alpha numérique

FICHE RÉSUMÉ

Cliquer ou ne pas cliquer : reconnaître et se protéger de l'hameçonnage

Qu'est-ce-que l'hameçonnage ?

Selon le *Centre canadien pour la cybersécurité*, l'hameçonnage se définit comme suit : « Terme générique qui désigne la conception et la fabrication de courriels, de messages texte et de sites Web par des criminels de sorte à donner l'impression que ce contenu numérique provient d'entreprises bien connues et fiables, dont les institutions financières et les organismes gouvernementaux. Les criminels diffusent ce contenu pour tenter de recueillir de l'information sensible de nature personnelle ou financière. »

Quels sont les différents types de fraudes en ligne ?

COURRIELS

Les fraudeurs envoient des courriels ciblés pour berner leurs victimes et voler leurs renseignements confidentiels.

MÉDIAS SOCIAUX

Les fraudeurs utilisent les médias sociaux pour faire circuler de la fausse information et ainsi piéger leurs victimes.

SITES WEB

Les fraudeurs créent de faux sites d'apparence légitime dans lesquels ils copient des logos officiels.

L'hameçonnage par courriel : qu'est-ce qu'un pourriel ?

Un pourriel est un courriel non sollicité envoyé à un grand groupe de personnes (publicité, offre de cadeau ou demande d'argent). Le message est conçu pour cacher la véritable adresse ou identité de l'expéditeur et contient souvent des liens dangereux.

Si vous avez répondu à un courriel suspect, donné des renseignements personnels ou perdu de l'argent, veuillez communiquer avec le Centre antifraude du Canada au 1 888 495-8501.

Les 7 signaux d'alarme d'un message d'hameçonnage

1. PRESSION OU LANGAGE MENAÇANT

Les vrais messages d'urgence sont rarement envoyés par courriel.

2. INFORMATIONS SENSIBLES DEMANDÉES

Les organisations ou individus de confiance demandent rarement de fournir ce type d'information par courriel.

3. TROP BEAU POUR ÊTRE VRAI

Il est rare de gagner à la loterie sans y avoir participé ou de toucher un héritage d'un proche dont on a jamais entendu parler !

4. COURRIELS INATTENDUS

Recevoir des reçus et des suivis concernant des articles qui n'ont jamais été commandés est plutôt surprenant.

5. RENSEIGNEMENTS DOUTEUX

Suivre son instinct et chercher des indices peut permettre de repérer l'hameçonnage. Voici des réflexions qui peuvent aider :

- L'adresse courriel de l'expéditeur est-elle correcte ?
- Les liens mènent-ils vers une page officielle ?
- Y a-t-il des erreurs d'orthographe ou de grammaire qu'une organisation légitime saurait éviter ?

6. PIÈCES JOINTES SUSPECTES

Rester méfiant est important si les noms ou les types de fichiers accompagnant un courriel sont inhabituels ou comportent des fautes.

