L’Association des banquiers canadiens (ABC) a créé une trousse pour les aîné(e)s, destinée à les aider à déceler les arnaques et à adopter de façon proactive les mesures nécessaires pour protéger contre la fraude leurs renseignements personnels et financiers.

Les banques au Canada travaillent sans relâche afin d’assurer la protection de leurs clients contre la fraude et les cybermenaces. Elles collaborent étroitement entre elles et avec les organismes de réglementation du secteur bancaire, les forces de l’ordre et tous les niveaux de gouvernement en vue de protéger du crime leurs clients et le système financier. Vous pouvez suivre de simples mesures pour contribuer à votre propre protection et à celle de votre argent contre la fraude et les escroqueries.

Contenu

01 **Prévention de la fraude – liste de vérification**

02 **Défense contre les arnaques fréquentes**

- **02.1** Fraude par courriel, ou hameçonnage
- **02.2** Arnaque téléphonique ou vocale
- **02.3** Arnaque des grands-parents
- **02.4** Arnaque du soutien technique
- **02.5** Fraude sentimentale
- **02.6** Applications et sites frauduleux
- **02.7** Rançongiciel

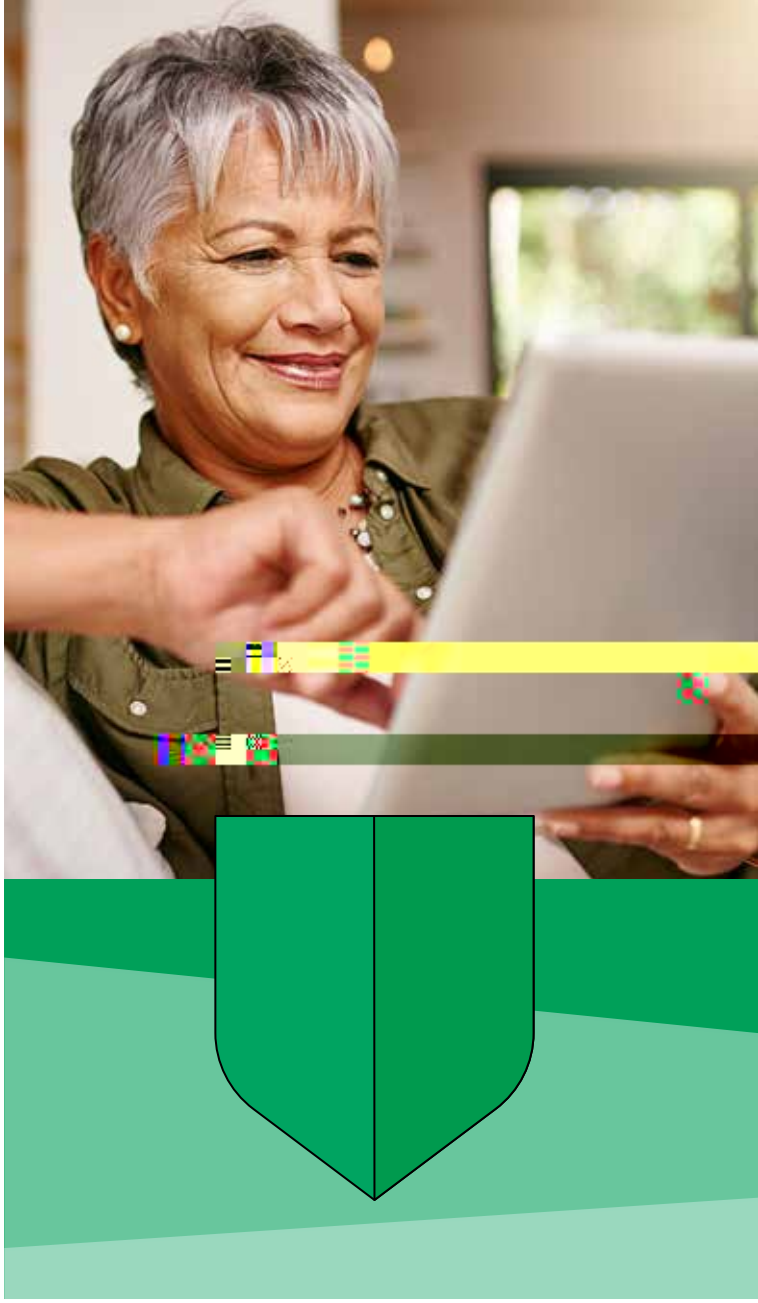
03 **Choix de mots de passe complexes**

04 **Protection contre l’exploitation financière**

05 **Ressources additionnelles**

Prévention de la fraude – liste de vérification

Renseignements personnels, finances et appareils connectés à Internet : protection contre la fraude et les arnaques



