Coupez la ligne des courriels hameçons

Les fraudeurs qui cherchent à mettre la main sur des renseignements personnels ont élaboré un nouveau moyen d'attirer des victimes sans méfiance. Ils lancent un « hameçon ».

« UN HAMEÇON POUR CHERCHER DE L'INFORMATION »

L'hameçon, également appelé **« usurpation de marque »** consiste à créer des messages électroniques et des sites Web qui sont des répliques d'entreprises et de sites existants tout à fait légitimes. Ces sites Web et ces courriels servent à leurrer les utilisateurs et à les amener à divulguer des renseignements personnels et financiers ainsi que leurs mots de passe. Ces courriels réclament des données, telles que des numéros de carte de crédit, de l'information sur des comptes bancaires, des numéros d'assurance sociale et des mots de passe, qui serviront à commettre des fraudes.

Le mot « hameçon » provient de l'analogie entre la pêche et ces escrocs virtuels qui utilisent des leurres sous forme de courriels pour « attraper » des mots de passe et des données financières dans le vaste océan d'Internautes.

Rappelez-vous que Visa et ses institutions membres ne sollicient jamais de renseignements personnels par voie électronique. Si vous recevez un courriel suspect semblant provenir de Visa, communiquez immédiatement avec Visa à l'adresse **phishing@visa.com**. Pour signaler des courriels hameçons possibles provenant d'autres organisations, envoyez un courriel à l'adresse **reportphishing@antiphishing.org**.

Qu'est-ce qu'un message hameçon ?

L'hameçonnage consiste à envoyer un courriel non sollicité, en prétendant faussement être une entreprise légitime, pour inciter le destinataire à divulguer des renseignements personnels. Ces courriels demandent souvent de l'information, telle que des numéros de carte de crédit, de l'information sur les comptes bancaires, des numéros d'assurance sociale et des mots de passe. L'objectif des usurpateurs de marque est de faire croire aux consommateurs qu'une demande d'information leur est adressée par une entreprise légitime. En réalité, c'est une tentative malicieuse de recueillir des renseignements personnels du client dans le but de commettre une fraude.

Comment fonctionne l'hameçonnage ?

Le client reçoit un courriel non sollicité qui semble provenir d'une entreprise légitime avec laquelle il fait affaire – par exemple le fournisseur de services Internet, le service de paiement en ligne ou son institution financière. Le message électronique prétend qu'il y a une erreur de facturation ou un problème avec le compte bancaire ou encore que ses renseignements personnels doivent être mis à jour ou validés. On demande ensuite au client de suivre les instructions qui l'amèneront sur un site Web qui semble légitime, arborant la raison sociale de l'entreprise, son logo et ses couleurs – autrement appelé un site Web de « marque usurpée ». Pendant sa visite sur le site, on demande au client de fournir des renseignements personnels et financiers à jour en remplissant un formulaire en ligne. Le formulaire exige des renseignements variés, tels que des numéros de carte de crédit et de compte, des mots de passe, la date de naissance, le numéro du permis de conduire et celui de la carte d'assurance sociale.

Puisque ces sites Web et ces courriels semblent « officiels », quelques destinataires se laissent prendre à y répondre et divulguent ainsi leurs renseignements personnels et financiers à des criminels. Ces fraudeurs utilisent alors l'information pour acheter des produits et des services, obtenir du crédit ou commettre un vol d'identité.

Comment signaler un message « hameçon » à Visa

Si vous avez reçu un courriel suspect qui vous semble être un message « hameçon » provenant de Visa, signalez-le à Visa au moyen d'un courriel à l'adresse **phishing@visa.com**, en suivant ces simples directives :

Si vous utilisez Outlook ou Netscape :

1. créez un nouveau message courriel adressé à **phishing@visa.com**;
2. faites glisser le message hameçon de votre boîte de réception dans le nouveau message; si vous utilisez Netscape, faites-le glisser dans la section « pièce jointe »;
3. n'utilisez pas la fonction « transférer », parce que des éléments d'information se perdent et que le traitement manuel est plus complexe, à moins d'employer une interface Web à Outlook, car dans ce cas, transférer le message est la seule option possible.

Pour signaler des courriels hameçons possibles provenant d'autres organisations, envoyez un courriel à l'adresse **reportphishing@antiphishing.org**, en suivant les directives ci-dessus.

Comment déceler et éviter les escroqueries du genre « hameçon » et « usurpation de marque »

- **Protégez votre ordinateur.** Vous pouvez protéger votre ordinateur, vos fichiers de nature délicate et votre réseau contre les pirates et les virus en prenant certaines précautions de base. Utilisez des outils pour protéger votre ordinateur et vos renseignements et lutter contre les fraudes. Voici certains outils faciles à utiliser : **un antivirus, des bloqueurs d'espions, des filtres de courriels** et **des pare-feu** (accès haute vitesse à large bande).

