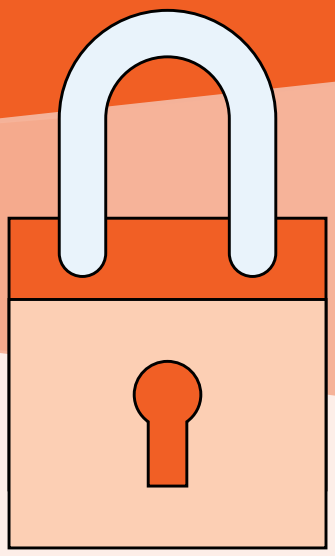
Trousse de cybersécurité pour nouveaux arrivants au Canada

Protection contre les cybermenaces



ASSOCIATION DES BANQUIERS CANADIENS

En partenariat avec

PENSEZCYBERSECURITE.CA

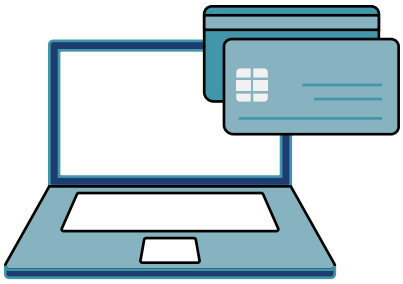
Grâce à cette trousse conçue par l'Association des banquiers canadiens et la campagne Pensez Cybersécurité, vous serez au courant des cybermenaces qui visent les nouveaux arrivants au Canada et développerez une routine de cyberhygiène afin de vous en protéger.

Nous sommes tous concernés. Les banques au Canada sont à l'avant-garde de la prévention et de la détection des cybermenaces. Elles collaborent avec les organismes de réglementation, les forces de l'ordre et tous les niveaux de gouvernement afin de protéger le système financier ainsi que leurs clients contre le cybercrime. Par ailleurs, vous pouvez prendre de simples mesures en vue de déceler les cybermenaces les plus en cours au Canada et de vous protéger de la fraude financière.

Contenu

Abécédaire de la cybersécurité pour nouveaux arrivants au Canada

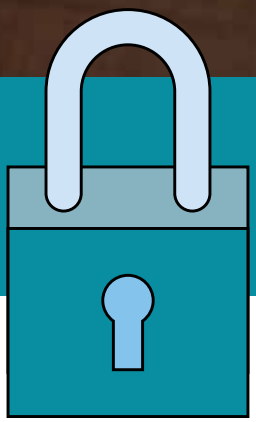
Internet a facilité de façon inédite les contacts avec la famille et les amis, ainsi que les activités commerciales et la gestion des finances, qui se font désormais plus rapidement, plus efficacement et plus confortablement.



Malheureusement, les criminels, eux aussi, utilisent Internet, mais pour tenter d'accéder à des renseignements personnels, comme les mots de passe, les détails sur les comptes bancaires et les cartes de crédit ainsi que les numéros d'assurance sociale, afin de commettre des activités frauduleuses.

Les nouveaux arrivants doivent rester bien vigilants, car ils sont particulièrement ciblés par les fraudeurs, vu qu'ils ne connaissent pas nécessairement les lois et les pratiques au Canada relativement aux escroqueries.

Notre monde devenant de plus en plus interconnecté, nos renseignements personnels sont davantage exposés au risque de se faire voler par des criminels, qui vont profiter du manque de solides mesures uniformes de cybersécurité. La bonne nouvelle est qu'il n'est pas nécessaire d'être un expert en informatique pour adopter des pratiques rigoureuses de cyberhygiène.



Qu'est-ce que la cybersécurité?

La cybersécurité est un ensemble de pratiques que vous adoptez afin de protéger vos renseignements personnels et financiers des cybercriminels qui essaieront de s'approprier les données exploitables et vous voler ainsi votre argent.

Liste de vérification de la cyberhygiène

Protéger les appareils et les données des cyberattaques

La cyberhygiène est l'ensemble des mesures importantes qu'il faut adopter en permanence afin de proactivement protéger contre les cyberattaques tous les appareils qui se connectent à Internet, comme les cellulaires, les ordinateurs portatifs, les ordinateurs de bureau et les appareils intelligents.

