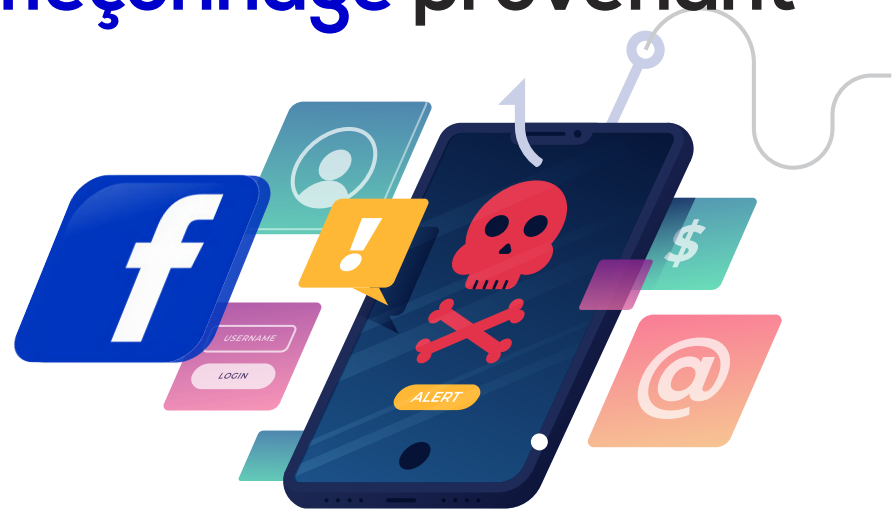
ARS SOLUTIONS

PASSION AFFAIRES et technologies

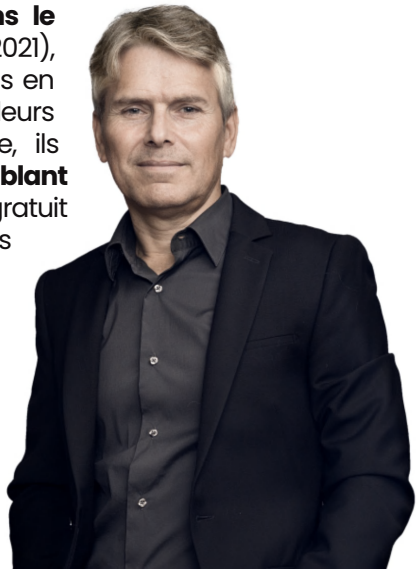
Présentés ce mois-ci :

Entreprise TI classée #1 à Québec en 2022 par **ThreeBest Rated®**

Les entreprises sont ciblées par une tentative d'hameçonnage provenant de Facebook



Avec plus de **200 millions de PME dans le monde qui utilisent Facebook** (Facebook, 2021), il n'est pas étonnant que les cybercriminels en profitent pour cibler les organisations dans leurs tentatives d'hameçonnage. Pour ce faire, ils envoient **des courriels de masse semblant provenir de Meta Business Suite**, un outil gratuit qui centralise Facebook, Instagram et les outils de messagerie à un endroit pour permettre aux entreprises de gagner du temps, de créer des liens avec davantage de personnes et d'obtenir de meilleurs résultats commerciaux.



SUITE PAGE 2

« Nous avions besoin d'un véritable partenaire d'affaires, et ARS Solutions a su répondre à nos attentes…

Ils nous amènent une conception globale de nos TI avec une vision axée sur les meilleures pratiques en cybersécurité. **Les interventions proactives d'ARS Solutions permettent que notre infrastructure demeure stable, sécuritaire et performante afin d'éviter les arrêts de production.**

De plus, les membres de leur équipe technique sont compétents, efficaces et très courtois. Merci pour votre professionnalisme! »

Ann Larochelle
Maison Orphée
Vice-présidente finances

Récemment, nous avons reçu un courriel de Meta Business Suite à l'adresse générale d'ARS Solutions et celui-ci pouvait sembler très légitime à première vue. Toutefois, **lorsque vos employés sont bien formés et sensibilisés contre les différentes techniques d'hameçonnage, ils devraient être en mesure de détecter les indices qu'il pourrait s'agir d'une tentative de fraude**.