  L'antivirus analyse votre ordinateur et les courriels que vous recevez afin de détecter les virus et les éliminer. Pour vous assurer que votre logiciel vous procure le niveau de protection le plus élevé, vous devez mettre régulièrement à jour votre antivirus. La plupart des antivirus comportent une caractéristique vous permettant de télécharger automatiquement des mises à jour lorsque vous êtes relié à Internet.

Les faux sites Web « sosies » sont conçus pour tromper les consommateurs et leur soutirer des renseignements personnels. Assurez-vous que les sites Web sur lesquels vous transigez affichent des énoncés sur la protection des renseignements personnels ainsi que sur la sécurité.

Bon nombre des antivirus actuellement sur le marché comportent aussi des bloqueurs d'espions. Un **espion** est un programme qui s'installe sur un ordinateur pour recueillir secrètement de l'information sur l'utilisateur et le transmettre à des spécialistes du marketing ou à d'autres parties. Lorsqu'on choisit un antivirus, il importe de s'assurer qu'il comporte un bloqueur d'espions.

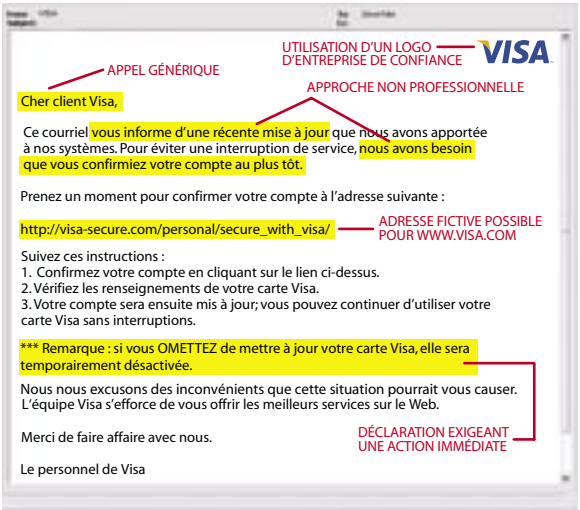
La plupart des fournisseurs de courrier électronique possèdent des **filtres de courriels** intégrés à leur application. Ces filtres bloquent les courriels non désirés, comme les pourriels.

Les utilisateurs qui ont un accès à large bande devraient prendre des précautions supplémentaires pour assurer la sécurité de leur ordinateur et de leurs fichiers informatiques. La vitesse à laquelle l'information peut être transférée d'un ordinateur à l'autre et le fait que l'ordinateur demeure branché à Internet pendant de longues périodes le rendent plus vulnérable aux pirates que dans le cas des Internautes sporadiques. Un **pare-feu** est un logiciel ou une pièce d'équipement qui empêche une communication Internet non autorisée d'entrer ou de sortir de votre ordinateur. La meilleure façon de se protéger est d'utiliser un antivirus doté d'un pare-feu.

- **Surveillez les courriels frauduleux.** Si vous recevez un courriel qui vous prévient, sans aucun ou avec très peu de préavis, qu'un de vos comptes sera fermé à moins de confirmer à nouveau vos renseignements personnels liés à la facturation, ne répondez pas au message et ne cliquez pas sur le lien qu'il contient.

  Les fraudeurs incluent en général des messages troublants ou intéressants (mais factices) dans leurs courriels pour inciter les gens à réagir sur-le-champ. Ces courriels ne sont habituellement PAS personnalisés, tandis que les messages valides qui proviennent de votre banque ou d'une entreprise faisant du commerce électronique le sont en général.

Voici un exemple de courriel hameçon type.



Si vous recevez l'un de ces courriels suspects, signalez-le à **reportphishing@antiphishing.org**; si le courriel semble provenir de Visa, signalez-le à **phishing@visa.com**. Ne cliquez sur aucun lien fourni dans le courriel, car vous pourriez insérer un programme cheval de Troie dans votre réseau ou votre ordinateur.

QU'EST-CE QU'UN PROGRAMME « CHEVAL DE TROIE » ?

Les programmes « cheval de Troie » s'installent dans votre ordinateur à votre insu et peuvent retracer les touches que vous avez utilisées sur votre clavier, ouvrant ainsi à des criminels l'accès à vos renseignements personnels.