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 antiespions sur tous vos appareils connectés et mettez-les à jour régulièrement. Veillez à ce qu'un coupe-feu soit installé sur votre système d'exploitation ou téléchargez-en un afin de protéger vos appareils des intrusions malveillantes.

2. Mises à jour et correctifs

Installez toutes les versions mises à jour, aussitôt lancées, sur tous vos appareils connectés. Ne retardez pas l'installation des nouvelles versions, car elles contiennent d'importants correctifs de sécurité qui protègent les appareils contre les vulnérabilités connues.

3. 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, et déclenchez l'authentification multifactorielle. 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. 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'aurez également utilisé.

4. Sauvegardes périodiques des données

Sauvegardez fréquemment vos fichiers. Pour les fichiers très importants, envisagez une sauvegarde sur un support externe, un disque dur externe ou une clé USB. Vous protégerez ainsi vos données des cybermenaces, comme les rançongiciels (maliciels qui verrouillent vos appareils et vos fichiers contre une rançon). La sauvegarde de vos données vous redonne accès à vos informations importantes si votre appareil est compromis. Vous devez toujours tester vos sauvegardes pour vous assurer qu'elles fonctionnent.

5. Désactivation des réseaux de partage de fichiers

Les réseaux de partage de fichiers, appelés aussi « pair à pair », sont populaires parce qu'ils permettent aux utilisateurs de télécharger toutes sortes de fichiers et de programmes informatiques entre des réseaux mondiaux. Toutefois, l'utilisation de ces réseaux est considérée comme une activité à risque élevé. En effet, ces réseaux sont régulièrement utilisés par des criminels pour distribuer des fichiers répréhensibles ou illégaux, de même que des virus insérés dans des téléchargements qui semblent autrement inoffensifs.

Cyberhygiène
(Suite)

6. Attention au téléchargement d'applications, de fichiers, de programmes et de logiciels gratuits

Faites attention lorsque vous cliquez sur un lien ou téléchargez un fichier. Apprenez à reconnaître les tentatives d'hameçonnage et à éviter la mystification afin de pouvoir protéger vos appareils et vos données. Les maliciels (logiciels malveillants), comme les rançongiciels, les logiciels espions (qui épient vos activités en ligne) et les espions de clavier (qui épient ce que vous tapez sur votre clavier) peuvent être cachés dans le téléchargement et servir à accéder à des renseignements personnels, comme vos mots de passe et vos données financières.

7. Limite du partage en ligne de renseignements personnels importants

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. Attention aux renseignements saisis en ligne.

Ne fournissez donc jamais votre date de naissance, votre numéro d'assurance sociale ou tout autre renseignement personnel ou financier, car il s'agit de renseignements fréquemment utilisés pour l'accès aux comptes importants.

8. 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 changez les paramètres par défaut. Choisissez soigneusement qui peut accéder à vos réseaux sociaux ou les consulter, et limitez le type de renseignements que vous y affichez.

N'acceptez que les demandes provenant de personnes que vous connaissez, et passez en revue vos contacts régulièrement pour en éliminer ceux qui ne sont plus pertinents.

Votre liste de vérification de la cyberhygiène

- ☐ Installation de logiciels de protection
- ☐ Mises à jour et correctifs
- ☐ Mots et phrases de passe complexes et distincts
- ☐ Sauvegardes périodiques des données
- ☐ Désactivation des réseaux de partage de fichiers
- ☐ Attention au téléchargement d'applications, de fichiers, de programmes et de logiciels
- ☐ Limite du partage en ligne de renseignements personnels importants
- ☐ Raffermissement des paramètres de sécurité et de confidentialité des réseaux sociaux

Déceler les arnaques courantes

Voici une liste d'arnaques courantes que vous devez connaître :

- Hameçonnage et courriels frauduleux
- Code à usage unique
- Hameçonnage vocal
- Arnaque de la saison des impôts
- Offres d'emploi frauduleuses
- Applications et sites Web frauduleux
- Rançongiciels

De nombreuses escroqueries sont des variations d'un ensemble de techniques utilisées par les cybercriminels afin de vous amener à révéler vos renseignements personnels ou financiers.