Une vérification facile afin de veiller à ce que vous preniez les mesures simples mais nécessaires pour préserver vos renseignements personnels et financiers est un excellent moyen proactif de vous protéger contre la fraude et les arnaques.

Au Canada, les banques utilisent une technologie de pointe et des niveaux de sécurité complexes afin de protéger leurs clients contre la fraude. Cela dit, vous êtes également responsable de votre propre protection, et donc de l'adoption de mesures dans ce sens.

1. Protection de vos appareils

Installez des logiciels antivirus et anti espions ainsi qu'un pare-feu sur tous vos appareils connectés (comme le cellulaire, l'ordinateur de bureau et la tablette), et mettez-les à jour régulièrement. Installez toutes les nouvelles versions aussitôt commercialisées pour vous protéger des plus récentes menaces. Encore mieux : déclenchez la mise à jour automatique afin de ne rien rater!

2. Choix de phrases et de mots de passe distincts et complexes

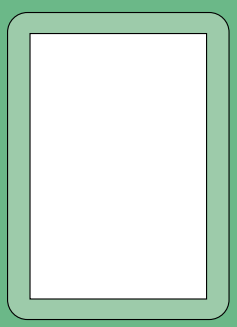
Créez un mot ou une phrase de passe distincts pour chaque compte en ligne et chaque site! C'est très important vu que l'atteinte à la sécurité des données dans un site Web pourra entraîner l'acquisition de vos coordonnées de connexion par des criminels qui essaieront de les utiliser sur d'autres sites au moyen de tentatives d'infiltration simultanées. Si vous avez un doute quant à l'intégrité du mot de passe d'un compte, changez-le immédiatement ainsi que sur tout autre compte où vous l'auriez également utilisé.

3. Déchiquetage des documents comportant des renseignements sensibles

Détruisez tous vos documents financiers avant de les jeter à la poubelle ou de les mettre au recyclage. Déchiquetez, déchirez ou brûlez les relevés bancaires et de cartes de crédit, ainsi que tout autre document comportant des renseignements sensibles.

4. Restriction du partage en ligne de renseignements personnels sensibles

Les cybercriminels n'ont besoin que d'une infime quantité de vos renseignements personnels pour voler votre identité en ligne et commettre des crimes financiers. Choisissez bien quelles données personnelles vous communiquez en ligne. Ne fournissez donc jamais votre date de naissance, votre addresse à domicile, votre numéro d'assurance sociale ou tout autre renseignement personnel ou financier qui pourra servir dans les questions de vérification. Ne communiquez que les renseignements nécessaires, en privé et seulement si vous avez initié le contact et vérifié l'identité de l'interlocuteur.



Défense contre les arnaques fréquentes

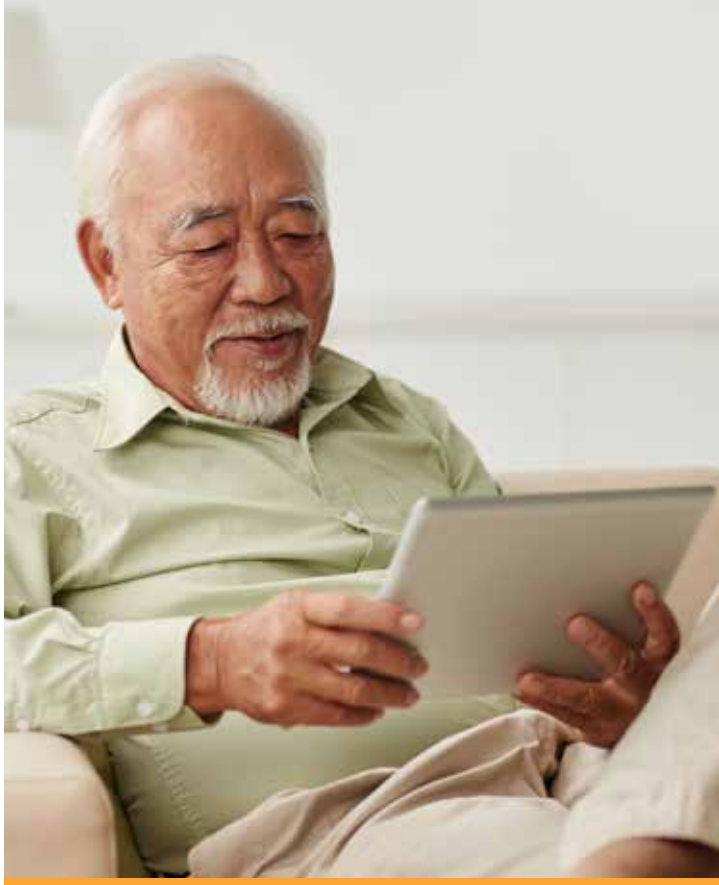
Quelques-unes des arnaques les plus répandues dont il faut se méfier :

