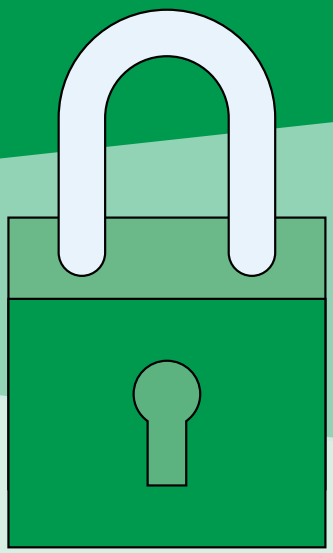
# Trousse de prévention de la fraude pour adultes plus âgés

**Protection contre la fraude et les escroqueries**



ASSOCIATION DES BANQUIERS CANADIENS

En partenariat avec

PENSEZCYBERSECURITE.CA

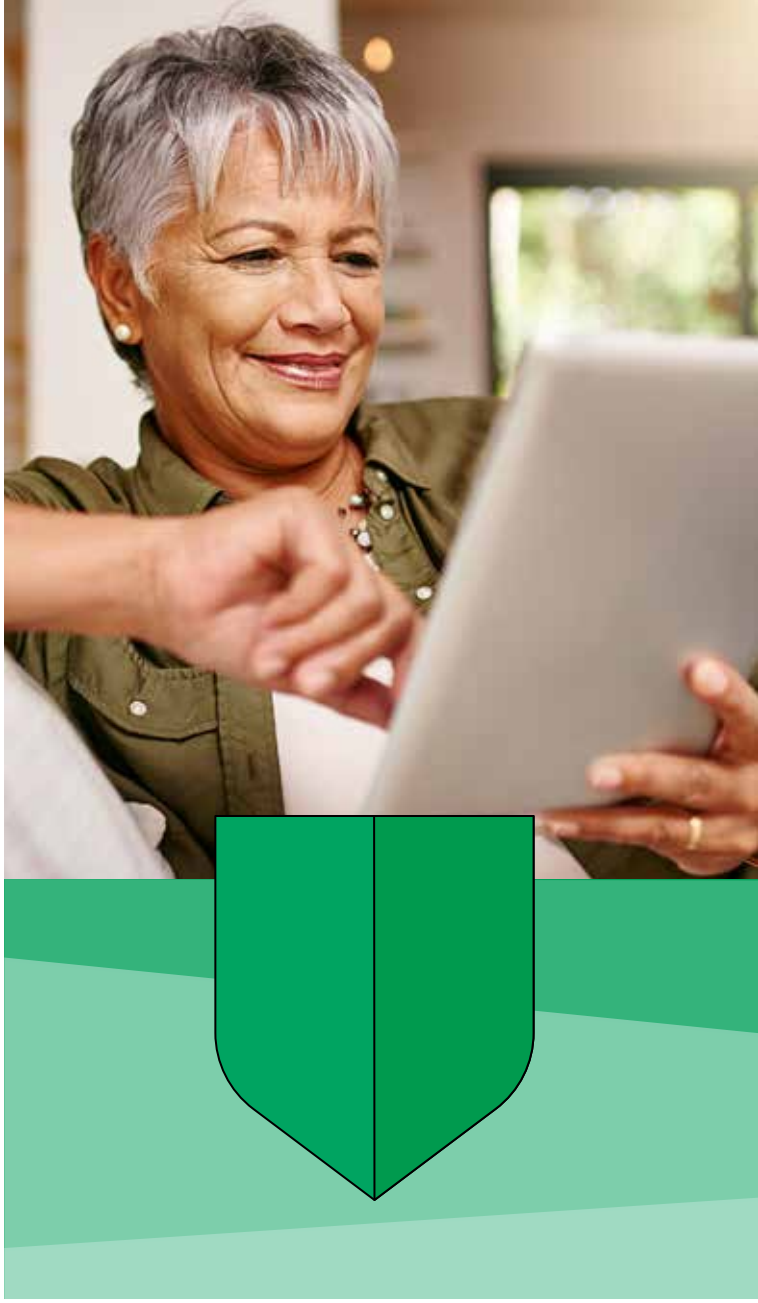
# L'Association des banquiers canadiens (ABC) a créé une trousse pour les aîné(e)s, destinée à les aider à déceler les arnaques et à adopter de façon proactive les mesures nécessaires pour protéger contre la fraude leurs renseignements personnels et financiers.

