Soyez un aîné **avisé**

Stratégies de protection contre la fraude et le **vol d'identité**

fiche 5

Les fraudeurs utilisent vos qualités pour abuser de vous. Ils visent les aînés parce qu'ils sont confiants et optimistes et qu'ils répondent au courrier qu'ils reçoivent.

Repérez la fraude. Soyez vigilant.

Hameçonnage et logiciels malveillants

Bernadette vérifie son courriel. Elle voit un message provenant d'UPS intitulé « Numéro de suivi 76290X00P4Q38Z ». Elle l'ouvre. Le message dit que sa commande est arrivée : il ne lui reste qu'à cliquer sur le lien au bas du message et à entrer ses renseignements personnels pour finaliser la livraison du colis. Bernadette ne se rappelle pas avoir commandé quoi que ce soit, mais c'est bientôt son anniversaire de naissance… peut-être est-ce un cadeau de son cousin qui vit en Arizona?

REPÉREZ LA FRAUDE.

- Vous recevez un courriel qui semble provenir de votre banque ou d'une entreprise ou d'un service public que vous connaissez
- Si vous cliquez sur le courriel, vous aboutirez à un faux site Web qui aura l'air légitime—ou un peu suspect ou contiendra des fautes d'orthographe
- Si vous entrez des renseignements sur votre compte ou votre carte de crédit, ou un mot de passe, les escrocs saisiront ces renseignements à l'aide d'un logiciel
- Le faux site Web peut contenir un virus qui infectera votre ordinateur et y recueillera vos renseignements personnels

SOYEZ VIGILANT.

- Ne répondez pas au courriel et ne téléphonez pas au numéro indiqué
- N'utilisez que les numéros de téléphone, adresses courriel et numéros de service à la clientèle qui figurent sur d'anciennes factures provenant de l'organisme; cherchez les numéros dans l'annuaire téléphonique ou en ligne; renseignez-vous sur la légitimité du courriel auprès de l'organisme
- Ne cliquez pas sur les liens contenus dans un courriel à moins de connaître l'expéditeur
- Regardez les politiques des organismes avec lesquels vous faites affaire en ligne; les banques disent clairement qu'elles n'envoient jamais de courriels à leurs clients
- Utilisez un logiciel de détection de virus et mettez les fichiers suspects en quarantaine; vous pouvez télécharger un logiciel antivirus gratuit ou en acheter un

Connaissez votre ordi—ne vous faites pas avoir!

Les fraudeurs ciblent des adresses courriel au hasard en espérant que quelqu'un répondra. Le partage de renseignements personnels augmente le risque de vol d'identité.

Soyez un aîné **avisé**

Stratégies de protection contre la fraude et le **vol d'identité**

Télémarketing frauduleux et arnaque au messages texte

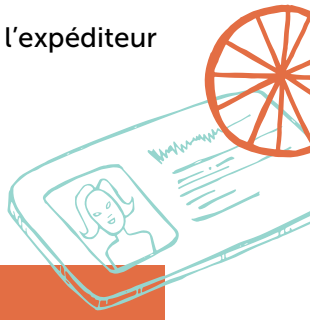
Joanne reçoit un message texte lui disant qu'elle a gagné un prix : un voyage tous frais payés à San Francisco! On lui demande de cliquer sur un lien pour réclamer son prix. Le lien l'amène à un site Web où on lui demande des renseignements personnels tels que son nom complet, sa date de naissance et son numéro d'assurance sociale (NAS). Elle fournit les renseignements et répond au texto « Qui êtes-vous? » Avant qu'elle ait pu s'en rendre compte son identité avait été volée —quelqu'un se fait passer pour elle. Les escrocs peuvent utiliser vos renseignements personnels pour obtenir des cartes de crédit, faire des achats, changer vos données de facturation ou même réhypothéquer votre maison!

REPÉREZ LA FRAUDE.

- Vous recevez un texto ou un téléphone d'un numéro inconnu vous offrant un prix
- Pour réclamer ce prix, vous devez partager des renseignements personnels ou bancaires, des mots de passe ou des numéros d'identité
- Le texto ou l'appel téléphonique peut provenir d'une personne qui prétend travailler pour votre institution financière (banque, caisse populaire), un service public (hydro, câble) ou une agence gouvernementale; elle peut dire, par exemple, que la sécurité de votre compte a été compromise

SOYEZ VIGILANT.

- Conservez votre numéro d'assurance sociale, votre passeport et tous vos autres renseignements personnels en lieu sûr
- Ne répondez pas à ces messages, même pour dire « Non, merci », « Qui êtes-vous? » ou « Ne m'écrivez plus ». Ils s'emparent de vos renseignements dès que vous répondez.
- Si vous êtes inquiet au sujet de votre compte, trouvez un ancien relevé et appelez vous-même votre institution, service public ou agence
- Ne cliquez pas sur un lien fourni dans un texto ou courriel dont vous ne connaissez pas l'expéditeur
- Verrouillez votre boîte aux lettres pour prévenir le vol de courrier
- Videz régulièrement votre boîte aux lettres
- Déchiquetez les documents qui pourraient contenir des renseignements personnels —les voleurs fouillent dans vos poubelles!



Soyez discret—protégez vos renseignements personnels.

Ne partagez pas vos NIP, mots de passe, votre NAS ou autre identifiant personnel. Ne donnez votre adresse et numéro de téléphone qu'à des personnes en qui vous avez confiance.

Pour signaler les fraudes et arnaques, appelez :

1. Votre GRC locale ou
2. le Centre canadien de lutte contre la fraude au 1.888.495.8501

Vous trouverez d'autres stratégies de protection contre la fraude sur le site : www.bcli.org/be-savvy

CENTRE CANADIEN D'ÉTUDES SUR LE DROIT DES AÎNÉS
Centre for Public Legal Education Alberta
Government of Canada / Gouvernement du Canada
Canada