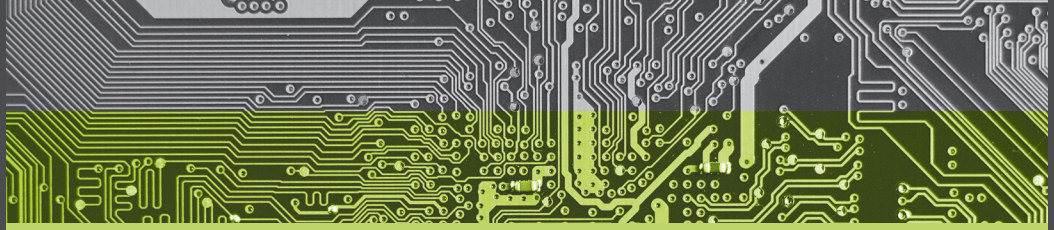

JUILLET 2019

FEUILLE-INFO
SUR LA TECHNOLOGIE

Se protéger contre l'hameçonnage

Les pirates informatiques recourent souvent à l'hameçonnage, une attaque qui, lorsqu'elle est fructueuse, pose une sérieuse menace à la sécurité des documents électroniques et des renseignements personnels.

Les lois ontariennes sur la protection de la vie privée obligent les institutions publiques et les organismes de soins de santé à prendre des mesures raisonnables pour protéger les renseignements personnels dont ils ont la garde ou le contrôle.

L'hameçonnage pose une sérieuse menace à la sécurité des documents électroniques et des renseignements personnels

QU'EST-CE QUE L'HAMEÇONNAGE?

L'hameçonnage est un type d'attaque en ligne où le pirate envoie à une ou plusieurs personnes un courriel non sollicité, un message sur les médias sociaux ou un message instantané et, en recourant à des tactiques technologiques et psychologiques, les incite à révéler des renseignements délicats ou à télécharger un logiciel malveillant.

> Les logiciels malveillants sont conçus pour perturber ou endommager un système informatique, ou pour y accéder sans autorisation.

L'hameçonnage peut être générique ou personnalisé, et s'en prendre à des particuliers ou à des organisations. Une attaque visant une personne ou une organisation particulière est couramment appelée « harponnage ».

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Le principal objectif de l'hameçonnage consiste à inciter la personne à faire une chose qui porte atteinte à la sécurité de son organisation. Le pirate y parvient lorsque le destinataire :

- répond à un courriel d'hameçonnage en incluant des renseignements personnels;
- ouvre une pièce jointe contenant un logiciel malveillant;
- clique sur un lien menant à un faux site Web ou à une page qui installe un logiciel malveillant;
- entre un nom d'utilisateur ou un mot de passe, ou d'autres renseignements délicats, dans un faux site.

Le principal objectif de l'hameçonnage consiste à inciter le destinataire à faire une chose qui porte atteinte à la sécurité de son organisation

CONSÉQUENCES DE L'HAMEÇONNAGE

Les conséquences immédiates d'un hameçonnage fructueux peuvent comprendre :

- l'accès non autorisé à des systèmes informatiques, réseaux et comptes en ligne;
- le vol, la perte et l'utilisation ou la divulgation non autorisée de renseignements délicats ou personnels;
- la destruction ou l'altération de documents;
- la défaillance de systèmes et la perturbation des services.

Souvent, les effets de l'hameçonnage ne sont pas visibles dans l'immédiat. Il arrive que les victimes ignorent qu'il y a eu une attaque avant que ses conséquences ne s'aggravent. Après avoir obtenu l'accès à des renseignements confidentiels ou piraté des comptes ou des appareils informatiques, le pirate peut utiliser d'autres techniques pour pénétrer dans le réseau et recueillir plus de renseignements. En fin de compte, il peut commettre des crimes tels que la fraude, le vol ou l'extorsion.

Les attaques fructueuses peuvent se répercuter sur toute organisation et causer la perte de temps, d'argent et de réputation.

EXEMPLES D'HAMEÇONNAGE

Les attaques d'hameçonnage semblent provenir de sources légitimes, et exploitent la confiance, la curiosité ou la peur des gens, ou encore leur volonté de se rendre utiles et leur souci d'efficacité.