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

# 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.

# Liste de vérification pour prévention de la fraude (Suite)

## 5. Attention au téléphone

Ne donnez jamais des renseignements personnels au téléphone, à moins d'avoir initié l'appel vous-même. Raccrochez si vous recevez des appels de faux employés de banque ou de prétendus membres des forces de l'ordre qui vous prient de retirer de l'argent de votre compte bancaire afin de les aider dans une enquête. Ces appels constituent un premier pas dans le lancement d'arnaques connues. Également, restez sur vos gardes si vous recevez un appel d'un de vos petits-enfants vous priant de l'aider urgemment.

## 6. Signalement immédiat des pertes et des vols de cartes ou de documents personnels

Signalez immédiatement toute perte et tout vol de carte de débit ou de crédit, du permis de conduire, de la carte d'assurance sociale et de tout autre document qui sert à vous identifier. Dans le cas de la carte de crédit ou de débit, votre banque pourra la bloquer ou l'annuler afin que personne d'autre ne puisse l'utiliser. Également, prenez le temps de passer en revue vos relevés bancaires et de carte de crédit mensuels pour voir si des paiements ou des retraits que vous n'avez pas effectués y figurent.

## 7. Raffermissement des paramètres de sécurité et de confidentialité des réseaux sociaux

Vérifiez les paramètres de sécurité et de confidentialité sur tous vos comptes de réseautage social et renforcez les paramètres par défaut. Les sites Web des médias sociaux que vous utilisez affichent des détails supplémentaires au sujet des paramètres de sécurité et de confidentialité. Veillez à n'accepter que les demandes de personnes que vous connaissez et passez en revue vos contacts régulièrement pour en éliminer ceux qui ne sont plus pertinents.

## 8. Attention au téléchargement d'applications, de fichiers, de programmes et de logiciels gratuits, et importance de supprimer les applications non utilisées

Une logique malveillante, ou maliciel, comme un rançongiciel qui verrouille vos appareils et vos fichiers, un logiciel espion qui surveille secrètement vos activités en ligne, ou un espion de clavier qui enregistre secrètement les touches frappées sur votre clavier, peut s'infiltrer dans le téléchargement et servir à accéder à des renseignements personnels, comme vos mots de passe et vos renseignements financiers. Examinez votre appareil périodiquement et supprimez les applications que vous n'utilisez plus afin d'éviter les risques connexes.

## 9. Courriels, appels et textos douteux à ignorer

Ne donnez pas suite aux messages douteux. Jamais votre banque ne vous enverra un courriel vous demandant de révéler des renseignements personnels, comme votre numéro de carte de crédit, vos coordonnées d'accès en ligne ou le nom de jeune fille de votre mère. Également, ni par courriel, ni au téléphone, ni par message texte, jamais votre banque ne vous demandera le mot de passe à usage unique que vous recevez lors de votre connexion sécurisée à vos comptes.

## 10. Vigilance sur les applications de rencontre

Les fraudes sentimentales sont à la hausse. Surveillez ces signes qui montrent que votre nouvelle relation est une arnaque. Soyez vigilant et rappelez-vous de couper toute communication si votre nouvelle connaissance vous demande des renseignements sensibles ou de l'argent. Dans une fraude sentimentale, le criminel va donner l'impression d'être fiable et honnête pour arnaquer sa victime.

