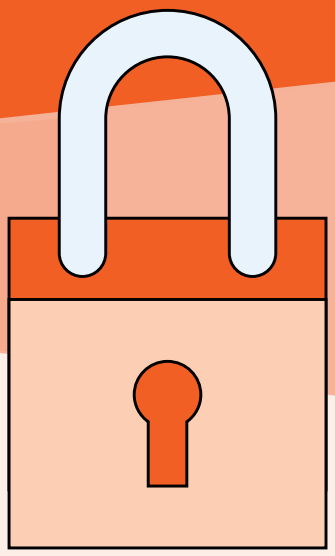
Trousse de prévention de la fraude pour nouveaux arrivants au Canada

Protection contre les cybermenaces



ASSOCIATION DES BANQUIERS CANADIENS

En partenariat avec

PENSEZCYBERSECURITE.CA

Version 2025

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.

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 les crimes financiers. Par ailleurs, vous pouvez prendre de simples mesures en vue de déceler les tentatives de fraude les plus en cours au Canada et de vous protéger de la fraude financière.

Contenu

01 Abécédaire de la cybersécurité

02 Liste de vérification de la cyberhygiène

03 Protection contre les fraudes courantes

- 03.1 Hameçonnage et courriels frauduleux
- 03.2 Code à usage unique
- 03.3 Fraude téléphonique
- 03.4 Fraudes axées sur les contribuables
- 03.5 Offres d'emploi frauduleuses
- 03.6 Fraude générée par l'IA
- 03.7 Applications et sites Web frauduleux
- 03.8 Rançongiciels

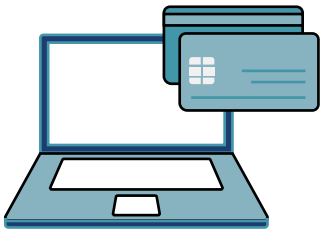
04 Choisir un mot de passe complexe

05 Signaler la fraude

06 Ressources additionnelles

Abécédaire de la cybersécurité pour nouveaux arrivants au Canada

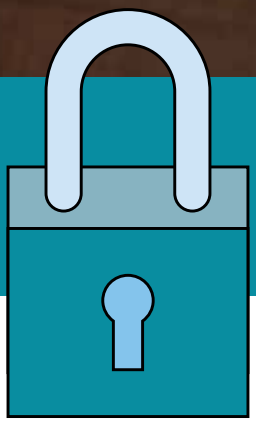
Internet a facilité de façon inédite les contacts avec la famille et les amis, ainsi que les activités commerciales et la gestion des finances, qui se font désormais plus rapidement, plus efficacement et plus confortablement.



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 contre les tentatives de fraude ses données personnelles, son argent et ses appareils connectés à Internet

Coup d'œil périodique pour veiller à ce que l'ensemble des mesures simples mais essentielles soient suivies en permanence afin de proactivement protéger vos renseignements financiers et personnels des tentatives de fraude.

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. Sécurité des comptes

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. De plus, vous devez déclencher l'authentification multifactorielle sur vos comptes en ligne lorsque possible.

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

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.

5. Attention particulière au téléphone

Également, restez sur vos gardes si vous recevez un appel ou un message vocal d'un supposé responsable du gouvernement qui vous annonce que vous avez commis une erreur, comme vous n'avez pas rempli tous les papiers nécessaires. Il vous incitera à agir immédiatement pour éviter la perte de votre statut d'immigrant(e) ou de réfugié(e). C'est probablement une fraude.

Cyberhygiène (Suite)

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

Signalez immédiatement, à votre banque, au poste de police du quartier ou au Centre antifraude du Canada, 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

Une logique malveillante, ou maliciel, comme un rançongiciel qui verrouille vos appareils et vos fichiers, un logiciel espion qui vous surveille secrètemen, 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 fréquemment 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.

Votre liste de vérification de la cyberhygiène

- [ ] 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 appelstéléphoniques ou aux messages textes douteux
- [ ] Rester vigilant sur les applications de rencontre

Protection contre les fraudes courantes

Voici une liste de tentatives de fraude courantes que vous devez connaître :

- Hameçonnage et courriels frauduleux
- Code à usage unique
- Hameçonnage vocal
- Fraude de la saison des impôts
- Offres d'emploi frauduleuses
- Fraude générée par l'IA
- 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 et des urgences comme motivation. Les courriels, les appels et les messages 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 messages suspects. Ces messages, qui contiennent des demandes urgentes pour des renseignements personnels, sont une flagrante indication qu'on essaie de vous amener à prendre rapidement une décision que vous regretterez.