- Fraude par courriel, ou hameçonnage
- Arnaque au téléphone ou par messagerie vocale
- Arnaque des grands-parents
- Arnaque du soutien technique
- Fraude sentimentale
- Applications et sites Web frauduleux
- Rançongiciels
- Arnaques d'urgence

De nombreuses arnaques sont des variations sur un même ensemble de tactiques utilisées par les criminels pour vous amener à leur révéler vos renseignements personnels sensibles.

Ingénierie sociale – comprendre les techniques utilisées par les arnaqueurs

L'ingénierie sociale est le processus par lequel les criminels exploitent la nature humaine et notre soif de répondre aux demandes urgentes, d'être utile ou de de régler le problème d'un proche afin de nous amener à révéler des renseignements qui serviraient à commettre de la fraude financière. Les tactiques d'ingénierie sociale nous poussent à immédiatement ouvrir un lien ou une pièce jointe contenant un maliciel, ou à révéler sans hésiter des renseignements sensibles qui seront utilisés pour lancer des cybercrimes et de commettre de la fraude financière.



Méfiez-vous de ces trois techniques d'ingénierie sociale

01 Usage de la peur comme motivateur. Les courriels, les appels et les textos menaçants ou intimidants sont des tactiques d'ingénierie sociale utilisées afin de nous motiver à accéder aux demandes de renseignements personnels ou de fonds.

02 Demandes urgentes. Les messages de toute forme qui contiennent des demandes urgentes pour des renseignements personnels sont une flagrante indication d'arnaque.

03 Opportunités alléchantes ou demandes inusitées. Attention, si l'un de vos contacts en ligne vous offre un accès gratuit à une application, à un jeu ou à un programme en échange de vos coordonnées de connexion! Également, les applications et les logiciels gratuits comportent souvent un maliciel.

Les appels et les

ATTENTION à

ATTENTION à l’arnaque

Fonctionnement de l’arnaque

Cette arnaque présente quelques variations, toutes sur le même thème.

- Un escroc vous appelle prétendant que votre ordinateur a été piraté ou distribue des virus. Il vous propose de régler le problème moyennant paiement.
- Des fenêtres contextuelles s’ouvrent sur votre écran avec un numéro à appeler pour supprimer le virus détecté sur votre ordinateur.
- Vous recevez un courriel hameçon contenant une fausse facture d’un abonnement à un antivirus que vous devez renouveler, avec un numéro de téléphone à appeler pour annuler le service.

Une fois que l’arnaqueur aura établi un contact avec vous, il demandera un accès à distance à votre ordinateur pour essayer de voler des données financières et personnelles, ou vous demandera de l’argent pour en supprimer de dangereux virus qui n’existent évidemment pas.

ATTENTION à la fraude sentimentale

La fraude sentimentale se trouve dans le peloton de tête des arnaques les plus fréquentes, selon le Centre antifraude du Canada. Cette fraude a coûté aux Canadiens plus de 50,3 millions de dollars en 2023.

Fonctionnement de ce stratagème

Généralement, la victime et le criminel se rencontrent sur les médias sociaux ou sur un site de rencontre. Notons que le criminel, tout comme la victime, peut être un homme ou une femme. Le criminel essaiera de créer une relation avec sa victime, y consacrant parfois des mois, dans l'objectif de convaincre la victime qu'ils vivent une relation amoureuse.

