Utiliser la technologie? Certainement!

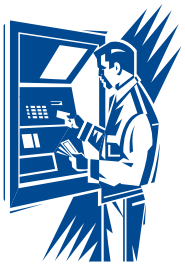
FEUILLETS DE RENSEIGNEMENTS SUR LES TECHNOLOGIES COURANTES ET LES AÎNÉS CANADIENS

LES TECHNOLOGIES COURANTES SONT-ELLES SÛRES?

Le feuillet n° 6 porte sur les questions de sécurité liés aux technologies courantes.

L'émergence de nouvelles technologies a engendré de nouvelles façons de commettre des crimes. Depuis les méfaits perpétrés par voie électronique jusqu'aux organismes de bienfaisance frauduleux, la technologie offre aux criminels de nouveaux outils. Elle fait toutefois également partie de la solution, puisque les entreprises, les banques, les organismes, les services policiers et les gouvernements échangent de l'information et prennent des mesures pour enrayer le crime. Les institutions bancaires et les fournisseurs de services internet ont défini des codes et des mots de passe ainsi que des systèmes de chiffrement pour protéger leur clientèle. Bien que certaines manoeuvres criminelles et frauduleuses visent directement les personnes âgées, il y a certaines règles fort simples que vous pouvez suivre afin de réduire grandement les risques de « vous faire avoir ». Bien sûr, la meilleure protection consiste à être prudent au moment d'effectuer une transaction qui met en cause une somme d'argent ou des renseignements personnels.

Conseils au sujet des services bancaires automatisés



- Prenez garde aux gens qui vous entourent lorsque vous êtes dans une file ou devant le guichet.
- Soyez discret au moment d'inscrire votre numéro d'identification personnelle (NIP) au guichet automatique ou chez un détaillant. Cachez le clavier numérique avec votre corps ou votre main.
- N'écrivez pas votre NIP et ne le confiez à personne. Si vous devez l'écrire, gardez-le dans un endroit distinct de votre carte.
- Assurez-vous de ne pas laisser votre carte ou votre argent dans la machine.
- Si vous avez besoin d'aide, ne vous adressez pas à la personne derrière vous. Entrez dans la banque et parlez à un employé.

Préparé par le *Nova Scotia Centre on Aging,* Mount Saint Vincent University, pour les ministres fédéral, provinciaux, territoriaux responsables des aînés. Septembre 2001

- Conservez tous vos reçus de transaction afin de vérifier votre livret ou votre état de compte mensuel.

Conseils touchant la sécurité sur Internet

- Effacez sans l'ouvrir tout message (courriel) non sollicité (message poubelle) venant de personnes ou de compagnies inconnues.
- Si vous achetez en ligne, faites affaire avec des compagnies réputées qui fournissent de l'information claire sur la façon de les rejoindre et qui garantissent la sécurité des transactions.
- Demandez à toute compagnie inconnue de vous fournir des références et faites-en la vérification avant d'effectuer des achats.
- Recherchez en haut ou en bas de l'écran de votre ordinateur un symbole illustrant une clé intacte ou un cadenas fermé pour indiquer que vous vous trouvez dans un environnement sécurisé au moment d'entrer l'information sur votre carte de crédit.

- Si vous visitez des forums ou des groupes de discussion, ne donnez pas spontanément certains renseignements personnels comme votre nom, votre numéro de téléphone ou votre adresse.
- Si vous visitez l'Internet régulièrement, renseignez-vous sur les logiciels coupe-feu qui vous protégeront des pirates informatiques, ou vérifiez si votre ordinateur est muni de dispositifs de sécurité. Pour détecter les virus dans les pièces jointes aux courriels, sauvegardez-les d'abord sur une disquette, puis soumettez-les à votre programme antivirus.

Télémarketing frauduleux

Bien qu'il existe un grand nombre de firmes de télémarketing légitimes, on démasque une entreprise frauduleuse toutes les 48 heures. En 2000, plus de 50 % des victimes canadiennes déclarées avaient plus de 60 ans et plus de 60 % d'entre elles étaient des femmes. Les entreprises légitimes ne font pas pression sur la clientèle et ne se contentent pas de demander de l'argent; elles vous envoient de l'information écrite et vous donnent amplement de temps pour prendre une décision.

PhoneBusters est un centre national d'appel contre le télémarketing trompeur qui est exploité depuis 1993 par la Police provinciale de l'Ontario. En plus de renseigner le public, **PhoneBusters** recueille des données probantes et des statistiques sur les victimes et diffuse ces renseignements aux organismes d'application de la loi. Il existe maintenant une nouvelle cassette vidéo intitulée « **Combattez la fraude par**

téléphone - C'est un piège! », dont vous pouvez obtenir copie gratuitement en téléphonant au **1-888-654-9426**. Vous pouvez également demander qu'un exposé soit livré à votre organisme.

SeniorBusters est un groupe de bénévoles qui travaillent pour PhoneBusters et fournissent de l'information et du soutien téléphonique aux personnes âgées ayant pu être victimes de fraude téléphonique. Pour signaler une fraude ou obtenir de l'information, vous pouvez communiquer avec **PhoneBusters** ou **SeniorBusters** au **1-888-654-9426**. Vous pouvez également visiter leur site Web à **www.phonebusters.com**.

Méfiez-vous...

