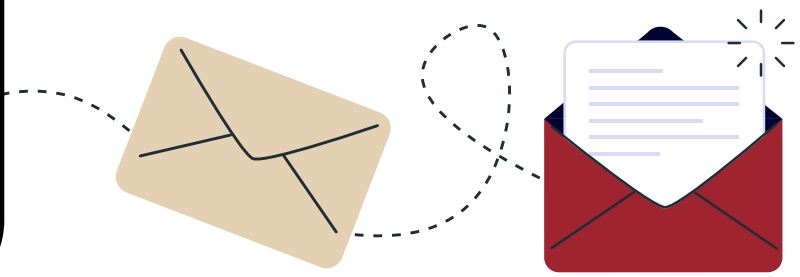


Dernièrement, chez ARS Solutions, certains de **nos employés ont reçu un courriel de Connexion Affaires de TELUS**, l'outil de collaboration et de téléphonie IP que nous utilisons à l'interne, et **celui-ci semblait très légitime**.

Il s'agissait d'un **avis de verrouillage de connexion suite à plusieurs tentatives de connexion infructueuses**. Heureusement, nos employés nous l'ont signalé rapidement donc nous avons pu avertir le reste de l'équipe qu'il s'agissait d'un courriel frauduleux et qu'il ne fallait pas cliquer sur le lien.

Il serait toutefois **très intuitif pour certains de croire que quelqu'un a réellement tenté de se connecter à leur compte** et donc qu'il faut modifier leur mot de passe au plus vite. **Mais le simple fait de cliquer sur le lien pourrait être bien dommageable pour l'entreprise et infecter l'ensemble du réseau.**

En cybersécurité, **un seul clic peut être fatal**. On doit se méfier d'absolument tout pour éviter le pire, car **il vaut mieux être paranoïaque que piraté**... N'hésitez pas à nous contacter pour obtenir de l'aide à ce sujet ou pour vérifier la légitimité d'un courriel reçu.



#2

TENTATIVE D'HAMEÇONNAGE PROVENANT D'UN CLIENT PIRATÉ

Tout comme votre entreprise, **vos clients peuvent être la cible des cybercriminels et voir leur réseau infecté** à la suite d'une tentative d'hameçonnage fructueuse.

Récemment, chez ARS Solutions, nous avons reçu un courriel à l'adresse générale de l'entreprise (info@ars-solutions.ca) et celui-ci semblait très authentique. Il provenait de l'un de nos clients, que nous ne nommerons pas pour respecter la confidentialité. Le courriel contenait la véritable bannière de signature professionnelle de l'adjointe aux ressources humaines sur place et il faisait **mention d'une facture partagée via un fichier OneDrive Entreprise et que pour l'afficher, il fallait cliquer sur le lien ci-dessous :**

[redacted] a partagé un fichier OneDrive Entreprise avec vous.
Pour afficher, cliquez sur le lien ci-dessous.

facture 560986.pdf

---

veuillez ouvrir la facture ci-jointe qui vous a été envoyée et

contactez-moi pour plus

d'informations

Merci beaucoup!

Pour consulter la facture en question, **nous devions cliquer sur un lien qui menait vers une page de connexion à un compte Microsoft pour accéder au fichier via OneDrive.** Il s'agit d'une technique d'hameçonnage couramment utilisée pour usurper des identifiants personnels **(adresse courriel et mot de passe)**.

Heureusement, nos employés sont tellement sensibilisés aux différentes techniques d'hameçonnage que personne n'a cliqué sur le lien et ça n'a pris que quelques secondes après la réception du courriel pour que l'un de nos employés visés par l'envoi frauduleux avertisse le reste de l'équipe qu'un courriel malicieux avait été reçu de la part de l'un de nos clients, qu'il ne fallait surtout pas cliquer dessus et qu'on devait le détruire. **Le simple fait de cliquer sur le lien aurait pu être bien dommageable pour notre entreprise et infecter l'ensemble du réseau.**

Quelques heures plus tard, **nous avons reçu un courriel du client en question qui tenait à nous informer que la boîte courriel de l'un de leurs employés avait été piratée** le jour-même en nous invitant à supprimer le courriel si nous l'avions reçu, de changer immédiatement notre mot de passe si nous avions déjà cliqué sur le lien en plus d'effectuer un scan de notre poste avec un antivirus et de rapporter l'incident à notre partenaire TI.

#3 AUGMENTATION DE 800 % DES ATTAQUES D'HAMEÇONNAGE DUES AU CONFLIT EN RUSSIE

La société Avanan, spécialisée dans la cybersécurité des courriels, a déclaré qu'elle avait constaté au début du mois de mars une augmentation soudaine et significative des attaques d'hameçonnage et de collecte d'informations d'identification basées sur la Russie.

L'Agence pour la cybersécurité et la sécurité des infrastructures (CISA) a lancé un avertissement le 16 février au sujet d'une **campagne de 2 ans en cours menée par la Russie**. La forte augmentation a commencé le 27 février et est environ **8 fois plus importante que le volume normalement observé**. Le PDG d'Avanan, Gil Freidrich, a déclaré que son entreprise traite généralement environ 100 millions de courriels de clients par jour.

Pour chaque tranche de 100 000 courriels traités, l'entreprise trouve habituellement entre 30 et 50 attaques d'hameçonnage, et normalement, seule une infime partie de cette activité (environ 1 %) correspond à des attaques de collecte d'informations d'identification. Cependant, **les attaques de type russe ont augmenté de façon spectaculaire, passant de 50 à 400 par jour depuis le 27 février**. Donc si vous recevez plus de courriels étranges depuis, il se peut fort bien que ce soit relié.

L'activité observée **ne semble pas suivre la même stratégie de masse que celle que l'on observe habituellement** dans les attaques d'hameçonnage. **Les cibles sont des clients des secteurs de la fabrication, de l'expédition internationale et du transport. L'augmentation de ces attaques coïnciderait avec les premiers jours d'une invasion de l'Ukraine par la Russie**, qui a entraîné de sévères sanctions économiques contre le pays et son économie.

Pendant des mois, ce scénario potentiel a suscité l'alarme des experts en cybersécurité quant à la possibilité de cyberattaques, mais Avanan n'attribue pas les attaques au gouvernement russe et ne confirme pas qu'elles sont liées aux tensions.

Les appâts utilisés dans ces courriels ne diffèrent pas de ceux que l'on voit habituellement dans le domaine de l'hameçonnage, comme **l'usurpation de l'identité d'un PDG ou d'un employé interne qui envoie des documents "urgents"** ou des courriels Microsoft 365 usurpés vous demandant de cliquer sur un lien pour que votre compte reste actif. La principale différence qu'Avanan constate dans les données est l'ampleur, et non les méthodes de ces attaques.

« Je soupçonne que nous allons commencer à voir peut-être de **nouvelles méthodes pour contourner les protections d'Office 365**. **Je ne serais pas surpris que les cybercriminels aient gardé certaines de leurs méthodes de dissimulation les plus sophistiquées pour un événement comme celui-ci.** », a déclaré Freidrich. Donc en cas de doute, ne **cliquez sur rien et avisez rapidement votre fournisseur TI pour vérifier la légitimité d'un courriel et éviter sa propagation**. N'hésitez pas à nous contacter pour obtenir de l'aide.

Source : Derek B. Johnson

6655, boul. Pierre-Bertrand, bureau 301, Québec, QC G2K 1M1
www.ars-solutions.ca I info@ars-solutions.ca I 418 872-4744