INGÉNIERIE SOCIALE : comprendre comment les cybercriminels essaieront de vous duper

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 d'aider un ami dans le besoin) afin de nous leurrer dans la perspective de leur fournir des renseignements personnels qui seront utilisés aux fins de fraude financière. Les tactiques suivies essaient de nous amener à cliquer sur des liens ou des pièces jointes contenant des maliciels ou à fournir des renseignements personnels nécessaires à la perpétration de crimes financiers.

Lorsqu'il s'agit de cybersécurité, les systèmes de sécurité informatique les plus performants ne peuvent rien contre le fait que des utilisateurs dupés révèlent leurs coordonnées de connexion et autres renseignements personnels.

Trois façons de détecter les tactiques d'ingénierie sociale

01 Usage de la peur comme motivation. Les courriels, les appels et les textos menaçants ou intimidants sont des techniques d'ingénierie sociale utilisées afin de motiver le receveur à accéder aux demandes de renseignements personnels ou d'argent.

02 Courriels ou textes suspects. Ces messages, qui contiennent des demandes urgentes pour des renseignements personnels, sont une flagrante indication qu'on essaie de vous arnaquer.

03 Offres impossibles à croire ou comportant des demandes inhabituelles. Attention, si 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 offres gratuites en ligne comportent souvent une logique malveillante.

Hameçonnage et courriels frauduleux

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 un 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 appellera 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. Par ailleurs, les banques et le gouvernement au Canada jamais ne vous demanderont un paiement par carte cadeau ou carte prépayée, par cryptomonnaie ou par transfert de fonds.

Expéditeur douteux

Vérifiez l'adresse électronique de l'expéditeur. Si vous placez votre curseur au-dessus du nom sans cliquer, l'adresse électronique apparaîtra. Certaines tentatives d'hameçonnage utilisent des adresses électroniques qui peuvent sembler légitimes, mais ne le sont pas. La meilleure façon pour en avoir le cœur net est de voir si le nom de domaine du courriel correspond au nom de l'organisation d'où il est censé provenir.

Pièces jointes et liens douteux

Vous devez toujours vous méfier des pièces jointes et des liens auxquels vous ne vous attendez pas. Les courriels frauduleux contiennent souvent des liens intégrés qui semblent valides. Placer le curseur au-dessus du lien sans cliquer révélera une adresse électronique ou un nom suspect.

Avertissements

Ne donnez pas suite aux avertissements de fermeture de votre compte ou de la limitation de l'accès à votre compte si vous ne répondez pas au message. Il s'agit d'une arnaque par hameçonnage.

Des remerciements ou des messages de confirmation de commande non sollicités

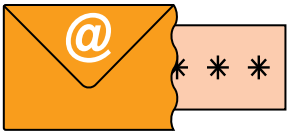
Vous pourrez recevoir un message vous remerciant pour un récent achat dont vous ne vous souvenez pas ou une confirmation d'une commande que vous n'avez pas faite. Il s'agit probablement d'une arnaque. Restez donc sur vos gardes.

Testez vos habiletés à reconnaître une arnaque avec les questionnaires de l'ABC : abccybersecurite.ca

Code à usage unique

L'arnaque du code à usage unique est de plus en plus utilisée par les escrocs pour tenter d'accéder à vos comptes.

Voici quelques conseils pour vous aider à éviter les arnaques axées sur le code à usage unique.



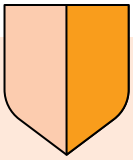
Fonctionnement de l'arnaque

Le processus d'authentification multifactorielle d'un grand nombre de sites Web nécessite un mot de passe à usage unique (OTP de son acronyme anglais), qui est en fait un code numérique à court temps d'expiration envoyé une fois, que vous pouvez recevoir soit par message texte soit par courriel. Cette étape est destinée à renforcer la sécurité, car sans ce code à usage unique il serait impossible à un fraudeur qui aurait volé votre mot de passe d'accéder à votre compte.

Or, les fraudeurs ont réussi à contourner cette protection. Désormais, ils se font passer pour une organisation réelle, comme le bureau de poste, votre banque ou toute autre société reconnue, et vous appellent pour demander le code à usage unique que vous venez de recevoir.