# Liste de vérification des mesures à adopter

- ☐ Protéger vos appareils
- ☐ Créer des mots et des phrases de passe distincts et complexes
- ☐ Déchiqueter les documents contenant des renseignements personnels et sensibles
- ☐ Limiter le partage en ligne de renseignements personnels et sensibles
- ☐ Rester vigilant au téléphone
- ☐ Signaler immédiatement la perte ou le vol de cartes de paiements et de pièces d'identité
- ☐ Resserrer les paramètres de sécurité et de confidentialité sur les réseaux sociaux
- ☐ Ne pas télécharger des applications, des fichiers, des programmes et des logiciels gratuits, et supprimer les applications non utilisées
- ☐ Ne pas répondre aux courriels, aux appels téléphoniques ou aux messages textes douteux
- ☐ Rester vigilant sur les applications de rencontre

# Défense contre les arnaques fréquentes

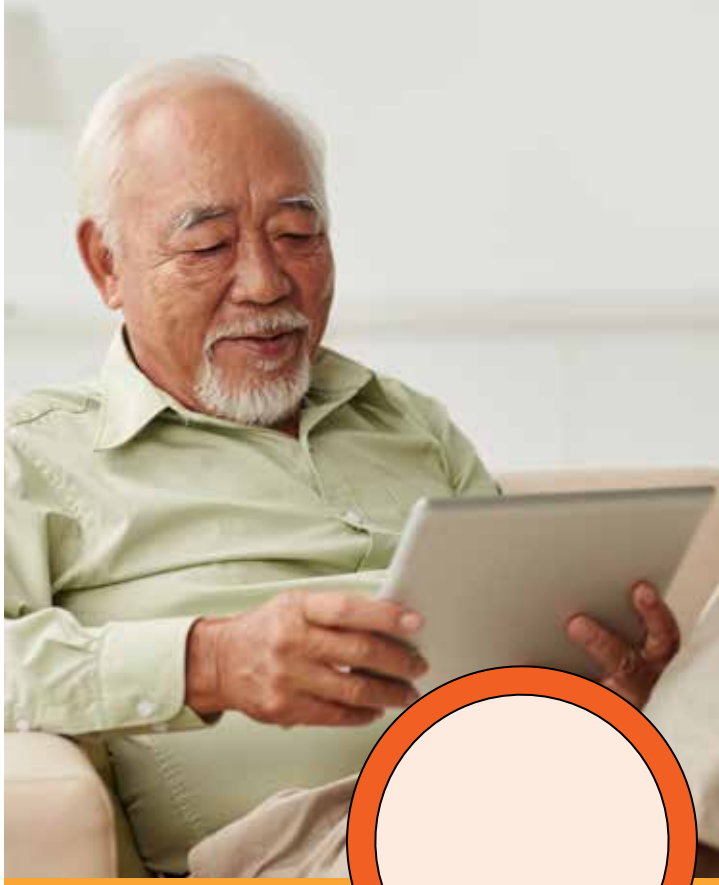
Quelques-unes des arnaques les plus répandues dont il faut se méfier :

- 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.

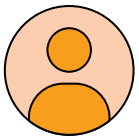
# ATTENTION à l'hameçonnage

Les tentatives d'hameçonnage existent depuis que le courriel existe. Ce qui a changé, c'est la nature plus raffinée de ces arnaques – les fautes linguistiques et grammaticales n'en sont plus le seul signe révélateur –, ce qui nécessite une vigilance soutenue.

## Signes que le courriel reçu est un hameçon

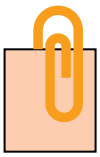
### Exigences et menaces

La demande de renseignements provient-elle d'une source légitime? Votre banque ne vous enverra jamais de courriel menaçant ni ne vous téléphonera pour exiger la divulgation de renseignements personnels, comme votre mot de passe, le numéro de votre carte de débit ou de crédit ou le nom de jeune fille de votre mère.



### Expéditeur douteux

Vérifiez l'adresse électronique de l'expéditeur. Le texte dans le champ de l'expéditeur peut sembler celui de l'organisation, mais l'adresse électronique qui y est rattachée ne l'est pas nécessairement. Pour vérifier, il suffit de placer votre curseur au-dessus du nom, sans cliquer.



