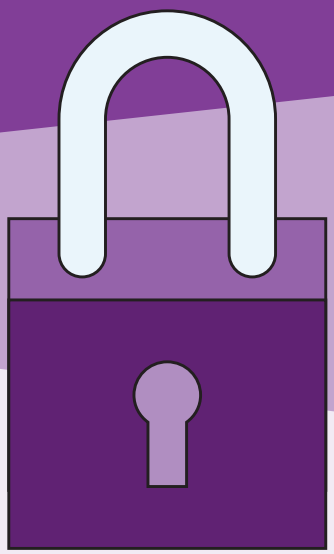
Prévention de la fraude pour les consommateurs

Protection contre les cybermenaces



ASSOCIATION DES BANQUIERS CANADIENS

En partenariat avec

PENSEZCYBERSECURITE.CA

Version 2026

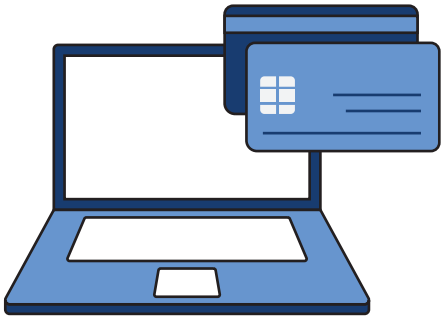
L’Association des banquiers canadiens et la campagne PensezCybersécurité ont conçu cette trousse afin de vous aider à comprendre les cybermenaces et l’importance d’adopter une habitude de cyberhygiène.

Les banques au Canada sont à l’avant-garde de la prévention et de la détection des cybermenaces, et 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. Il existe également des mesures simples que vous pouvez prendre afin de reconnaître les cybermenaces et de vous protéger ainsi que votre argent contre la fraude financière.

Contenu

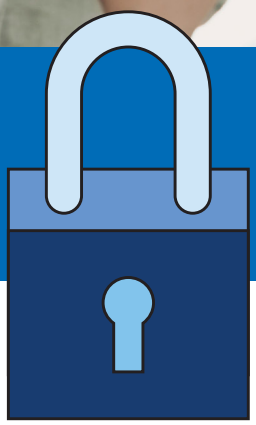
Abécédaire de la cybersécurité

La technologie facilite indéniablement la vie à tous les niveaux : relations avec les proches, exploitation d'une entreprise ou gestion des finances personnelles.



À mesure que notre vie transite en ligne, les cybercriminels trouvent les moyens de mettre la main sur 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, pour commettre des activités de fraude.

Or, les mesures de protection personnelle ne nécessitent pas des compétences informatiques poussées. Il suffit de suivre quelques simples conseils de cyberhygiène pour réduire les risques et garder en sécurité les renseignements personnels et financiers.



Qu'est-ce que la cybersécurité?

La cybersécurité est un ensemble de techniques, d'outils et de pratiques que vous adoptez afin de protéger vos données et vos renseignements personnels contre les cybercriminels qui essaieront de s'approprier les renseignements et données exploitables afin de vous voler 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 carte 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 secrètement, 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 pouvoir arnaquer sa victime.

Votre liste de vérification de la cyberhygiène

- ☐ Protéger les 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

Déceler les arnaques les plus fréquentes

- Fraude par courriel ou hameçonnage
- Fraude générée par l'intelligence artificielle
- Fraude du mot de passe à usage unique
- Fraude téléphonique ou vocale
- Fraude sentimentale
- Fraude des sites de vente en ligne
- Fraude des jeux en ligne
- 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.

Au lieu d'utiliser les techniques de piratage pour mener une cyberattaque, les criminels utilisent l'ingénierie sociale pour gaver les gens d'histoires dans l'espoir qu'ils passent pour crédibles.

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.

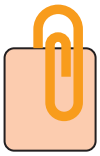
Protection contre l'hameçonnage

Les fautes linguistiques et grammaticales ne sont plus un signe révélateur de l'hameçonnage. La nature de plus en plus raffinée de cette fraude nécessite une vigilance soutenue.