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 de fraude sont désormais plus raffinées et 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.

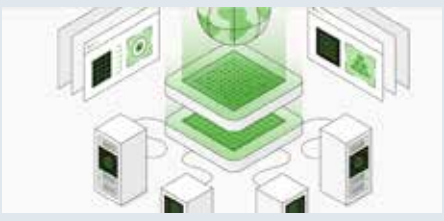
Avertissements

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 tentative d'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 activité frauduleuse. Restez donc sur vos gardes.

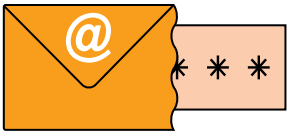
Testez vos habiletés à reconnaître une fraude avec les questionnaires interactifs de l'ABC :
cba.ca/consommateurs/questionnaires-anti-fraude



Code à usage unique

La fraude 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 fraudes axées sur le code à usage unique.



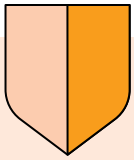
Fonctionnement de la fraude

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. 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.

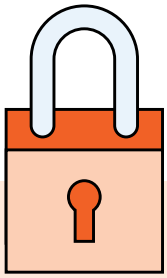
Si vous êtes victime de cette fraude

Les banques ne ménagent aucun effort pour protéger les renseignements personnels qui leur sont confiés.Si vous être victime de la fraude 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 lui communiquer votre code à usage unique.

Fraude téléphonique

La fraude téléphonique peut prendre diverses formes qui ont en commun certaines tactiques.

Exemple du fonctionnement de la fraude

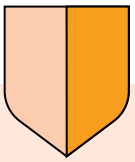
Vous recevez un appel ou un message texte de la part d'un criminel qui se fait passer pour un représentant d'une agence gouvernementale ou de la police. Le message affirme que vous avez commis une erreur, comme omis de soumettre certains documents, et que vous devez agir rapidement pour éviter de perdre 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 fraude 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 criminels 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 pas.

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 activités frauduleuses.

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

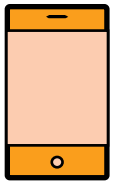
Également, vous pourrez bloquer le numéro et le signaler au service de police local et au Centre antifraude du Canada.

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

Fraudes 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 la fraude

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. »

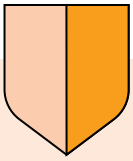
« Vous avez droit à un remboursement d'impôt de 750 $, cette année. Cliquez ici pour remplir le formulaire en ligne. »

Si vous croyez en être une cible ou une victime

Si vous recevez un appel ou un message déclarant que vous devez de l'argent à l'ARC, n'y donnez pas suite ni ne cliquez sur le lien fourni. 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 criminels exploitent les personnes impatientes de trouver un emploi en élargissant la portée 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 la fraude

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 la fraude 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 l’aider à cacher la source des fonds.

Protégez-vous

Vérifiez toujours la légitimité de l’entreprise qui offre l’emploi. Ne donnez aucun renseignement personnel avant d’avoir confirmé la légitimité de l’offre.

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.

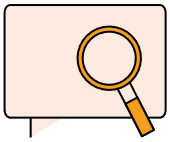
N’acceptez jamais de déposer des fonds au nom d’un inconnu.

Ressources

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

Fraudes générées par l'IA

Entre l'hameçonnage et le clonage vocal générés par l'IA, les escroqueries deviennent plus complexes... mais vos moyens de défense également! Voici des conseils pour reconnaître les tentatives de fraude et vous en protéger.



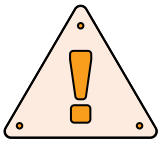
Hameçonnage généré par l'IA

- **Langage anormal ou excessivement aseptisé** – Les fraudes générées par l'IA peuvent utiliser des phrases ou un ton un peu trop astiqué. Attention aux messages qui vous semblent étranges.
- **Intelligence accrue de l'IA** – Les progrès technologiques permettent aux criminels de rendre leurs stratagèmes plus difficiles à détecter. Maintenir sa vigilance est essentiel!
- **Toute demande d'informations est suspecte** – Rappelez-vous que jamais votre banque ne vous enverra un courriel ni ne vous appellera pour vous demander des renseignements personnels, comme votre mot de passe ou le code à usage unique qui donnent accès à votre compte, votre numéro de carte de crédit ou le nom de jeune fille de votre mère.