- des prix que vous auriez soi-disant remportés sans même avoir participé à un concours;
- de la nécessité de payer « un montant minime » ou des frais d'expédition pour recevoir votre prix;
- des promesses de prix de valeur en retour d'un achat peu coûteux;
- des numéros 1-900. Ils engendrent des frais automatiques élevés - vérifiez le numéro auprès du Bureau d'éthique commerciale ou de PhoneBusters;
- des appels téléphoniques d'une personne qui prétend être un inspecteur de banque ou un agent de police - raccrochez et communiquez avec votre banque;.
- des transactions où on vous demande votre numéro de carte de débit ou votre numéro d'assurance sociale sans raison valable.

La **protection de la vie privée du consommateur** est devenue une préoccupation de premier plan pour bon nombre de Canadiens, compte tenu de la prolifération des cartes de débit, des services bancaires par téléphone et par Internet, des programmes de primes d'achat et des autres méthodes électroniques de stockage d'information. Protégez vos renseignements personnels — le numéro d'assurance sociale, le numéro de carte santé, les numéros de comptes et même l'état matrimonial constituent de l'information privée!

La meilleure façon de contrer la fraude est de la prévenir. Soyez informé. Soyez préparé. Soyez alerte!

Sources :

Partners Against Consumer Telefraud. *Don't Fall for a Telephone Line!: Working to Reduce Telemarketing Fraud in Nova Scotia.* (Brochure)

Guide du consommateur canadien. Ottawa : Industrie Canada, 1999. No de cat. C2-422/1999F.

Lindsay, Colin. *Un portrait des aînés au Canada* , 3e édition. Ottawa : Statistique Canada, 1999. No de cat. 85-519F.

Statistiques sur la fraude téléphonique, site web de Phonebusters. Information extraite le 11 mai 2001 de www.phonebusters.com/Fr/Statistics/canada_stats7_2000.html.

Autres feuillets dans la série

No 1. Survol de la série
No 2. Télécommunications : téléphones et autres systèmes
No 3 Ayez l'œil sur votre argent : technologie et opérations bancaires
No 4. Les ordinateurs : pour être branché sur Internet
No 5. Pour le bien de votre santé : technologie et soins de santé
No 6. Les technologies courantes sont-elles sûres?
No 7. Les personnes âgées, un marché important!

Mots techno

Chiffrement - Conversion ou embrouillage des données informatiques ayant pour objet de protéger l'information que vous transmettez lors d'une transaction délicate comme l'utilisation de services bancaires sur Internet ou un achat en direct avec une carte de crédit.

Coupe-feu - Dispositif de sécurité installé dans certains ordinateurs, mais pas tous, dans le but de protéger l'information en empêchant d'autres ordinateurs d'y avoir accès par le biais d'Internet. Beaucoup de réseaux sont dotés de **coupe-feu** qui assurent la protection des renseignements personnels. Si vous avez l'intention d'utiliser régulièrement Internet à partir de votre domicile, vérifiez si votre ordinateur possède déjà un logiciel coupe-feu ou si vous devez en installer un.

En direct, ou **en ligne** - Le fait d'être branché à un ordinateur ou à un système de télécommunications. Le terme **en ligne** est souvent utilisé pour désigner quelqu'un qui est connecté à Internet à un moment précis.

Fournisseur de service Internet - Entreprise qui offre aux particuliers et à d'autres entreprises l'accès à Internet et à d'autres services connexes.

Guichet automatique - Sert à effectuer des transactions bancaires courantes telles déposer ou retirer de l'argent, transférer des fonds, obtenir le solde du compte ou un relevé des transactions effectuées et payer des factures. Les guichets sont accessibles en tout temps et vous permettent d'effectuer ces transactions au moment qui vous convient, 24 heures par jour.

Internet - Immense réseau informatique au sein duquel les ordinateurs sont reliés à des fournisseurs de service internet de manière à pouvoir échanger de l'information. L'Internet est accessible à toute personne qui a accès à un ordinateur relié à un fournisseur de service.

Message poubelle (courriel non sollicité) - Ce genre de message abonde sur Internet, où l'on transmet de multiples exemplaires d'un même message afin qu'il parvienne à des personnes qui, autrement, n'auraient pas choisi de le recevoir.

NIP (numéro d'identification personnelle) - Code, formé de lettres, de chiffres, ou des deux, qui vous permet d'accéder à vos comptes bancaires à l'aide du guichet automatique, du téléphone ou d'un ordinateur.

Pirate informatique - Terme que certains utilisent pour désigner un « habile programmeur » et d'autres, pour parler de « quelqu'un qui tente de s'infiltrer dans les systèmes informatiques ».

Virus informatique - Code de programmation qui est transmis à votre ordinateur par le biais d'une annexe à un message électronique qui est infectée, d'un document téléchargé à partir d'un site web infecté ou d'un fichier se trouvant sur une disquette infectée. Les virus peuvent entraver le fonctionnement de votre ordinateur et il arrive souvent qu'ils soient conçus pour se transmettre automatiquement à d'autres utilisateurs. Vous pouvez protéger votre ordinateur en vous procurant un logiciel de détection des virus (ou antivirus).

Dans cette série, le masculin est employé comme genre neutre dans le but d'alléger les textes; on ne doit y voir aucune discrimination.

Préparé par le *Nova Scotia Centre on Aging,* Mount Saint Vincent University, pour les ministres fédéral, provinciaux, territoriaux responsables des aînés. Septembre 2001