### Pièces jointes et liens douteux

Les courriels hameçons contiennent souvent des liens qui ont l'air légitimes, mais conduisent plutôt à des sites frauduleux. Là également, il suffit de placer le curseur au-dessus du lien pour voir l'adresse du site vers lequel il mène. Par ailleurs, n'ouvrez jamais des pièces jointes auxquelles vous ne vous attendez pas.

### Avertissements

Avertissements que votre compte sera fermé ou l'accès à votre compte sera limité si vous ne répondez pas aux demandes dans le courriel.

# ATTENTION à l'hameçonnage vocal

La fraude téléphonique, ou hameçonnage vocal, peut prendre diverses formes qui ont en commun certaines tactiques.

## Fonctionnement de l'arnaque

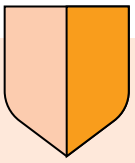
Vous recevez un appel d'un criminel qui se fait passer pour un représentant d'une agence gouvernementale ou des forces de l'ordre. Le message affirme que vous devez de l'argent, que vous avez une dette impayée ou que vous faites l'objet d'un mandat d'arrestation. Dans une variation sur ce même thème, le criminel peut se faire passer pour un employé de banque et vous demander de l'aider dans son enquête sur des activités frauduleuses détectées visant votre compte de banque ou votre carte de crédit.

**Les appels et les messages vocaux semblent authentiques. Or, ils comprennent toujours des indications flagrantes qu'il s'agit d'une arnaque.**

Très souvent, ces courriels ou messages vocaux utilisent un ton urgent et un langage menaçant afin de vous faire peur et vous forcer à payer la supposée dette ou de révéler vos coordonnées de connexion.

Les appels et les messages contiennent un avertissement que la police sera contactée si vous n'y donnez pas suite.

L'appelant exige que vous payiez la dette par carte-cadeau, bitcoin ou transfert bancaire.



## Protégez-vous!

Les banques suivent d'importantes mesures afin de protéger les renseignements personnels que vous leur confiez et pour vous aider à les protéger. Les banques et les agences gouvernementales n'exigeront jamais le paiement d'une dette ou d'une facture par carte-cadeau.

Si vous recevez un appel de la part d'un fraudeur, raccrochez ou effacez le message vocal.

Vous pouvez également faire bloquer le numéro de l'appel entrant et le signaler au Centre antifraude du Canada.

# ATTENTION à l'arnaque des grands-parents

Avez-vous déjà reçu un appel d'une personne qui se dit votre petit-fils (ou petite-fille) et vous annonce qu'il lui est arrivé un grand malheur – comme un accident de voiture – et qu'elle a besoin d'argent? Un appel du genre est vraisemblablement une indication que vous êtes visé par l'arnaque des grands-parents, une version de l'arnaque d'urgence. Ces arnaques sont courantes. Vous devez donc toujours évaluer la situation à fond avant d'agir.

## Fonctionnement de l'arnaque

La personne visée reçoit un coup de fil d'un individu qui lui dit : « Grand-maman, m'as-tu reconnu(e)? » Croyant qu'il s'agit de l'un de ses petits-enfants, la future victime répond « Oui, oui, c'est (donne le prénom) ».

Il va demander à ce que son grand-parent lui fasse parvenir immédiatement de l'argent, car il a eu un accident de voiture ou il se trouve en prison dans une autre ville ou un autre pays. Parfois, l'arnaqueur peut avoir un partenaire qui va prétendre être un policier, une personne qui a payé la caution ou un avocat.

La victime va alors retirer de l'argent de son compte et le transférer à son « petit-fils » ou sa « petite fille ». Il se peut aussi que le criminel envoie un coursier chez la victime pour collecter l'argent.