Voici à quoi ressemblait le courriel que nous avons reçu :

lun. 16/05/2022 12:01

Meta for Business <metacaseid782101@outlook.com>

Facebook Report #1003457673422101

À Informations

Assurer un suivi. Commencer avant 17 mai 2022. Échéance le 17 mai 2022

Hi,

Your page has been found to be in violation of the Facebook Terms of Use. Compliance with the Facebook Policy is required to ensure a (quality and brand-safe environment for Facebook's users. We previously warned you that if you continued to infringe the rights of third partie, qe would terminate your account. Accordingly, your account and your pages will be disabled and you will no longer permitted to use Facebook.

If you think this is a mistake, please let us know.
https://www.facebook.cam/1012550486746101

Thanks,
Facebook Team

Quoi surveiller?

1. Le courriel **provient d'une adresse Outlook** et non du domaine officiel de Facebook qui est normalement @facebookmail.com.

2. Le courriel est **impersonnel** et contient l'appellation générale "Hi".

3. Ce type de courriels d'hameçonnage comprend souvent un appel à l'action à l'aide d'un lien. Dans ce cas-ci, si l'on passe notre curseur devant le lien affiché dans le courriel, on peut voir que **le lien de redirection n'est pas le même que celui qui est affiché** dans le courriel. Il est important de ne PAS cliquer sur aucun lien d'un courriel avant d'avoir bien vérifié sa légitimité.

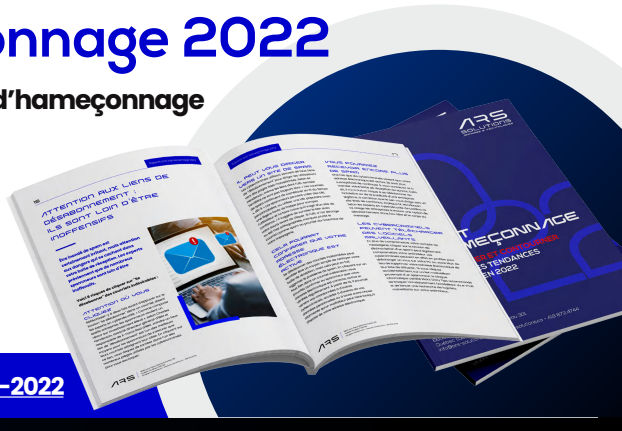
4. **Le courriel est en anglais**, alors que les notifications par courriel de Facebook sont normalement en français pour les utilisateurs francophones.

En cybersécurité, **un seul clic peut être fatal**. On doit être vigilant en tout temps pour éviter le pire. N'hésitez pas à nous contacter pour obtenir de l'aide à ce sujet ou pour vérifier la légitimité d'un courriel reçu.

NOUVEAU! Rapport anti-hammeçonnage 2022

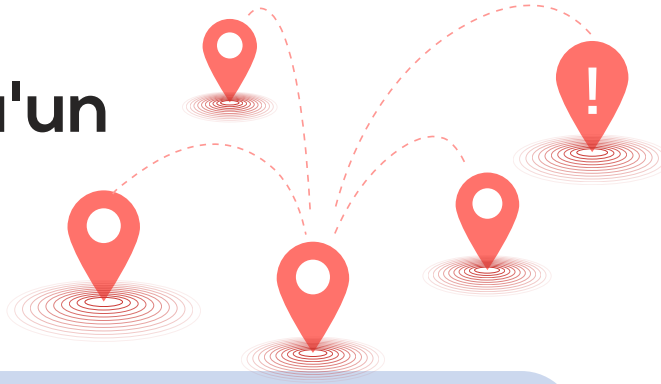
Découvrez comment identifier et contourner les plus récentes tendances d'hameçonnage en 2022! En téléchargeant ce rapport, vous découvrirez :

1. Formulaire d'autoévaluation de votre niveau de sécurité;
2. 9 prédictions de cybersécurité 2022;
3. 3 méthodes d'attaques par hameçonnage;
4. Des exemples réels de tentatives d'hameçonnage reçues chez ARS;
5. Et plus encore....



