Attention aux arnaqueurs!

La sécurité des informations, j'y veille! *Volume 3, Numéro 1, Mai 2013*

Que ce soit par le Web, par courriel ou même par téléphone, soyez toujours vigilant quant aux informations que vous donnez à des étrangers. L'hameçonnage est une technique courante utilisée par les fraudeurs pour essayer de soutirer des renseignements personnels. Voici quelques exemples et techniques de piratage informatique auxquels il faut être très attentif, tant au travail qu'à la maison.

L'hameçonnage téléphonique!

Dans la dernière année, des cybercriminels ont tenté d'effectuer des escroqueries du style assistance technique par téléphone. Ces escrocs utilisent souvent des annuaires téléphoniques publics pour connaitre votre nom et d'autres informations personnelles quand ils vous appellent.

Par exemple, certains prétendent appeler de la compagnie Microsoft. Ils proposent de résoudre vos problèmes d'ordinateurs ou de vous vendre une licence pour un logiciel. Une fois qu'ils vous ont mis en confiance, ils vous demanderont d'aller sur un site Web, pour installer un logiciel leur donnant accès à votre ordinateur, ou encore requerront votre nom d'utilisateur et votre mot de passe.

Ne divulguez jamais d'informations confidentielles par téléphone, telles que numéro de carte de crédit, informations bancaires ou **informations concernant votre ordinateur**. Les compagnies, telle Microsoft, ne font pas d'appels téléphoniques non souhaités pour solliciter des informations de la sorte. Lorsque ces fraudeurs ont l'information désirée, ils peuvent :

- installer un logiciel malveillant qui pourrait capturer des données sensibles comme vos informations d'authentification pour vos services bancaires en ligne;
- contrôler votre ordinateur à distance et ajuster les paramètres pour rendre votre ordinateur vulnérable;
- demander votre numéro de carte de crédit pour vous facturer des services fictifs;
- vous diriger vers des sites Web frauduleux et vous demander d'entrer votre numéro de carte de crédit et d'autres informations personnelles ou financières.

Ce qu'il faut faire si vous pensez être victime de fraude

⇒ Prenez des notes : inscrivez le moment où vous avez constaté la fraude et les mesures que vous avez prises, y compris le nom des personnes avec lesquelles vous avez parlé et les dates des communications.
⇒ Déposez un rapport à la police de votre municipalité.
⇒ Entrez en communication avec vos institutions financières et toute autre société où vos comptes ont été trafiqués, ou risquent de l'être.
⇒ Informez les deux agences d'évaluation du crédit du Canada, TransUnion et Equifax.
⇒ Communiquez avec le Centre antifraude du Canada.

Agence de la santé et des services sociaux de la Côte-Nord
Québec

L'hameçonnage par courriel

Technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. Le malfaiteur tend des milliers d'hameçons, souvent par courriel frauduleux, et fait croire à la victime qu'elle s'adresse à un tiers de confiance afin de lui soutirer des renseignements personnels.

Ce type d'attaque est souvent utilisé pour voler de l'argent. Les cibles les plus courantes sont les services bancaires, Paypal, les organismes gouvernementaux, les sites de ventes aux enchères tel eBay, etc.