Les attaques d'hameçonnage semblent provenir de sources légitimes, et exploitent la confiance, la curiosité ou la peur des gens, ou encore leur volonté de se rendre utiles et leur souci d'efficacité

Les messages d'hameçonnage semblent souvent authentiques; il peut s'agir :

- de courriels professionnels qui semblent officiels : avis de boîte aux lettres pleine ou de pourriels en quarantaine, avis de changement de mot de passe, plans d'évacuation, avis de prestations, factures, documents confidentiels;

- de courriels commerciaux : confirmations d'expédition, demandes de virement télégraphique, invitations à télécharger des documents d'un service d'infonuagique ou à utiliser un service de partage de fichiers pour récupérer, créer ou modifier un document;
- de courriels imitant des offres ou comptes que les gens ont déjà : comptes bancaires, d'impôt ou de programme pour grands voyageurs, marquage photo, réseaux sociaux, avis de carte-cadeau, mise à jour de sécurité pour le magasinage en ligne.

Une pièce jointe inattendue ou inhabituelle dans un message peut contenir un logiciel malveillant

COMMENT RECONNAÎTRE LES MESSAGES D'HAMEÇONNAGE

Les messages d'hameçonnage peuvent être très simples, mais aussi très sophistiqués. En voici des signes courants (voir l'illustration à la page 7) :

- Adresse d'envoi ou de réponse douteuse : soyez toujours prudent quand vous recevez des messages d'expéditeurs ou de comptes inconnus.
- Message inattendu : un message d'un expéditeur qui est inhabituel ou n'est pas relié à vos fonctions peut signaler qu'un compte est faux ou a été piraté.
- Pièce jointe douteuse : une pièce jointe inattendue ou inhabituelle dans un message peut contenir un logiciel malveillant.
- Lien douteux : un hyperlien sur lequel un message invite le destinataire à cliquer peut mener à un site Web qui n'est pas relié au message et dont le pirate a le contrôle.
- Message mal écrit : des fautes d'orthographe et de grammaire peuvent être un signe d'hameçonnage, car les organisations légitimes les évitent généralement dans leurs communications.

COMMENT SE PROTÉGER CONTRE L'HAMEÇONNAGE

Vous pouvez protéger votre organisation contre l'hameçonnage en adoptant les pratiques exemplaires suivantes.

- Filtrez les messages entrants : veillez à ce que votre système informatique filtre les messages entrants pour réduire les pourriels et les contenus indésirables. Les fonctions antimystification peuvent vérifier l'authenticité des expéditeurs et empêcher les pirates d'atteindre leur cible.
- Installez des détecteurs et filtres de logiciels malveillants : vos systèmes devraient automatiquement bloquer ou mettre en quarantaine les messages contenant des virus, des rançongiciels ou d'autres éléments malveillants. Utilisez des logiciels qui préviennent, détectent et éliminent les logiciels malveillants et effectuent une surveillance en temps réel.

- Tenez à jour les navigateurs et autres logiciels : les pièces jointes et logiciels malveillants exploitent souvent les vulnérabilités de navigateurs et d'autres logiciels périmés. Veillez à ce que votre personnel d'informatique mette à jour régulièrement tous les logiciels et systèmes d'exploitation s'il n'est pas possible d'effectuer des mises à jour automatiques.
- Verrouillez les postes de travail : les pirates peuvent exploiter un ordinateur dont l'utilisateur est autorisé à installer des logiciels et à régler les paramètres. Limitez ou désactivez les privilèges d'administrateur pour les utilisateurs habituels et limitez le nombre d'ordinateurs ou de comptes comportant un niveau élevé de privilèges ou ayant l'autorisation d'accéder à des renseignements délicats. Les personnes ayant un niveau élevé de privilèges ne devraient pas partager leur compte ou s'en servir à des fins non professionnelles.
- Obligez les employés à utiliser des mots de passe uniques et complexes : la réutilisation de mots de passe volés présente un risque élevé d'hameçonnage. Des méthodes d'authentification plus fortes, comme des jetons à mots de passe à usage unique, des justificatifs d'identité cryptographiques ou des données biométriques devraient être exigés dans le cas des administrateurs de système ou des utilisateurs qui se servent de données délicates ou accèdent à distance à des ressources de l'organisation.
- Identifiez les messages externes : il est plus facile de déceler les messages d'hameçonnage si tous les messages externes sont clairement étiquetés comme provenant de l'extérieur de l'organisation :

Il est plus facile de déceler les messages d'hameçonnage si tous les messages externes sont clairement étiquetés

Permettez aux utilisateurs de signaler les cas d'hameçonnage et de demander de l'aide

ATTENTION : COURRIEL EXTERNE. NE PAS CLIQUER SUR LES LIENS NI OUVRIR LES PIÈCES JOINTES À MOINS DE CONNAÎTRE L'EXPÉDITEUR