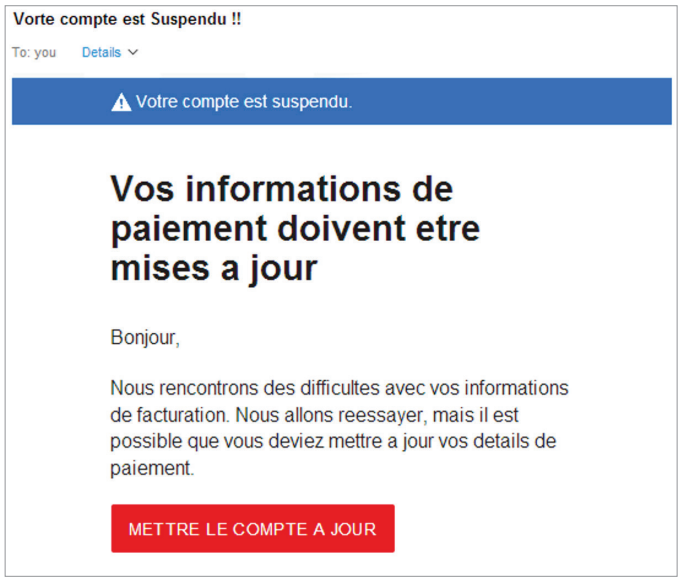
7. GRAPHISME AMATEUR

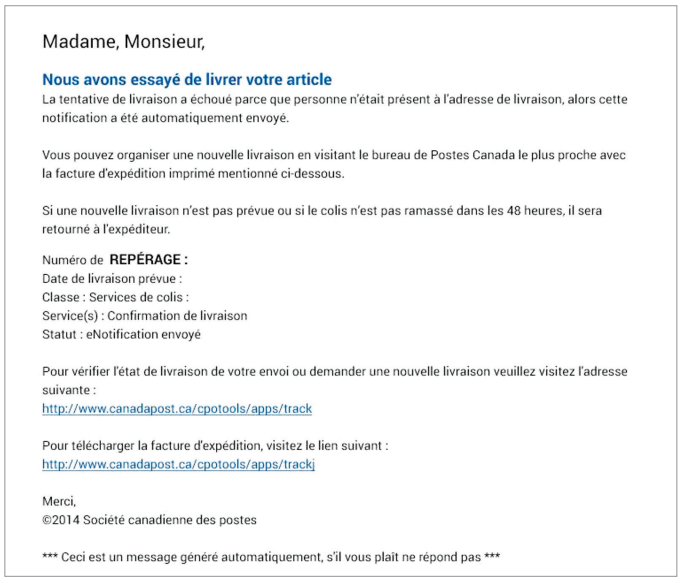
Les cybercriminels embauchent rarement des graphistes professionnels. Attention aux logos flous ou inexacts ainsi qu'aux mises en page hasardeuses.

Les quatres étapes de l’hameçonnage par courriel

1. Vous recevez un message qui semble venir d’un proche ou d’une institution.
2. On vous demande d’effectuer une action urgente en cliquant sur un lien ou une pièce jointe.
3. Vous communiquez des informations personnelles par message ou en remplissant un formulaire en ligne sur un site Web qui semble fiable.
4. Le fraudeur utilise ces informations sans votre consentement.

Voici deux exemples d’hameçonnage avertissant d’une urgence ou d’un problème :





J’ai cliqué sur un lien ou ouvert une pièce jointe dans un courriel frauduleux. Que faire ?

Si vous n’avez pas fourni vos informations confidentielles :

- Modifiez sans tarder votre mot de passe pour ce site.
- Appliquez la même procédure pour tous vos accès confidentiels.

Si vous avez fourni vos informations confidentielles :

- Contactez votre police locale
- Vos institutions bancaires
- Aviser les agences de crédit telles qu’Équifax (1 800 465-7166 ou 514 493-2314) et TransUnion (1 877 713-3393 ou 514 335-0374). Elles ajouteront une note à votre dossier pour alerter les fournisseurs de crédit que vous avez peut-être été victime d’une activité frauduleuse.

Reconnaître une publication frauduleuse sur les réseaux sociaux

- L'auteur de la publication ne semble pas légitime.
- On vous incite à cliquer sur un lien douteux qui ne mène pas vers un site officiel.
- La publication peut contenir plusieurs fautes d'orthographe et de grammaire.
- Un ton menaçant est généralement utilisé.
- Un contexte d'urgence est souvent établi pour que vous agissiez rapidement.
- Certains passages sont parfois rédigés dans une autre langue.
- Les commentaires inscrits sous la publication paraissent faux, voire fabriqués.

Site Web et sécurité : Comment reconnaître un site Web frauduleux ?

- Adresse différente que celle inscrite
- Fautes d'orthographe et de grammaire
- Logos utilisés différents des logos officiels
- Polices et couleurs d'écriture non uniformes
- Mise en page simpliste des formulaires à remplir
- Utilisation de formules générales pour se donner de la crédibilité

Https : pourquoi c'est important ?

Pour répondre aux exigences de sécurité toujours plus élevées sur le Web et rendre la vie plus dure aux pirates informatiques, Google a pris la décision en 2017, de pénaliser les sites non sécurisés qui utilisent un protocole HTTP, c'est-à-dire la vaste majorité ! De plus, Google annonçait récemment qu'au premier juillet 2018, les domaines n'ayant toujours pas d'authentification HTTPS s'afficheront sur le navigateur Google Chrome, comme n'étant « pas sécuritaire ».

Continuez à apprendre sur alphanumerique.ca !