- **Communiquez immédiatement avec Visa ou votre institution financière et faites-leur part de votre doute.** Si vous recevez un courriel suspect semblant vous avoir été envoyé par une institution financière membre de Visa, ou par Visa, avertissez votre institution financière ou Visa à l'adresse **phishing@visa.com**. Pour signaler des courriels hameçons possibles provenant d'autres organisations, envoyez un courriel à l'adresse **reportphishing@antiphishing.org**.

- **Ne répondez à aucun courriel réclamant des renseignements personnels.** Ne répondez à aucun courriel non sollicité réclamant des renseignements financiers névralgiques, tels que les numéros de votre carte de crédit, les trois derniers chiffres imprimés sur la bande de signature au verso de votre carte ou vos numéros de compte bancaire, de permis de conduire ou d'assurance sociale. Méfiez-vous également des messages affichant vos renseignements personnels et vous demandant de les mettre à jour ou de les confirmer.

- **Soyez prudent en saisissant des renseignements personnels ou financiers sur des sites Web.** Avant de saisir des renseignements financiers sur un site Web, vérifiez si l'icône d'un cadenas s'affiche sur la barre d'état de votre navigateur – ce qui signale que vos renseignements sont en sécurité pendant la transaction.

- **Soyez vigilant.** Les faux sites Web « sosies » sont conçus pour tromper les consommateurs et leur soutirer des renseignements personnels. Assurez-vous que les sites Web sur lesquels vous transigez affichent des énoncés sur la protection des renseignements personnels ainsi que sur la sécurité et lisez-les attentivement. Assurez-vous de toujours utiliser un site Web sécurisé lorsque vous fournissez des renseignements sur votre carte de crédit ou de l'information de nature délicate. Pour vous assurer que vous êtes sur un serveur Web sécurisé, vérifiez le début de l'adresse Web dans la barre d'adresse de votre navigateur – **elle devrait commencer par « https:// »**, plutôt que simplement par « http:// ».

- **Surveillez les fautes d'orthographe.** Les fautes d'orthographe dans un message ou un hyperlien ou bien sur un site Web signalent souvent des escroqueries par « usurpation de marque ».

- **Soyez prudent avant de cliquer sur un lien contenu dans un courriel.** Si le courriel contient un lien, ne cliquez pas dessus car il pourrait vous mener vers un site Web frauduleux. En cliquant sur ce lien, vous pourriez introduire un programme « cheval de Troie » dans votre réseau ou sur votre ordinateur. Tapez plutôt l'adresse Web de l'entreprise dans la barre d'adresse de votre navigateur. Si vous ne connaissez pas l'adresse, trouvez le nom de l'entreprise à l'aide d'un moteur de recherche pour vous aider à la localiser. Une fois sur son site, repérez tout renseignement, bulletin ou avis qui affiche le même message que celui contenu dans le courriel que vous avez reçu.

- **Quittez les sites suspects.** Si vous soupçonnez qu'un site Web n'est pas ce qu'il prétend être, quittez-le immédiatement et ne suivez aucune des instructions qui y sont affichées.

- **Surveillez vos transactions.** Vérifiez vos relevés de carte de crédit et de compte bancaire aussitôt que vous les recevez et assurez-vous qu'aucuns frais non autorisés n'y figurent. Si votre relevé est en retard de plus de quelques jours, appelez l'institution émettrice de votre carte de crédit ou votre banque pour confirmer votre adresse de facturation et le solde de votre compte. De plus, vous devriez entrer régulièrement en liaison avec vos comptes en ligne.

- **Signalez toujours les courriels hameçons ou les escroqueries par usurpation de marque.** Si vous recevez un courriel suspect semblant provenir de Visa, communiquez immédiatement avec Visa à l'adresse **phishing@visa.com**. Pour signaler des courriels hameçons possibles provenant d'autres organisations, envoyez un courriel à l'adresse **reportphishing@antiphishing.org**. Si vous estimez qu'un courriel hameçon est à l'origine d'une activité frauduleuse, communiquez immédiatement avec votre institution financière et votre service de police local.

Foire aux questions

Comment savoir si j'ai reçu un courriel « hameçon » ?
Méfiez-vous de tout courriel qui vous demande de fournir rapidement des renseignements personnels ou financiers. La plupart des courriels hameçons ne sont pas personnalisés, ce qui laisse supposer l'utilisation d'une liste d'envoi de masse. Vérifiez aussi s'il comporte des erreurs d'orthographe ou de grammaire.

Que dois-je faire si je soupçonne la réception d'un courriel « hameçon » ?
Si vous recevez un courriel semblant provenir de Visa, mais qui vous semble suspect, communiquez immédiatement avec Visa à l'adresse **phishing@visa.com**. Si vous estimez avoir été victime d'un hameçon, communiquez avec votre service de police local.