Le plus souvent, le fraudeur annonce qu'il se trouve dans une autre ville ou un autre pays et désire rencontrer l'élu(e) de son cœur en personne. Il laissera entendre qu'il n'a pas les moyens de se payer le voyage et demandera l'aide de la victime à cet égard.

Une variante veut que le criminel annonce qu'il a une urgence, un membre de la famille malade par exemple, et qu'il a besoin d'une aide financière de la part de la victime pour se rendre au chevet du patient.

Les appels à l'aide sont une arnaque et tout l'argent transféré par la victime, souvent de grosses sommes, se retrouve entre les mains d'escrocs.

Vu la prépondérance des arnaques sentimentales, gardez en tête qu'il se peut que votre âme sœur trouvée sur un site de rencontre fasse partie des arnaqueurs. Voici quelques signes révélateurs d'un possible stratagème de rencontre.

ATTENTION aux applications et sites Web frauduleux (mystification)

Les escrocs conçoivent des applications et des sites d'achat en ligne qui ressemblent aux applications et aux sites des vrais détaillants, avec leur logo et leur nom.

Ces sites Web ne sont qu'une façade pour que ces criminels puissent voler des données de cartes de crédit et des renseignements personnels importants.

Voici des exemples pour vous aider à identifier les faux magasins en ligne.

Sites Web

- Le site Web est mal conçu, ne présente pas une image professionnelle et contient des hyperliens rompus.
- Vous ne parvenez pas à connaître l'adresse civique ou le numéro de téléphone de l'entreprise.
- Les politiques relatives aux ventes, aux retours et à la confidentialité sont difficiles à repérer ou ne sont pas claires.
- Le bouton « Retour » ne fonctionne pas. En d'autres termes, vous n'arrivez pas

ATTENTION aux rançongiciels

Comment éviter le téléchargement de rançongiciels

Installez des logiciels de protection antivirus et anti-maliciels sur votre réseau, et gardez ces logiciels à jour. Prenez le temps d'installer la plus récente version de vos systèmes d'exploitation et de vos applications. Sauvegardez fréquemment vos fichiers sur des systèmes de stockage externes, comme un disque dur externe ou une plateforme infonuagique, qui ne sont pas reliés à votre ordinateur.

S'ils le sont, vos données ainsi sauvegardées pourraient être verrouillées également.

Faites preuve de prudence! Ne cliquez pas sur des liens ni n'ouvrez des pièces jointes provenant d'adresses inconnues et désactivez les macros – vous pourriez par inadvertance télécharger des maliciels en activant des macros, et en cliquant sur une pièce jointe, un lien ou une fenêtre contextuelle en ligne.

Que faire si vous en êtes victime?

Il serait bien difficile de déverrouiller vos fichiers et de supprimer le rançongiciel de votre système informatique. Si votre entreprise est victime d'un rançongiciel, envisagez les actions suivantes :

Ne payez pas la rançon.
Sinon, vous ouvrez la voie à des attaques additionnelles. Les criminels profiteront de votre acceptation de payer la rançon afin de demander plus d'argent.

Déconnectez tous vos appareils.
Les rançongiciels peuvent se propager entre appareils et réseaux.

Consultez votre fournisseur de logiciel antivirus.
Si vous vous connaissez en récupération de données, vous pourrez essayer de supprimer les logiciels malveillants vous-même. Certains fournisseurs peuvent déceler ce maliciel et offrir des instructions et des logiciels pour remédier au problème.

Consultez un spécialiste de la sécurité informatique.
Un professionnel peut être en mesure de vous aider à supprimer le rançongiciel et à restaurer vos fichiers si vous les avez sauvegardés.

Changez vos mots de passe.

Choisir un mot de passe complexe et distinct pour chacun de vos importants comptes en ligne, comme le courriel et les services bancaires, est essentiel puisqu'une fuite de données pourrait mettre un mot de passe entre les mains de criminels qui l'essaieront pour accéder à d'autres comptes qui vous appartiennent.

Importance des mots de passe distincts

Des criminels utilisent la technique de tentatives d'infiltration simultanées, ou bourrage d'identifiants, où ils téléchargeront ces données dans un programme informatique pour tenter de se connecter simultanément à de nombreux autres sites, dont votre compte en banque. Et si vous utilisez les mêmes coordonnées de connexion pour plusieurs sites Web, le risque que les criminels puissent accéder à vos comptes sur ces sites sera grand.