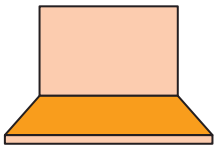
**Si vous avez été victime d'une arnaque de ce genre, appelez votre service de police. Le personnel des banques est au courant de telles arnaques et les employés ont reçu une formation leur permettant de remarquer toute transaction inhabituelle effectuée par un client – par exemple, le retrait d'une somme plus importante que d'habitude.**

## Protégez-vous

- N'offrez jamais de l'information à votre interlocuteur. S'il vous demande « M'as-tu reconnu(e)? », dites simplement « non » et demandez-lui son identité.
- Demandez des détails à votre interlocuteur. Si la personne vous explique une situation, demandez-lui des détails sur l'endroit exact où elle se trouve et demandez-lui de répéter l'histoire. Un criminel se rappelle difficilement des détails qu'il a inventés sur le champ.
- Posez à votre interlocuteur quelques questions personnelles auxquelles seuls vos vrais petits-enfants sauront répondre.
- Après que vous aurez raccroché, vérifiez l'histoire en appelant les parents ou d'autres membres de la famille du présumé « petit-fils ».
- Ne faites jamais un virement d'argent électronique (p. ex, par Interac) peu importe les circonstances. Il est pratiquement impossible de recouvrer ou de trouver l'argent ainsi transféré.
- Ne fournissez jamais votre numéro de carte de crédit par téléphone ou sur Internet à moins d'être certain(e) du destinataire.

# ATTENTION à l'arnaque du soutien technique

Cette arnaque assez fréquente met en scène un escroc qui se fait passer pour un représentant d'une entreprise de soutien technique et essaie de vous convaincre de vous abonner à un service inutile et coûteux ou de lui donner accès à votre ordinateur et à vos renseignements personnels.

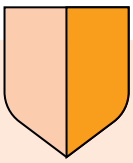


## Fonctionnement de l'arnaque

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.



## Moyens de vous protéger

- Méfiez-vous des appels sans préavis. Les entreprises informatiques respectables ne font pas d'appels téléphoniques non sollicités.
- N'appelez pas un numéro ni ne cliquez sur un lien qui sont présentés sous des formes suspectes.
- Déclenchez le logiciel antivirus afin de trouver et de surveiller les vulnérabilités sur votre appareil.
- Ne vous connectez jamais à vos comptes au moyen d'un WiFi public ou non sécurisé, ou si vous partagez votre écran avec une autre personne.
- Gardez vos logiciels à jour. Ainsi, vos appareils seront protégés des menaces les plus récentes.
- Si vous avez besoin d'une aide technique ou de renseignements spécifiques, communiquez avec des entreprises fiables et confirmées (comme le fabriquant de votre appareil).

# 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.

**Si vous croyez être victime d'une fraude sentimentale, ou de tout autre type de fraude, il est important de communiquer immédiatement avec la police.**

## Protégez-vous

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.

- Votre interlocuteur ne perd pas son temps. Les escrocs veulent développer une relation rapidement. Ne vous laissez pas prendre.
- Votre interlocuteur vous demande de lui envoyer de l'argent. Dans ce cas, mettez fin à vos communications.
- Si la personne a un profil public, vérifiez les incohérences entre ce qu'elle affiche et ce qu'elle vous dit.
- Vérifiez son existence sur d'autres plateformes. D'habitude, les escrocs se limitent à un média et si jamais ils en ont plus, leurs comptes renfermeront peu d'informations pour éviter de se faire prendre.
- Si vous recevez un message de votre flamme avec un prénom qui n'est pas le vôtre, pensez-y bien. Les escrocs – qui ne perdent pas de temps, rappelez-vous – travaillent sur plusieurs victimes à la fois.
- L'arnaqueur prétend être originaire de votre région, mais travaille actuellement à l'étranger. Il s'agit d'un des prétextes pour vous demander de l'argent plus tard. Restez sur vos gardes!
- Si votre interlocuteur vous demande de déposer un chèque et de lui en renvoyer une partie, ne le faites pas! Il s'agit, en plus, de l'arnaque de paiement en trop.

# 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.

**Conseils pour reconnaître les applications et les sites Web frauduleux**

## 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 à quitter une page ou à retourner à la page précédente.
- On vous demande des informations sur votre carte de crédit à un moment où vous n'achetez rien.

Les principales plateformes d'achat d'applications mobiles, comme le App Store d'Apple ou le Play Store de Google, surveillent le contenu versé dans leur plateforme et suppriment régulièrement les applis malveillantes. Vous devez quand même faire attention à ce que vous téléchargez.