Téléchargez-le SANS FRAIS : www.ars-solutions.ca/rapport-anti-hameconnage-2022

Comment savoir si quelqu'un utilise vos comptes?



Les cyberattaques sont de plus en plus nombreuses et sophistiquées. Malheureusement, vous ne vous rendrez probablement pas compte que quelqu'un s'est immiscé dans votre vie numérique avant qu'il ne soit trop tard.

Parfois, le coupable est plus proche de vous. Vous craignez que quelqu'un ait fouiné dans votre ordinateur? **On vous explique comment vérifier les appareils et les personnes qui les utilisent et qui ne devraient pas être là.**

Vérifiez qui est connecté à votre compte Google

Pensez à tout ce à quoi votre compte Google peut donner accès : vos courriels, vos contacts, l'historique de votre localisation, vos recherches, vos photos... Et plus encore. **Soyez proactif et consultez la page des appareils de Google avant de remarquer des signes d'alerte :**

- Rendez-vous sur www.google.com/devices et connectez-vous si ce n'est pas déjà fait.
- Vous verrez une liste des appareils pour lesquels vous êtes actuellement connecté ou l'avez été au cours des 28 derniers jours.

Il se peut que le même appareil apparaisse plusieurs fois, ce qui est normal. Ne vous inquiétez pas si vous voyez plusieurs instances d'un système d'exploitation ou votre iPhone listé à plusieurs reprises. Vous pouvez cliquer sur chacune d'elles pour voir quel navigateur a été utilisé. Cela peut être un indice que quelqu'un d'autre s'est connecté, si vous voyez Firefox, par exemple, mais que vous utilisez toujours Safari.

Si vous voyez un appareil ou un emplacement qui vous semble suspect, cliquez dessus, puis choisissez "Vous ne reconnaissez pas quelque chose?". Google déconnectera cet appareil à distance. Ensuite, changez votre mot de passe au cas où quelqu'un le détiendrait.

Vérifiez les appareils connectés à Facebook

Chaque jour, un bon nombre de personnes perdent l'accès à leur compte Facebook. Parfois, il s'agit d'un mot de passe oublié, mais il peut aussi souvent s'agit d'un malfaiteur. **Voici comment voir les appareils connectés à votre compte Facebook (le plus simple est de le faire à partir d'un ordinateur) :**

- Connectez-vous, puis cliquez sur votre photo de profil dans le coin supérieur droit.
- Cliquez sur "Paramètres et confidentialité"/ "Paramètres".
- Enfin, cliquez sur "Sécurité et connexion".
- Vous verrez une section intitulée "Où vous êtes connecté". Elle indique les deux appareils les plus récents et leurs emplacements de connexion approximatifs. Cliquez sur l'option "Voir plus" pour obtenir plus de détails.

Examinez attentivement chaque résultat et recherchez les lieux où vous n'êtes jamais allé ou les appareils que vous ne possédez pas. **Vous utilisez un VPN?** Cela peut se refléter dans vos derniers lieux. Avant de paniquer, **vérifiez la ville par laquelle votre VPN se connecte**.

Sur cette page, vous pouvez cliquer sur les 3 points situés à côté d'un appareil pour sélectionner "Ce n'est pas vous?" ou "Déconnexion". La première option vous donnera plus de détails sur l'appareil et son emplacement, ainsi que des **mesures pour sécuriser votre compte**. La seconde option permet de déconnecter cet appareil.

Si vous voyez des appareils et des emplacements que vous ne reconnaissez pas, suivez les instructions à l'écran pour **sécuriser votre compte Facebook**, déconnectez ces appareils et changez votre mot de passe immédiatement.

