

**Cet article de l'ABC a initialement été publié dans le numéro de février 2006 de 50Plus Magazine par la CARP, association canadienne pour les 50 ans et plus.**

## **« L'HAMEÇONNAGE » DE VOS RENSEIGNEMENTS PERSONNELS Se protéger contre les courriels frauduleux**

Il existe un nouveau type de courriel frauduleux qui n'est pas uniquement contrariant : il peut mener au vol d'identité. Cette fraude est appelée « hameçonnage » et utilise des courriels et des sites Web frauduleux pour obtenir vos précieux renseignements personnels. Comme mars est le Mois de la prévention de la fraude, voilà le moment tout indiqué pour apprendre comment se protéger contre la fraude par hameçonnage. *Identifiez-la. Signalez-la. Enrayez-la.*

« Les courriels hameçons peuvent sembler légitimes, mais ils sont envoyés par des criminels espérant leurrer leurs destinataires en les incitant à divulguer leurs renseignements personnels, déclare Caroline Hubberstey, directrice, Affaires publiques et relations avec la collectivité, à l'Association des banquiers canadiens (ABC). Vous ne donneriez pas votre numéro d'assurance sociale, votre mot de passe bancaire ou votre numéro de carte de crédit au premier venu que vous rencontrez sur la rue, qui vous téléphone ou qui frappe à votre porte. Appliquez les mêmes règles lorsque vous êtes en ligne. »

Les fraudeurs envoient des courriels hameçons souvent liés à une organisation qui semble légitime – banque, fournisseur de carte de crédit, commerce de détail ou organisme gouvernemental. Ces courriels peuvent vous amener à un site Web ou à une fenêtre apparaissant à l'écran, où l'on vous demande vos numéros de carte de crédit, vos mots de passe, des données sur vos comptes ou d'autres renseignements personnels. L'une des tactiques de l'hameçonnage consiste à faire parvenir un courriel indiquant que votre compte sera fermé ou gelé ou que vous devez répondre immédiatement parce que votre compte peut avoir été compromis.

Voici quelques mesures simples pour éviter d'être victime d'une fraude par courriel.

- Ne répondez jamais à un courriel vous demandant des renseignements personnels.
- Installez un anti-pourriel et un anti-virus sur votre ordinateur et maintenez-les à jour. Installez aussi un pare-feu personnel qui agira comme obstacle aux virus. Votre boutique d'informatique locale peut vous renseigner davantage à ce sujet.

- Soyez prudent lorsque vous téléchargez des fichiers à partir d'Internet et installez des programmes. Faites aussi preuve de prudence lorsque vous lisez des courriels comportant des pièces jointes – les courriels servent souvent à transmettre des virus.
- Passez en revue vos relevés bancaires et de carte de crédit afin de vous assurer que toutes les transactions sont légitimes.
- Lorsque vous entrez des renseignements personnels, assurez-vous d'utiliser un site Web sécuritaire. Recherchez le symbole du cadenas fermé dans le coin inférieur droit de votre écran.

### **Comment repérer un courriel hameçon?**

Affichez ces conseils à proximité de votre ordinateur comme moyen pratique de déceler les courriels frauduleux.

- Le courriel demande-t-il de fournir des renseignements personnels? Par exemple, votre banque ne vous fera jamais parvenir un courriel vous demandant de lui communiquer des renseignements personnels, comme vos numéros de compte ou vos mots de passe.
- Ce courriel est-il menaçant? Méfiez-vous des courriels non sollicités, de nature urgente, qui vous avertissent que vos comptes seront fermés ou que votre accès sera limité si vous n'y répondez pas.
- Le courriel commence-t-il par « Cher ami » ou « Cher client », plutôt que par votre nom? Les courriels frauduleux ne sont généralement pas personnalisés.
- Ce courriel vous semble-t-il inusité? Examinez-le soigneusement et vous pourriez y noter des erreurs d'orthographe, un langage inhabituel ou des logos qui semblent étranges.

Si vous répondez « oui » à l'une de ces questions, ne répondez pas à ce courriel et ne cliquez sur aucun lien qu'il renferme. Signalez-le à la banque ou à la compagnie dont l'identité est usurpée et détruisez-le. Si vous avez fourni des renseignements personnels en réponse à un courriel frauduleux, communiquez immédiatement avec votre banque ou l'organisation ciblée et la police.

Pour en savoir davantage sur l'hameçonnage et d'autres types de fraude financière, consultez le site Web de l'ABC à l'adresse [www.cba.ca/fraude](http://www.cba.ca/fraude). On peut aussi obtenir gratuitement la brochure de l'ABC, intitulée *Protéger son argent*, en ligne ou en composant le 1 800 263-0231.