- Séparez des autres réseaux ceux qui contiennent des données délicates. Si des ordinateurs et comptes sont compromis, vous pouvez limiter les conséquences en limitant leur accès à d'autres réseaux ou systèmes. Par exemple, les serveurs publics de courriel Web devraient être isolés des intranets ou des bases de données des ressources humaines.
- Utilisez des outils de renseignements sur les menaces et des outils de protection des postes de travail. Les outils évolués peuvent déceler les pirates et, parfois, les empêcher de pénétrer dans votre réseau en vous signalant des comportements inhabituels, par exemple, des tentatives d'ouverture de session irrégulières et des téléchargements de gros fichiers.

- Chiffrez par défaut les documents, appareils et bases de données contenant des renseignements délicats; le chiffrement constitue un autre moyen de défense contre l'accès, l'utilisation et la divulgation non autorisés.
- Sensibilisez régulièrement le personnel à l'hameçonnage et donnez-lui de la formation à ce sujet. Tenez des simulations d'hameçonnage pour vérifier les connaissances et les réactions de vos employés. De tels tests sensibilisent aux questions de sécurité et permettent de déterminer les employés qui ont besoin de formation supplémentaire.
- Permettez aux utilisateurs de signaler facilement les cas d'hameçonnage et de demander de l'aide en cas d'attaque. Il est utile aux organisations que leur personnel puisse faire des commentaires en temps réel sur les cas d'hameçonnage.

Une bonne planification et une conception judicieuse peuvent minimiser les risques et protéger la vie privée des particuliers

Les employés sont souvent la dernière ligne de défense contre l'hameçonnage; les sensibiliser et les former peut renforcer la sécurité. Renseignez-les sur les signes d'hameçonnage et dites-leur quoi faire des messages douteux.

- Vérifiez qui a envoyé un message en examinant attentivement l'adresse de l'expéditeur, qui devrait concorder avec le nom indiqué et le contexte du message. Par exemple, l'adresse de courriel d'une banque n'aurait pas pour nom de domaine « xbox.com » (le nom de domaine est après le @). Dans certaines attaques d'hameçonnage, l'adresse de courriel de l'expéditeur est semblable à l'adresse officielle d'une organisation, mais elle n'est pas identique. Par exemple, « omtario.ca » au lieu d'« ontario.ca ».
- Ne donnez pas de nom d'utilisateur, de mot de passe ou de code d'accès en réponse à un courriel ou dans une fenêtre surgissante non sollicitée. Les organisations légitimes ne demandent jamais ces renseignements par courriel; elles les recueillent uniquement par l'entremise de leur site Web ou de leurs applications. En cas de doute, appelez l'expéditeur.
- N'ouvrez pas les pièces jointes douteuses. Si vous recevez une pièce jointe inattendue, communiquez avec l'expéditeur (de préférence par téléphone) pour confirmer qu'elle est légitime. Si vous ne pouvez le confirmer, signalez-la à votre service d'informatique ou supprimez-la.
- Ne cliquez jamais sur un lien douteux. Survolez des parties du message avec le curseur de la souris sans cliquer. Si l'hyperlien qui apparaît semble bizarre ou ne correspond pas avec sa description, ne cliquez pas et signalez-le. Les images peuvent aussi cacher des liens suspects.
- Ne répondez pas aux messages douteux ou indésirables. Les pirates profitent de tout renseignement sur leurs cibles. Par exemple, demander de faire retirer son adresse de courriel d'une liste d'envoi appartenant à un individu malveillant confirme que

Ne cliquez jamais sur les liens douteux

cette adresse est valable, ce qui pourrait donner lieu à d'autres attaques. De même, le téléchargement d'images manquantes confirme que le message a été vu. Il est préférable d'identifier le message comme étant un pourriel ou de le supprimer.

- Signalez les messages douteux. Quand vous en recevez un et surtout si vous avez cliqué sur un lien ou une pièce jointe, informez aussitôt votre service d'informatique. Ce dernier déterminera s'il s'agit ou non d'une menace et prendra les mesures qui s'imposent pour minimiser tout risque pour votre organisation.

RÉAGIR AUX INCIDENTS D'HAMEÇONNAGE

Vous devriez disposer d'un plan d'intervention détaillé décrivant comment votre organisation réagira à une fuite de données ou à une cyberattaque éventuelle. Un bon plan limitera les dégâts et permettra un retour rapide à la normale.