Comment puis-je m'assurer que je communique avec une institution financière pendant une session sécurisée ?
Vous pouvez vérifier que vous communiquez avec une institution financière légitime en examinant le certificat de site Web pendant une session sécurisée. Le certificat du site Web vérifiera l'identité du site Web auquel vous accédez et confirmera la sécurité et l'authenticité du site. C'est également une assurance qu'aucun autre site Web ne peut assumer l'identité du site sécurisé original. Consultez la documentation de votre navigateur Web pour y lire les instructions sur la façon d'afficher un certificat. Assurez-vous de toujours utiliser un site Web sécurisé lorsque vous fournissez des renseignements sur une carte de crédit ou d'autres informations de nature délicate. Pour vous assurer que vous êtes sur un serveur Web sécurisé, vérifiez le début de l'adresse Web dans la barre d'adresse de votre navigateur – **elle devrait commencer par « https:// »**, plutôt que simplement par « http:// ».

Que devrais-je faire si j'ai déjà fourni des renseignements sur ma carte de crédit ou de débit en réponse à un courriel hameçon ?
Signalez le vol d'information à l'émetteur de votre carte le plus tôt possible. Si votre carte *Visa* est compromise, communiquez avec l'institution financière émettrice de votre carte **et** faites parvenir un courriel à l'adresse **phishing@visa.com**.

Après avoir communiqué avec toutes les institutions financières pertinentes, annulez votre compte et ouvrez-en un nouveau. Vérifiez soigneusement vos relevés de compte après l'incident. Si des transactions non autorisées y figurent, communiquez avec l'émetteur de votre carte pour lui en faire part.

Comment mes renseignements personnels sont-ils transmis de façon sécuritaire sur Internet ?
Les navigateurs Web utilisent des protocoles de sécurité standard, tels que le protocole SSL (couche de sockets sécurisés) et le protocole S-HTTP sécuritaire pour permettre la transmission sécuritaire de l'information de nature privée sur Internet. Lorsque vous visitez un site Web utilisant un protocole SSL, une connexion sécuritaire est créée entre votre ordinateur et le serveur du site Web en question. Une fois la connexion établie, vous pouvez transmettre toute l'information voulue au serveur Web en toute sécurité. Le protocole S-HTTP est au contraire conçu pour l'envoi sécuritaire de messages uniques.

Comment puis-je savoir si la session avec mon navigateur Web est sécuritaire ?

Avec la plupart des navigateurs Web, tels que Microsoft Internet Explorer et Netscape Navigator, l'affichage d'une icone de cadenas fermé ou d'une clé non brisée dans le coin inférieur droit ou gauche de la fenêtre du navigateur signale une session chiffrée et sécurisée. Vous pouvez également vérifier la barre d'adresse de votre navigateur. Si l'adresse du site commence avec un **« https:// »** plutôt qu'avec le « http:// » habituel, alors la session est sécurisée.

Que dois-je faire si j'ai téléchargé un virus ou un programme « cheval de Troie » ?

Certains courriels hameçons utilisent des virus ou des programmes « cheval de Troie » pour installer des « enregistreurs de touche » sur votre ordinateur. Ces programmes saisissent et envoient au fraudeur toute information que vous entrez sur votre clavier, y compris vos numéros de carte de crédit, vos noms d'utilisateur et vos mots de passe, vos numéros d'assurance sociale, etc. Dans ce cas, vous devriez :

- installer ou mettre à jour un antivirus et un pare-feu personnel;
- mettre à jour toutes les définitions de virus et faire une recherche complète de virus sur votre ordinateur;
- modifier tous vos mots de passe en ligne;
- vérifiez vos autres comptes! Les pirates peuvent avoir eu accès à plusieurs autres comptes :
  - vérifiez vos comptes d'enchères, votre fournisseur de service Internet, vos comptes bancaires en ligne, vos comptes d'opérations sur titres en ligne, vos comptes de commerce électronique ainsi que tout autre accès utilisant votre mot de passe en ligne.

Qu'est-ce qu'un certificat numérique et comment contribue-t-il à assurer la sécurité ?

Les certificats numériques sont délivrés par des autorités de certification soumis à des vérifications et à des contrôles intensifs avant d'authentifier un site Web ou les éléments qu'il contient. Ce certificat identifie l'origine du site, tout en vérifiant que le site n'a subi aucune violation. Lorsque votre navigateur Web est assorti d'un certificat, il vérifiera si celui-ci a été délivré par une autorité de certification légitime. S'il y a correspondance, votre session se poursuivra. Autrement, votre navigateur affichera un avertissement et l'annulation de la session sera le geste le plus sûr à poser.