Clonage vocal et vidéos frauduleuses générés par l'IA

Les criminels peuvent utiliser l'IA pour cloner des voix et des images afin d'usurper votre identité et demander de l'argent ou des renseignements confidentiels à vos proches. Ils peuvent aussi cloner la voix et l'image de vos proches pour vous faire croire qu'ils sont dans le besoin et vous soutirer de l'argent ou des informations.

- **Attention aux formes linguistiques anormales** – Le langage généré par l'IA peut paraître officiel et astiqué, avec de longues pauses entre les phrases ou dans les réponses. L'audio serait de mauvaise qualité et la voix aurait un ton robotisé.



Signaux et tactiques usuels

- **Usage de la peur comme motivation** – Courriels, appels ou textes menaçants, qui vous poussent à agir d'urgence.
- **Demandes urgentes de renseignements personnels** – Vérifiez bien les détails avant d'y donner suite.
- **Offres trop belles pour être vraies** – Évitez le partage de vos coordonnées de connexion ou le paiement de frais administratifs, même si l'offre est irrésistible. Les escrocs utilisent l'IA afin de créer des sites Web et des applications qui semblent vrais, mais qui sont destinés à voler vos données.

Dans le doute, consultez une personne en qui vous avez confiance ou un spécialiste.

Sécurité en ligne

- **Protégez vos appareils** – Ayez toujours la plus récente version du logiciel antivirus et du coupe-feu afin de bien vous protéger des maliciels.
- **Prenez le temps de réfléchir** – Grâce à l'IA, les escrocs sont en mesure d'élaborer des messages personnalisés qui ne laissent aucun doute quant à leur authenticité. Prenez le temps de bien vérifier tous les aspects de la demande avant d'agir.
- **Sollicitez un autre avis** – Dans le doute, avant de répondre, consultez un expert.
- **Signalez la fraude** – Si jamais vous soupçonnez une tentative de fraude, il est essentiel de faire un signalement sans tarder. Il s'agit d'une excellente façon de protéger tout le monde, autant vous que les autres. Les fraudeurs auront ainsi moins de victimes potentielles, donc moins de succès.

Applications et sites Web frauduleux

Les criminels 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 est différente du nom, ne serait-ce que par un caractère.
- 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, ou le numéro affiché n'est pas conforme à ce qui est publié par d'autres sources fiables.
- 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.
- 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.

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.

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.

Protégez-vous

- Magasinez auprès de détaillants connus et fiables qui ont une adresse postale avec numéro de rue et un numéro de téléphone opérationnel.
- Ne vous contentez pas de la chercher l'application d'un détaillant dans l'App Store. Téléchargez-la plutôt de son site Web pour garantir sa légitimité.
- 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.
- Utilisez votre carte de crédit, en évitant les applications et les sites Web qui demandent des paiements par transfert électronique, débit prépayé, cartes cadeaux, en espèces ou par une tierce partie.
- Évitez le magasinage et les activités bancaires en ligne quand votre connexion est sur un réseau public. Si vous devez effectuer de telles activités, utilisez un réseau privé virtuel.

Rançongiciels

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

Lorsqu'un rançongiciel prend le contrôle de votre appareil, votre accès à cet appareil, de même qu'à certains fichiers, sera complètement bloqué. Les cybercriminels exigeront alors le paiement d'une rançon afin de décrypter et de déverrouiller le système et les fichiers. N'en faîtes rien. Ces menaces sont destinées à vous faire peur.

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 déclenchez la mise à jour automatique.

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 fraude

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 :

Ne payez pas la rançon.
Payer la rançon vous exposera à de nouvelles attaques. Les criminels peuvent utiliser votre volonté de payer la rançon pour exiger plus d'argent.

Déconnectez tous les appareils.
Les rançongiciels se propagent à travers le réseau pour affecter tous les appareils qui y sont connectés. Afin d'éviter la propagation de rançongiciels dormants lorsque vous essayez de recouvrer les données ou de nettoyer, réinitialiser et mettre à jour les appareils, utilisez un réseau privé virtuel.