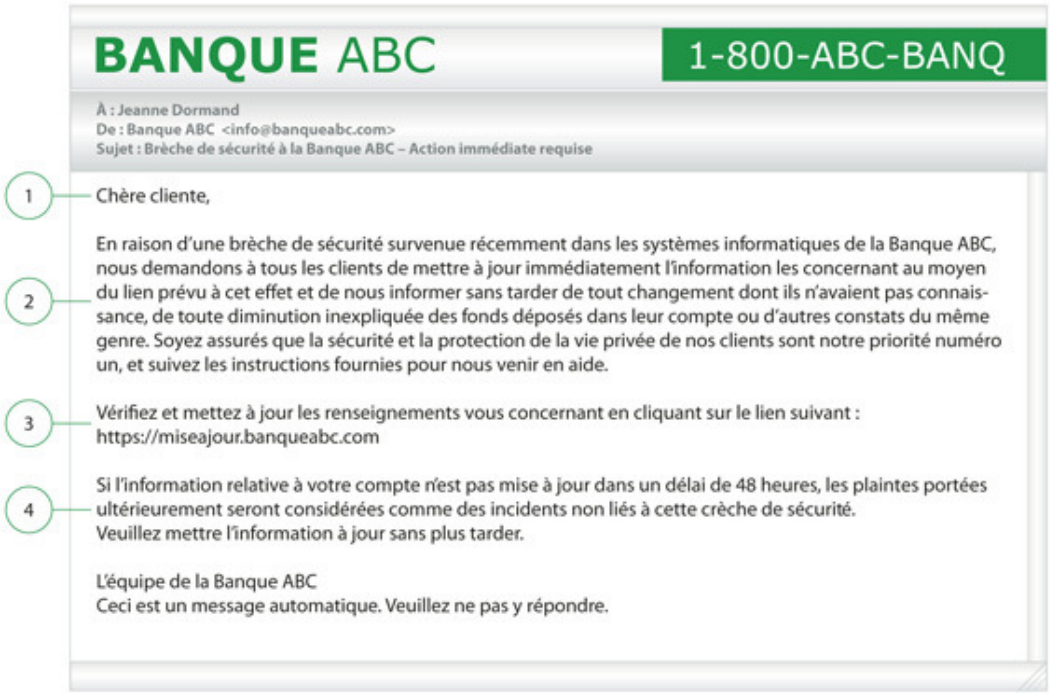
Comment reconnaître un courriel d'hameçonnage

1. Le courriel commence par une formule de salutation générale comme « Chère Cliente » plutôt que par votre nom.

2. Certains courriels feront référence à un problème au sujet de votre compte et insisteront sur la nécessité d'agir sans tarder en vous référant à un lien Web pour confirmer vos renseignements personnels.

3. Souvent, ces liens Web, qui semblent valides, vous mèneront vers de faux sites Web.
   Comment le savoir : faites glisser votre souris lentement sur le lien suggéré, sans cliquer, jusqu'à ce que s'affiche une boîte indiquant l'adresse URL (adresse Web). Vous pourrez alors constater que l'adresse Web de la boîte diffère de celle indiquée dans le courriel. Ne cliquez pas sur ce lien.

4. Habituellement, l'expéditeur du courriel invoque une situation urgente pour vous amener à répondre immédiatement.



BANQUE ABC 1-800-ABC-BANQ

À : Jeanne Dormand
De : Banque ABC <info@banqueabc.com>
Sujet : Brèche de sécurité à la Banque ABC – Action immédiate requise

1 Chère cliente,

2 En raison d'une brèche de sécurité survenue récemment dans les systèmes informatiques de la Banque ABC, nous demandons à tous les clients de mettre à jour immédiatement l'information les concernant au moyen du lien prévu à cet effet et de nous informer sans tarder de tout changement dont ils n'avaient pas connaissance, de toute diminution inexpliquée des fonds déposés dans leur compte ou d'autres constats du même genre. Soyez assurés que la sécurité et la protection de la vie privée de nos clients sont notre priorité numéro un, et suivez les instructions fournies pour nous venir en aide.

3 Vérifiez et mettez à jour les renseignements vous concernant en cliquant sur le lien suivant : https://miseajour.banqueabc.com

4 Si l'information relative à votre compte n'est pas mise à jour dans un délai de 48 heures, les plaintes portées ultérieurement seront considérées comme des incidents non liés à cette crèche de sécurité. Veuillez mettre l'information à jour sans plus tarder.

L'équipe de la Banque ABC
Ceci est un message automatique. Veuillez ne pas y répondre.

Anne Paquet
Officier de sécurité régional
Direction régionale des ressources informationnelles (DRRI)
Pour questions ou commentaires : anne.paquet.09siles@ssss.gouv.qc.ca

Dépôt légal
Bibliothèque et Archives nationales du Québec, 2013
ISSN : 1927-7911

Source : http*://www.microsoft.com/fr-fr/security/online-privacy/avoid-phone-scams.aspx,*
*http://www.fcac-*acfc*.qc.ca/fra/consommateurs/fraude/courrielTelepFraude/exCourriel-fra.asp*