Votre plan devrait prévoir ce qui suit :

- Les membres clés de la haute direction, du personnel d'informatique et du personnel juridique qui font partie de l'équipe d'intervention, et les tâches de chacun lorsqu'un incident est signalé;
- Les menaces possibles, afin de recueillir rapidement des indications importantes pour déterminer la portée et la gravité de la menace. Pour ce faire, il pourrait être nécessaire d'analyser attentivement le message d'hameçonnage, ses pièces jointes ou les liens qu'il contient, et le comportement de votre personnel et des réseaux informatiques.
- Les étapes à suivre pour maîtriser et éliminer les menaces éventuelles. Selon la nature de la menace, vous pourriez prévoir dans votre plan les mesures correctives suivantes :
    - o déconnecter les ordinateurs infectés des réseaux;
    - o changer les noms d'utilisateur et mots de passe des employés;
    - o éliminer les copies des messages ou fichiers infectés se trouvant dans les boîtes de réception ou les serveurs;
    - o réinstaller des logiciels ou récupérer les fichiers conservés dans une copie de sécurité;
    - o intensifier la surveillance de l'utilisation des ordinateurs et des réseaux;
    - o informer le personnel et signaler l'incident à des intervenants de l'extérieur (forces de l'ordre, organismes professionnels, compagnies d'assurances);
    - o mettre à jour vos mesures de prévention afin d'éliminer les failles que l'incident a révélées dans vos mesures de sécurité.

Vous devriez diffuser le plan d'intervention dans l'ensemble de votre organisation et tenir des exercices régulièrement afin que les interventions soient rapides et efficaces si un incident survient.

Les institutions publiques et les organismes du secteur de la santé qui ont fait l'objet d'une attaque d'hameçonnage fructueuse doivent communiquer avec le Bureau du commissaire à l'information et la protection de la vie privée de l'Ontario pour obtenir des conseils et des directives. Vous pouvez nous joindre au 1 800 387-0073 ou à **info@ipc.on.ca**.

Pour savoir comment protéger votre organisation contre les atteintes à la vie privée et les brèches de sécurité et y réagir, visitez notre site Web à **www.ipc.on.ca**.

RESSOURCES SUPPLÉMENTAIRES

- **Centre antifraude du Canada – Hameçonnage**
- **Conseil de la radiodiffusion et des télécommunications canadiennes Commission (CRTC) – Comment vous protéger contre les arnaqueurs**
- **Protection du consommateur de l'Ontario – Déclaration d'une escroquerie ou d'une fraud**

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

SIGNES COURANTS D'HAMEÇONNAGE

EXPÉDITEUR (CHAMP « DE ») :

- Le courriel semble provenir d'une **personne provenant de l'organisation** et est **très inhabituel**
- L'adresse de courriel semble appartenir à un **domaine douteux**

DESTINATAIRE (CHAMP « À ») :

- Le courriel a été envoyé à vous et à plusieurs autres personnes **que vous ne connaissez pas**
- Le courriel a été envoyé à un **groupe de personnes inhabituel**, par exemple, à des personnes de votre organisation dont le nom commence par la même lettre

OBJET :

- L'objet n'est **pas pertinent, comporte des fautes de grammaire ou d'orthographe ou ne concorde pas** avec le contenu du message

De : « PDG » nepasrepondre@Omtario.ca
À : « Vous », « Yasmine », « Yves », « Yvonne »
Date : Dimanche 12 juin, 3 h 1
Objet : On m'a volé mon argent

Allô, je suis en vacances à Londres et on m'a volé mon argent et mon passeport.Peux-tu m'envoyer 300 $ par Western Union? Ils m'ont donné un lien spécial alors l'argentva être déposé directement dans mon compte et je vais pouvoir acheter un billet de retour :

Clique ici --> http://western-onion.com/jhvfz9oq.exe

Merci beaucoup, ça va vraiment m'aider!

Ton PDG

DATE :

- Le courriel a été envoyé **après les heures normales de travail ou à une heure inhabituelle**

PIÈCES JOINTES :

- Le message contient une pièce jointe **inattendue** ou qui **ne concorde pas** avec le contenu du message

CONTENU :

- L'expéditeur vous demande de cliquer sur un lien ou d'ouvrir une pièce jointe pour **éviter une conséquence négative** ou pour **obtenir une chose ayant de la valeur**

HYPERLIENS :

- Lorsque vous survolez un hyperlien contenu dans le message avec la souris, **l'adresse qui apparaît appartient à un site Web différent**
- Le courriel contient **un hyperlien mal épelé** ressemblant à celui d'un site Web connu