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

ASSOCIATION DES BANQUIERS CANADIENS

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.

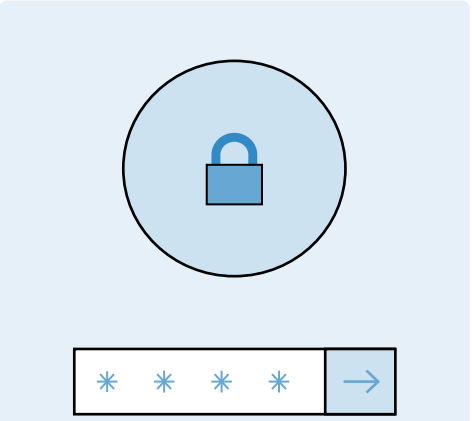
Votre institution financière pourrait avoir ses propres exigences pour les mots de passe sécurisés. Voici quand même un moyen facile de créer un mot de passe difficile à deviner, mais qui est assez facile pour vous en souvenir.

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 la phrase de passe est d'au moins 15 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

Si jamais vous croyez avoir été victime d'une tentative de fraude, vous devrez la signaler tout de suite. Ainsi, vous contribuerez à la protection de tout le monde, autant vous que les autres : les escrocs auront plus de difficultés à exécuter leurs activités frauduleuses.

Pourquoi signaler la fraude?

1. **Protéger autrui.** Lorsque vous signalez une activité frauduleuse, vous contribuez à attirer l'attention d'un plus grand nombre de personnes et donc à les protéger.
2. **Éliminer les escrocs.** Les forces de l'ordre et les agences de prévention de la fraude utilisent les signalements pour suivre et arrêter les escrocs. Plus elles disposent de données grâce aux signalements, plus elles sont efficaces.
3. **Protéger son argent.** Signaler la fraude aussitôt que possible aide à sécuriser les comptes et à réduire les risques de vol.

Quelques types d'activités frauduleuses fréquemment signalées

Hameçonnage par message texte

Vous recevez un message texte qui, souvent, semble parvenir d'une organisation connue, comme votre banque ou bien un organe fédéral ou provincial.

Hameçonnage par courriel

Dans ce type de fraude, les criminels essaient de vous faire croire que le message provient d'une personne ou organisation fiable afin que vous cliquiez sur le lien frauduleux qu'il contient ce qui leur facilitera la tâche de voler vos renseignements personnels ou financiers.

Appels frauduleux

Un escroc se fait passer pour un employé de votre banque, un fonctionnaire ou même l'un de vos proches dans le pétrin, avant de vous servir une raison fallacieuse pour vous demander d'envoyer de l'argent ou de révéler vos renseignements personnels.

Sites Web frauduleux

Ces sites ont l'air authentiques, mais ils sont plutôt des pièges destinés à voler vos données personnelles, les renseignements sur votre carte de crédit et votre argent.

Signaler la fraude (Suite)

Signaler une activité frauduleuse

1. Signalement au Centre antifraude du Canada (CAFC)
Le CAFC recueille les signalements de tous les types de fraude. Un signalement au CAFC contribue à protéger tout le monde, autant vous que les autres.

En ligne : Système de signalement de la fraude
Par téléphone: 1-888-495-8501

2. Signalement à votre banque
Si vous avez communiqué des renseignements personnels ou transmis de l'argent à la suite d'une fraude, contactez immédiatement votre banque ou le fournisseur de votre carte de crédit. Ces organisations peuvent contribuer à arrêter une transaction et à mettre votre compte à l'abri.

3. Signalement des pourriels
Vous pouvez signaler les pourriels facilement et gratuitement en les transférant par texto au 7726 (SPAM). Ainsi, vous contribuerez à l'identification de nouveaux types de pourriels et à l'amélioration des filtres utilisés par votre fournisseur de téléphonie mobile pour bloquer les pourriels nocifs. PensezCybersécurité présente des renseignements additionnels au sujet du signalement des pourriels par messages textes au 7726, ainsi que du signalement sur appareils Android et iOS.

4. Signalement des sites Web frauduleux au Bureau de la concurrence
Si vous tombez sur un site Web frauduleux, veuillez le signaler au Bureau de la concurrence, organisme chargé de contribuer à l'application de la loi en cas de pratiques malsaines sur le marché.