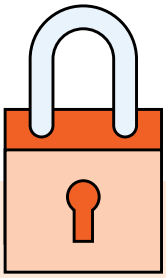
Si vous êtes victime de cette arnaque

Les banques ne ménagent aucun effort pour protéger les renseignements personnels qui leur sont confiés.Si vous être victime de l'arnaque du code à usage unique et que des escrocs sont en possession de vos renseignements personnels, contactez votre banque dans l'immédiat.



Protégez-vous

- Ne communiquez jamais votre code à quiconque, ni au téléphone ni par texte ni par courriel. Le code à usage unique que vous recevez vous est destiné exclusivement.



- Rappelez-vous que ni votre banque ni aucune autre organisation respectable ne vous demandera de leur communiquer votre code à usage unique au téléphone, par texte ou par courriel.

Hameçonnage vocal et par texte

La fraude téléphonique, ou hameçonnage vocal, et la fraude par message texte peuvent prendre diverses formes qui ont en commun certaines tactiques.

Exemple du fonctionnement de l'arnaque

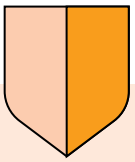
Vous recevez un appel ou un message texte de la part d'un criminel qui se fait passer pour un représentant d'une agence gouvernementale. Le message affirme que vous avez commis une erreur, comme omis de soumettre certains documents, et que vous devez agir rapidement pour éviter de perdre votre statut d'immigrant(e) ou de réfugié(e).

L'appel ou le message vocal ou texte semble authentique. Or, les indications flagrantes qu'il s'agit d'une arnaque ne manquent pas.

Très souvent, ces appels ou messages utilisent un ton urgent et un langage menaçant afin de vous faire peur et vous forcer à payer la supposée dette ou à révéler vos coordonnées de connexion. Une tactique utilisée par les cybercriminels à large échelle est de vous faire croire que vous devez de l'argent à la banque.

Les appels ou messages comportent des menaces de vous signaler à la police qui révoquera votre statut d'immigrant(e) ou de réfugié(e)s, si jamais vous n'y répondez

Votre correspondant exigera le paiement de votre dette par carte cadeau ou prépayée, par cryptomonnaie ou par transfert de fonds.



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.

Attention, Immigration, Réfugiés et Citoyenneté Canada n'usera jamais d'agressivité ni ne menacera de vous arrêter ou de vous déporter. De tels appels et messages sont toujours des arnaques.

Aussitôt que vous vous rendez compte que votre interlocuteur est un cybercriminel, raccrochez ou supprimez le message.

Également, vous pourrez bloquer le numéro et le signaler au service de police local et au Centre antifraude du Canada.

Conseils additionnels :

Protégez vos données des escrocs qui se font passer pour des représentants d'organismes gouvernementaux ou de la police : pensezcybersecurite.gc.ca/fr/blogues/protegez-vous-contre-escroqueries-usurpant-lidentite-dun-gouvernement-organismes-dapplication-loi

Arnaques axées sur les contribuables

Durant la saison des impôts, des fraudeurs usurpent l'identité d'employés de l'Agence du revenu du Canada (ARC) et vous leurrent ainsi avec des dettes factices pour vous soutirer de l'argent ou des renseignements personnels qu'ils pourront utiliser aux fins d'autres activités frauduleuses.

Fonctionnement de l'arnaque

Des fraudeurs pourront vous communiquer – par texte, courriel ou au téléphone – des messages convaincants ou menaçants, comme :

« Votre remboursement d'impôt est prêt. Cliquez ici pour le recevoir. »

« Vous devez de l'argent à l'ARC. Nous acheminerons bientôt votre dossier à une agence de recouvrement. Communiquez avec nous immédiatement. »

« Vous avez droit à un remboursement d'impôt de 750 $, cette année. Cliquez ici pour remplir le formulaire en ligne. »

Si vous êtes victime de cette arnaque

Si vous recevez un appel déclarant que vous devez de l'argent à l'ARC, communiquez directement avec Revenu Canada pour voir, ou consultez « Mon dossier » sur son site Web. Si vous croyez avoir donné accidentellement vos informations financières à des cybercriminels, communiquez sans tarder avec votre institution financière, l'ARC et le service de police local.

Ressources

Pour tous les renseignements sur les escroqueries en lien avec le gouvernement du Canada et pour savoir à quoi vous attendre quand le gouvernement communique avec vous, visitez canada.ca/fr/agence-revenu/campagnes/fraude-arnaques.html

Jamais l'ARC...