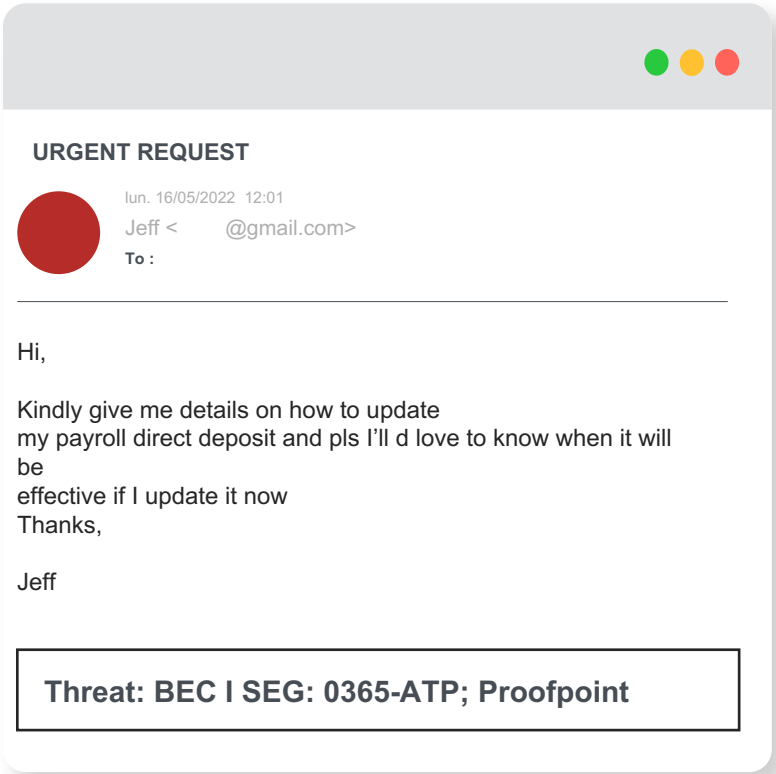
Source : Kim Komando, USA TODAY

Business Email Compromise : et si un malfaiteur détournait votre salaire?

Le Business Email Compromise (BEC) est responsable de milliards de pertes financières auprès d'entreprises à travers le monde.

Bien que toute notre attention se porte sur les liens cliquables des courriels frauduleux, il existe également des attaques par échanges de courriels sans lien cliquable. À faire attention puisque la victime n'est pas du tout en communication avec la personne qui semble se présenter.

Les tendances observées par Cofense incluent **les escroqueries de dépôt direct, la fraude de cartes-cadeaux et les arnaques de factures**. Dans la totalité de ces attaques, aucun logiciel malveillant ou virus n'est installé sur l'ordinateur de l'utilisateur. Elles reposent uniquement sur l'interaction humaine. **Ce mois-ci, on vous présente l'escroquerie de dépôt direct.**



L'une des attaques BEC les plus difficiles à attraper est l'escroquerie de dépôt direct, également appelée "détournement de salaire". Pour mener à bien ces attaques, les cybercriminels font de l'ingénierie sociale auprès des responsables de la paie ou des ressources humaines en leur demandant de mettre à jour les informations de dépôt direct des employés sur les comptes qu'ils contrôlent.

Pour limiter leurs risques d'exposition, les malfaiteurs utilisent des **cartes prépayées jetables au lieu de comptes bancaires traditionnels**, afin d'éviter la détection et de limiter l'impact d'un démantèlement. Pour ajouter une couche supplémentaire de dissimulation, **les acteurs recrutent des gens pour acheter les cartes prépayées en leur nom**, ce qui rend encore plus difficile la détection de l'auteur de l'escroquerie.

Pour mener à bien ces attaques, les attaquants créent **des comptes de messagerie ressemblant à la victime pour laquelle ils vont réacheminer les salaires**. Une fois la conversation engagée, les acteurs peuvent fournir des formulaires I9 remplis ou des chèques annulés pour renforcer l'authenticité de la fraude. Une fois réussies, **ces attaques peuvent prendre des semaines avant d'être remarquées**, causant ainsi un stress inutile à la fois à la victime et son employeur.

Les attaques par hameçonnage sont en pleine explosion et sont très dommageables financièrement pour les entreprises. Elles peuvent être **difficiles à détecter par vos employés**. La formation en continue de vos employés ainsi que les simulations d'hameçonnage régulières sont un incontournable. N'hésitez pas à nous contacter pour obtenir de l'aide à ce sujet ou pour vérifier la légitimité d'un courriel reçu.

Source : Cofense 2022 Annual State of Phishing Report

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