En ligne : Signalements des fraudes au Bureau de la concurrence

5. Signalement au service de police
Si la tentative de fraude s'est soldée par une grande perte financière ou par un vol d'identité, vous devrez signaler l'événement également au service de police de votre localité. La plupart des services de police acceptent les signalements de fraude non urgents, en ligne ou par téléphone.

À faire après le signalement

- **Conservez les documents** – Préservez toutes les communications en lien avec la fraude et documentez tous les signalements que vous faites.
- **Surveillez vos comptes** – Guettez toute activité anormale sur vos comptes bancaires, vos cartes de crédit et vos comptes en ligne.
- **Restez à jour** – Consultez le site Web du Centre antifraude du Canada pour les mises à jour régulières sur les activités frauduleuses en cours. Également, abonnez-vous au bulletin électronique gratuit *Conseils sur la prévention de la fraude* de l'Association des banquiers canadiens.

Le signalement des stratagèmes frauduleux est l'un des meilleurs moyens dont vous disposez pour vous protéger et protéger vos proches. Les quelques minutes que vous y investissez rapportent gros. En cas de doute quant à la présence d'une fraude, il est préférable de faire un signalement et de laisser les spécialistes en décider. Lorsque nous tous restons sur nos gardes et signalons les activités suspectes, les escrocs auront plus de difficultés à exécuter leurs activités frauduleuses.

Ressources additionnelles

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

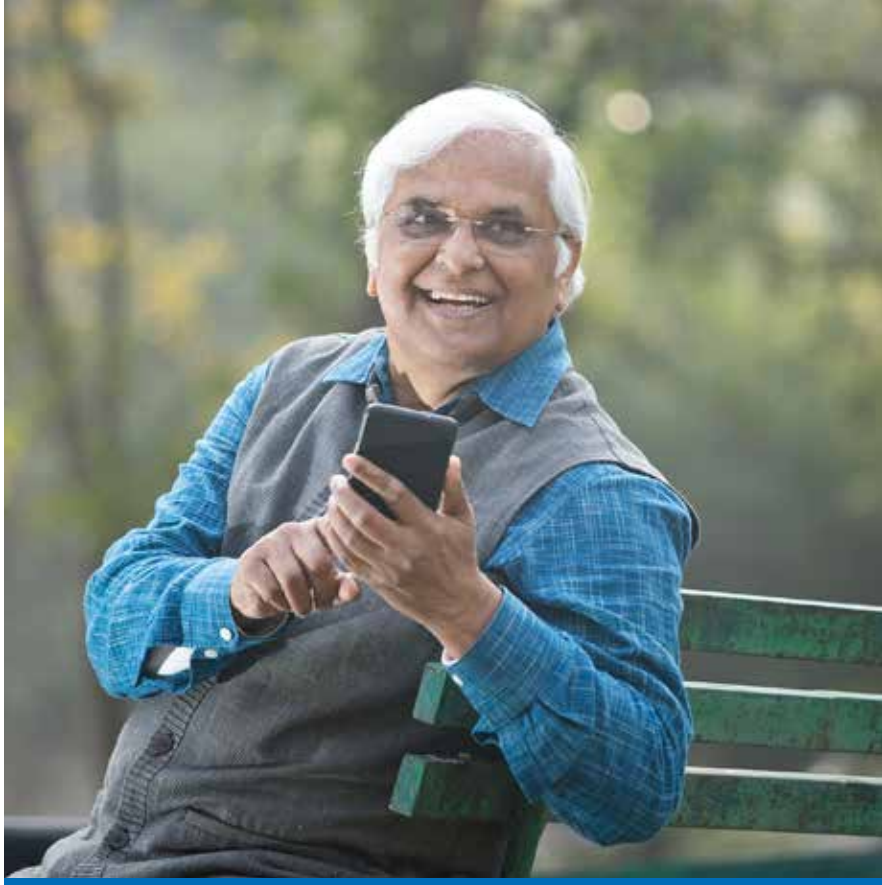
Bulletin gratuit *Conseils pour la protection contre la fraude*
Inscription en ligne.

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 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/article/services-bancaires-pour-nouveaux-arrivants-au-canada



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