- ne vous enverra un courriel avec un lien vous demandant de révéler vos renseignements personnels ou financiers;
- ne vous enverra un courriel ou un texte avec un lien pour déposer votre remboursement;
- ne vous menacera de vous faire arrêter par la police ou déporter;
- ne vous demandera un paiement par transfert électronique, cryptomonnaie ou par carte cadeau ou carte de crédit prépayée;
- n'entamera, dans aucune circonstance, des discussions par texte ou par messagerie instantanée avec les contribuables au sujet de leurs impôts ou de leurs avantages fiscaux.

Offres d’emploi frauduleuses

Les cybercriminels exploitent les personnes impatientes de trouver un emploi en élargissant la portée de l’arnaque des fausses offres d’emploi ou en impliquant les personnes à la recherche d’emploi dans des activités de blanchiment d’argent. Voici les signes révélateurs les plus flagrants des offres d’emploi frauduleuses.

Fonctionnement de l’arnaque

Les escroqueries liées à l’emploi se décomposent en maintes variantes pouvant être repérées grâce à des signes communs, dont :

- La réception d’une offre d’emploi non sollicitée, qui parvient par courriel ou par message texte avec une promesse de revenu rapide.
- L’envoi par « l’employeur » d’un chèque, accompagné souvent d’un « contrat » factice et d’une demande d’encaisser le chèque et de remettre une portion des fonds à une tierce partie (individu ou entreprise). Il s’agit d’une version de l’arnaque de paiement en trop.
- Annonce en ligne d’un poste « d’agent financier » ou « d’agent de traitement des paiements ». Les tâches consistent à déposer les paiements provenant de clients de l’entreprise dans votre propre compte et à transférer ces fonds selon les directives de « l’employeur ». Les fonds seraient le produit d’activités criminelles et le fraudeur vous aurait engagé comme acteur innocent pour ses activités de blanchiment d’argent.

Protégez-vous

Vérifiez toujours la légitimité de l’entreprise qui offre l’emploi.

Confirmez que l’annonce est vraie en vérifiant que le poste se trouve bien sur le site officiel de l’entreprise et non seulement sur un site d’emplois, ou en communiquant avec l’entreprise à son numéro officiel et non au numéro figurant dans l’offre d’emploi.

N’acceptez jamais de déposer des fonds au nom d’un inconnu.

Ressources

Le Centre antifraude du Canada expose les formes les plus courantes de l’offre d’emploi frauduleuse sur son site Web.

Applications et sites Web frauduleux

Les cybercriminels créent des applications et des sites Web de magasinage frauduleux, qui ressemblent à s'y méprendre aux vrais.

Ces applications et sites Web sont une façade qui permet aux cybercriminels de voler vos renseignements personnels et les détails de votre carte de crédit.

Voici quelques astuces pour pouvoir les déceler.

Signes d'un site Web de magasinage frauduleux

- Le site Web est mal conçu, ne présente pas une image professionnelle et contient des hyperliens rompus.
- L'adresse du site contient des acronymes et des termes qui n'ont pas leur place sur ce site.
- Le site affiche un cadenas déverrouillé ou utilise le format http (et non https), ce qui signifie que le site est non chiffré et donc que vos renseignements ne sont pas sécurisés. Un cadenas verrouillé et le format https affichés au début de l'adresse électronique du site signifient que le site est crypté et que vos renseignements sont sécurisés.
- Impossible de trouver l'adresse ou le numéro de téléphone de l'entreprise.
- Les politiques de retour et de confidentialité sont difficiles à trouver ou à comprendre.
- Le bouton de retour est désactivé et vous ne pouvez pas quitter la page.
- Les formes de paiement demandées sont inusuelles, comme un transfert électronique.
- On vous demande de fournir des renseignements confidentiels, comme votre numéro d'assurance sociale.
- On vous demande les détails de votre carte de crédit à tout moment, pas seulement lors de l'étape de paiement, après avoir choisi vos produits.

Assurez-vous que l'adresse électronique du site commence par « https » et qu'une icône de cadenas verrouillé 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.

Les principales plateformes d'achat d'applications mobiles, comme l'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.