## Protégez-vous

- Magasinez auprès de détaillants connus et fiables qui ont une adresse postale avec numéro de rue et un numéro de téléphone opérationnel.
- Téléchargez l'application mobile de votre détaillant à partir de son site Web au lieu de la chercher uniquement sur la plateforme des applis mobiles.
- Assurez-vous que l'adresse électronique du site commence par « https » et qu'une icône de cadenas est affichée sur la barre d'adresse. L'adresse qui commence par « https » au lieu de « http » (s pour sécurisé) signifie que le site est sécurisé au moyen d'un certificat SSL.
- Ne répondez jamais aux messages contextuels qui apparaissent sur les sites ou les applications et vous demandent vos renseignements financiers.
- Utilisez votre carte de crédit et évitez les sites et les applis qui demandent d'autres modes de paiement : transfert, carte de paiement prépayée, argent liquide ou paiement par un tiers prestataire.

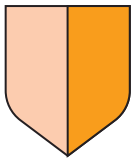
## Applications mobiles

- Le nom du diffuseur (habituellement affiché sous le nom de l'appli) d'une fausse application ressemblerait au nom d'un diffuseur légitime, mais il y a toujours des différences.
- La description de l'appli est mal rédigée ou n'affiche aucun commentaire.
- Il faut un nombre d'autorisations excessif pour l'installation.
- L'application produit beaucoup de fenêtres de publicité ou de demandes de saisie de renseignements personnels.

# ATTENTION aux rançongiciels

## Un rançongiciel est un logiciel malveillant, ou maliciel.

Une fois que le maliciel est installé sur votre ordinateur, rien n'arrivera jusqu'à ce que des pirates informatiques s'en emparent et cryptent vos fichiers. Lorsque les fichiers sont cryptés (verrouillés), les fraudeurs exigeront le paiement d'une rançon pour les décrypter et les déverrouiller. Ne payez pas la rançon. Les menaces visent à vous effrayer et à vous intimider. Payer la rançon ne garantit pas le déverrouillage de ces fichiers ni l'arrêt de la vente des données ou de leur publication en ligne.



### 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.**
Changez tous vos mots de passe en ligne. Ainsi, les criminels ne pourront pas accéder à vos comptes s'ils arrivent à récupérer vos mots de passe.

**Signalez la fraude.**
Informez-en le service de police local et le Centre antifraude du Canada.

# Choix de mots de passe complexes

ASSOCIATION DES BANQUIERS CANADIENS

**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 un mot de passe difficile à deviner, mais qui est assez facile pour vous en souvenir.

## Utilisez une phrase de passe plutôt qu'un mot de passe

Même si la phrases de passe est plus longue que le mot de passe, il est plus facile de s'en souvenir. Que ce soit une phrase (sans espaces) ou un mot de passe complexe, utilisez des idées qui ont rapport avec le site.

Par exemple, pour vous connecter à votre compte sur un site de partage de photos, vous pouvez recourir à la sagesse populaire.

**Dicton :**
**Qui n'a point d'amis ne vit qu'à demi**

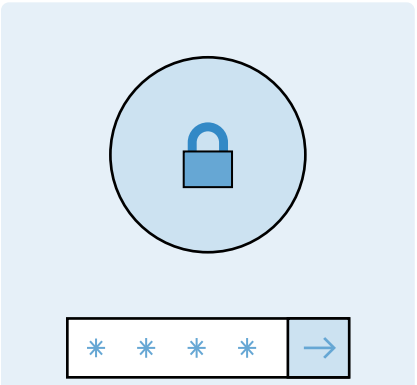
Et vous pourrez jouer avec ces mots pour les faire correspondre aux exigences de sécurité du site : nombre de caractères, caractères alphanumériques, caractères spéciaux, majuscules, etc.