Votre institution financière pourrait avoir ses propres exigences pour les mots de passe sécurisés. Voici quand même un moyen facile de choisir i qua12 8o2 (ec)Tj0tiffi-5 ( )]TJdev pu (oen)30 -1.2 Td[e)-1.maisd mi7ir ses me les mutilicilsouveni (oen9(-1.f-0n[, o5098 509.67(85[C)-91 t)0.

Protection contre l’exploitation financière

Exploitation financière (Suite)

Comment prévenir de tels abus?

- Si vous êtes capable de le faire, occupez-vous vous-même de vos transactions financières. À cette fin, profitez des services bancaires par téléphone ou en ligne.
- Au moment de planifier le cours des choses en cas d'incapacité à gérer vous-même vos finances, permettre à une personne (ou à des personnes) de confiance de vous aider serait une bonne idée. Mais usez de prudence dans le choix de la personne en question.
- Une procuration, un compte conjoint ou d'autres arrangements similaires peuvent être utiles. Toutefois, prenez en considération le fait qu'une procuration est généralement plus sûre – la personne désignée devra agir et prendre des décisions dans votre intérêt – qu'un compte conjoint – la personne désignée sera copropriétaire de votre argent et de vos investissements. Vous trouverez les détails au sujet de ces outils sur le site Web de l'ABC, à https://cba.ca/?tag=exploitation-financiere&l=fr.
- Vous pouvez dire « non » quand une personne tente de vous soutirer de l'argent ou de vous inciter à effectuer un achat – même un membre de votre famille.
- Assurez-vous de bien comprendre tous les documents que vous signez – ne signez jamais un document vide et ne donnez à personne votre carte de banque ou votre NIP.
- Demandez que vos chèques de pension, ou autres revenus, soient déposés directement dans votre compte bancaire et que les factures soient payées par retrait direct de votre compte ou portées automatiquement sur votre carte de crédit.

Rappelez vous que l'exploitation financière constitue une violation de vos droits. Vous n'en êtes pas responsable et vous pouvez obtenir de l'aide. Vous pouvez consulter la liste de ressources par province sur le site Web de l'ABC, à https://cba.ca/where-to-go-for-help?l=fr.

Veuillez solliciter un avis juridique sur toutes les questions relatives aux procurations et au mandat en cas d'inaptitude. Le présent texte donne uniquement de l'information générale et ne constitue pas un avis juridique. Les règles en matière de procuration variant d'une province à l'autre, l'ABC vous encourage fortement à consulter un expert juridique avant de prendre toute décision à cet effet.

Ressources additionnelles

L'ABC offre aux aînés un séminaire gratuit sur la prévention de la fraude dans le cadre de son programme de littératie financière Votre Argent-Aînés.

Le programme gratuit Votre Argent-Aînés est composé de trois modules d'une heure qui s'adressent aux personnes âgées de 55 ans et plus. Ces séminaires non commerciaux sont présentés par des banquiers bénévoles à l'échelle du pays, et portent sur trois thèmes : gestion de l'argent, prévention de la fraude et exploitation financière

- **Prévention de la fraude** – Déceler les fraudes visant les aînés et s'en protéger.
- **Exploitation financière** – Ce que c'est et comment l'éviter, avec une attention particulière aux risques associés aux procurations et aux comptes conjoints.
- **Gestion de l'argent** – Comment se préparer financièrement à la retraite.

Réservez un séminaire sur la prévention de la fraude dès aujourd'hui!

Association des banquiers canadiens
Prévention de la fraude :
www.cba.ca/fraude

Association des banquiers canadiens
Bulletin gratuit *Conseils pour la protection contre la fraude* :
Inscription en ligne.

Gouvernement du Canada
Pensez Cybersécurité
www.pensezcybersecurite.gc.ca

Agence de la consommation en matière financière du Canada
www.canada.ca/fr/services/finance/fraude.html

Votre banque est également une bonne source de conseils et de renseignements sur la cybersécurité. Vérifiez auprès de votre institution financière ce qu'elle vous offre comme services, guides et conseils en matière de sécurité.