Signes d'une application frauduleuse

- Le nom du diffuseur de l'application (habituellement affiché sous le nom de l'application) ressemble au nom du diffuseur légitime, mais quelque chose cloche.
- 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.
- L'application utilise une quantité énorme de données ou utilise des données même quand elle est fermée.

Protégez-vous

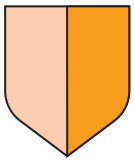
- Magasinez auprès de détaillants connus et fiables qui ont une adresse postale avec numéro de rue et un numéro de téléphone opérationnel.
- Assurez-vous de la légitimité de l'application sur le site du détaillant avant de la télécharger de l'App Store.
- Assurez-vous que l'adresse électronique du site commence par « https » et qu'une icône de cadenas verrouillé 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.

Rançongiciels

Un rançongiciel est un type de maliciel qui verrouille votre système et vos fichiers contre une rançon.

Un rançongiciel peut rester inactif sur votre appareil jusqu'à ce qu'un pirate informatique ne s'en empare et crypte vos fichiers (les verrouille). Des cybercriminels exigeront alors le paiement d'une rançon afin de décrypter et de déverrouiller le système et les fichiers.

Rappelez-vous, toutefois, qu'une fois la rançon payée rien ne garantit le déverrouillage des fichiers ni n'empêche la vente des données ou leur divulgation en ligne.



Comment éviter le téléchargement de rançongiciels

Installez des logiciels de protection antivirus et antimaliciels sur tous vos appareils, et gardez-les à jour.

Prenez le temps d'installer la plus récente version de vos systèmes d'exploitation et de vos applications.

Ajoutez une couche de sécurité en recourant à l'authentification multifactorielle pour tous vos systèmes et comptes.

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. Conservez vos données confidentielles sur une plateforme externe non connectée à Internet, comme une clé USB ou un disque dur externe portatif, car si jamais votre système est verrouillé, les appareils connectés le seront aussi.

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.

Si vous êtes victime de cette arnaque

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

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, le Centre antifraude du Canada et les institutions financières concernées.

Choisir un mot de passe complexe

CANADIAN BANKERS ASSOCIATION

Ajoutez une couche de sécurité en recourant à l'authentification multifactorielle pour tous vos systèmes et comptes

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 sur d'autres sites 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.

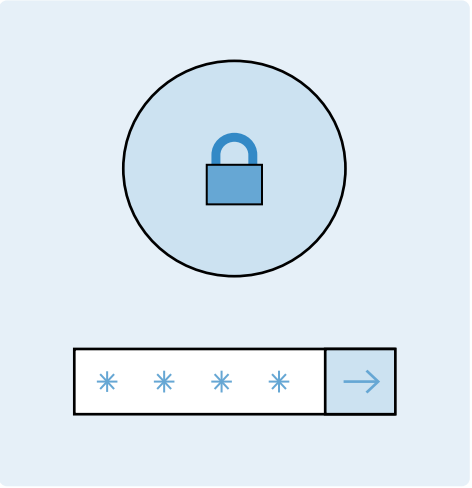
Votre institution financière pourrait avoir ses propres exigences pour les mots de passe sécurisés. Voici quand même un moyen facile de créer un mot de passe difficile à deviner, mais qui est assez facile pour vous en souvenir.

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

Vous vous souviendrez plus facilement d'une phrase de passe qui vous fait penser au site Web. 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.

Signaler la fraude

Ce n’est pas votre faute si vous tombez victime d’une arnaque. Toutefois, vous pouvez vous aider et aider autrui en agissant sans tarder.

Contactez votre institution financière

Si vous pensez avoir donné à un cybercriminel vos coordonnées de connexion à votre compte, les informations sur votre carte de crédit ou autres détails financiers, communiquez sans tarder avec votre banque au moyen du numéro de téléphone que vous savez être le bon (p. ex., le numéro figurant à l’endos de votre carte de débit ou de crédit).

Contactez la police

Déclarez au service de police de votre quartier tout incident de fraude. Les agents seraient en mesure de vous aider et d’épargner le même sort à d’autres personnes.

Signalez l’incident

Vous pouvez signaler tout acte de fraude et tout genre d’arnaque au Centre antifraude du Canada au numéro sans frais 1-888-495-8501, ou en ligne.