**Étape 1 :** Choisissez la phrase.

qui n'a point d'amis ne vit qu'à demi

**Étape 2 :** Utilisez la première lettre de chaque mot.

qnapdanvqd



**Étape 3 :** Ajoutez des majuscules..

QnapdanvqD

**Étape 4 :** Ajoutez des chiffres et des caractères spéciaux, modifiez selon ce qui rendra l'expression plus facile à mémoriser, du moment que le mot de passe est d'au moins 8 caractères et ne dépasse pas la limite spécifiée.

KiNaPAmVi1/2!

### Mesures additionnelles pour vous protéger

Un mot de passe solide n'est qu'une première ligne de défense pour vos renseignements personnels importants. Servez-vous donc de l'authentification multifactorielle (sécurité à deux étapes) pour vos comptes en ligne, lorsqu'elle est offerte. Également, installez sur votre ordinateur le système d'exploitation le plus récent, ainsi que les nouveaux logiciels de sécurité, et gardez le tout à jour.

# Protection contre l'exploitation financière

## Ce qu'il faut savoir et où obtenir de l'aide

L'exploitation financière survient lorsqu'une personne que vous connaissez essaie de s'accaparer ou de prendre le contrôle de ce qui vous appartient à son avantage et non au vôtre, qu'il s'agisse de votre argent, de vos biens ou de vos renseignements personnels. L'exploitation financière est immorale et, dans bien des cas, illégale.

### Les exploiteurs financiers – qui sont-ils?

Il peut s'agir d'une personne de confiance dans votre vie : un conjoint, un enfant ou un petit-enfant adulte, ou encore un autre membre de votre famille, un aidant naturel, un ami ou un voisin.

### Exemples d'exploitation financière

Il se peut qu'une personne à qui vous faites confiance vous exploite si elle :

- exerce des pressions sur vous pour que vous lui donniez ou prêtiez de l'argent ou pour avoir accès à votre information financière;
- utilise une procuration à son propre avantage;
- vous force à signer un document, notamment un contrat, un testament, une lettre ou une garantie, ou y parvient par la ruse;
- vous prend des biens ou de l'argent sans votre permission;
- fait un mauvais usage de votre carte de débit ou de crédit, ou vous demande de contracter un prêt pour l'aider;
- fait un mauvais usage des comptes bancaires conjoints ou exerce des pressions pour que vous transfériez votre compte actuel en compte conjoint;
- forge votre signature sur des chèques, y compris les chèques de pension, ou sur des documents légaux;
- vend ou transfère vos biens contre votre volonté ou vos intérêts; ou
- refuse de vous remettre l'argent ou les biens qu'elle a empruntés.

### Quelques signes d'alarme

- Une personne de confiance s'intéresse grandement à vos finances et s'en mêle.
- Vos relevés financiers montrent des retraits ou des transferts que vous n'avez pas faits.
- Une personne de confiance demande à ce que vos relevés bancaires lui soient envoyés (ou à ce que vous n'en receviez plus).
- Vous commencez à éprouver des difficultés à vous acquitter de vos obligations financières, ce qui ne vous est jamais arrivé.
- Une personne de confiance vous suggère d'effectuer des changements à des documents importants – p. ex., votre testament, vos procurations, vos fiducies, vos titres de propriété, vos actes ou vos prêts hypothécaires – sans que ce soit dans votre intérêt supérieur.
- Vous sentez une menace ou de la pression de la part d'une personne de confiance.

# 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

VOTRE ARGENT AÎNÉS

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

L'Association des banquiers canadiens est la voix de plus de 60 banques canadiennes et étrangères qui contribuent à l'essor et à la prospérité économiques du pays. L'ABC préconise l'adoption de politiques publiques favorisant le maintien d'un système bancaire solide et dynamique, capable d'aider les Canadiens à atteindre leurs objectifs financiers.
www.cba.ca

PENSEZCYBERSECURITE.CA

Pensez cybersécurité est une campagne nationale visant à informer les Canadiens sur les enjeux de la cybersécurité et à leur indiquer des façons simples de se protéger en ligne. Cette campagne est menée au nom du gouvernement du Canada par le Centre de la sécurité des télécommunications qui profite de l'expertise de son Centre canadien pour la cybersécurité.
Pensezcybersecurite.ca

**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.