Si vous recevez un courriel frauduleux, vous devrez le signaler et le supprimer. Le signalement de tout courriel frauduleux à la banque ou à l’entreprise dont le nom est utilisé pour effectuer la fraude (mystification) contribue à protéger d’autres victimes potentielles. Pour signaler un courriel frauduleux, assurez-vous d’envoyer ledit courriel comme pièce jointe.

Ressources

Que vous soyez au Canada ou à l’extérieur du Canada, le gouvernement fédéral met des ressources à votre disposition afin de signaler la fraude en matière d’immigration et autres arnaques :

canada.ca/fr/immigration-refugies-citoyennete/services/proteger-fraude/signaler-fraude.htm

Ressources additionnelles

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

Questionnaires de sensibilisation à la cybersécurité :
abccybersecurite.ca

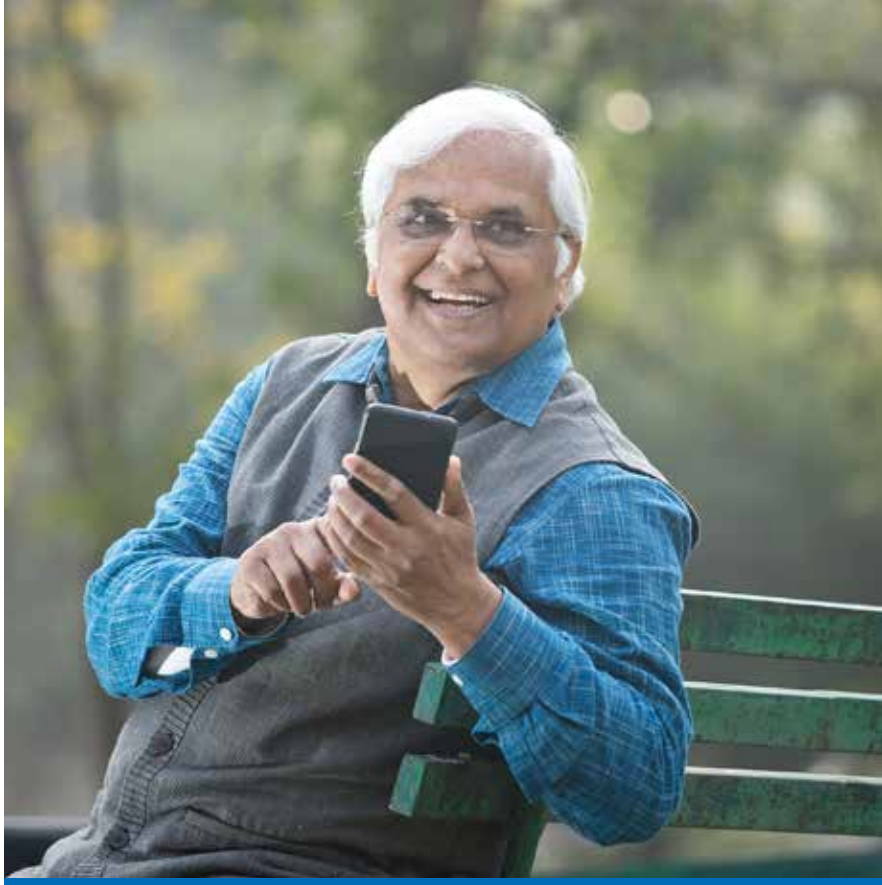
Bulletin gratuit *Conseils pour la protection contre la fraude* :
Inscription en ligne.

Gouvernement du Canada
Pensez Cybersécurité
pensezcybersecurite.gc.ca

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

Fraude et arnaque en matière d'immigration et de citoyenneté
canada.ca/fr/immigration-refugies-citoyennete/services/proteger-fraude.html

Votre banque est également une ressource inestimable lorsqu'il s'agit d'informations et de conseils pour la cybersécurité. Consultez votre institution financière pour connaître les services, les guides et les conseils de sécurité qu'elle vous offre à titre de client. L'ABC aussi offre davantage de renseignements et de ressources aux nouveaux arrivants au Canada sur son site Web cba.ca/newcomers-to-canada?l=fr



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 Canadiennes et Canadiens à atteindre leurs objectifs financiers. 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