Signes que le courriel reçu est un hameçon

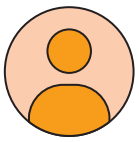
Exigences et menaces

La demande de renseignements provient-elle d'une source légitime? Votre banque ne vous enverra jamais de courriel menaçant ni ne vous téléphonera pour demander 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.



Pièces jointes et liens douteux

Les courriels hameçons contiennent souvent des liens qui ont l'air légitimes, mais conduisent plutôt à des sites frauduleux. Il suffit de placer le curseur au-dessus du lien pour voir l'adresse du site vers lequel il mène.



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.

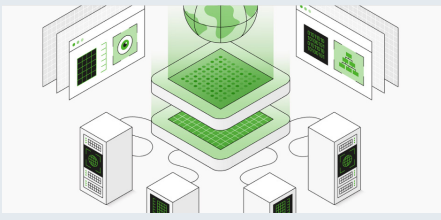
Avertissements

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

Messages de confirmation ou de remerciements non sollicités

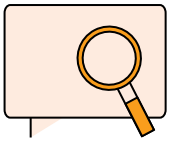
Des messages de remerciements pour un achat ou de confirmation d'une commande dont vous ne vous rappelez pas peut être une tentative de fraude. Y répondre pourra vous exposer à des risques. Si vous avez des doutes, vérifiez vos relevés ou contactez directement l'entreprise par des moyens autres que ceux qui sont proposés dans le message douteux. Restez toujours sur vos gardes!

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



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.



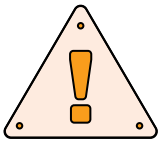
Hameçonnage généré par l'IA

- **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** – Evitez 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.

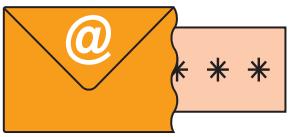
Sécurité en ligne

- **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.

Arnaque par mot de passe à usage unique

La fraude du mot de passe à usage unique est progressivement utilisée par les criminels pour accéder à vos comptes en ligne.

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



Fonctionnement de l'arnaque

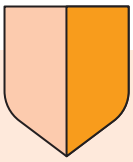
Un grand nombre de sites Web nécessite désormais qu'un mot de passe à usage unique (OTP de son acronyme anglais) vous soit envoyé.

Cette étape est destinée à raffermir 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, des fraudeurs peuvent vous appeler en se faisant passer pour une organisation réelle, comme le bureau de poste, la banque ou toute autre société connue, pour demander le code à usage unique que vous venez de recevoir.

Que faire si vous êtes victime de cette arnaque

Votre banque ne ménage aucun effort afin de protéger les renseignements personnels que vous lui confiez et de vous donner les outils pour faire de même. Si vous pensez avoir été victime d'une arnaque par mot de passe à usage unique où vous avez donné vos renseignements financiers à un fraudeur, communiquez immédiatement avec votre banque.



Conseils pour éviter cette arnaque

- Ne jamais donner votre code à usage unique à quiconque, encore moins à une personne qui vous appelle, vous texte ou vous écrit pour le demander. Le code à usage unique qui vous est envoyé est exclusivement pour votre usage personnel.
- La réception d'un code que vous n'avez jamais demandé peut s'avérer une tentative par un fraudeur d'accéder à vos comptes. Communiquez avec l'entreprise en question par des moyens autres que ceux qui sont proposés dans le message douteux pour signaler la fraude.
- Rappelez-vous que ni votre banque ni aucune autre organisation respectable ne vous demandera de lui communiquer votre code à usage unique par téléphone, par texte ou par courriel.

Protection contre l'hameçonnage vocal

Les tentatives de fraude téléphonique revêtent diverses formes qui ont en commun certaines tactiques.

Fonctionnement de l'arnaque

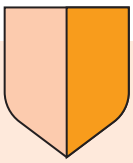
Vous recevez un appel d'un criminel qui se fait passer pour un représentant d'une agence gouvernementale ou des forces de l'ordre. Le message affirme que vous avez commis une infraction, avez un paiement en retard ou une dette impayée. Dans une variation sur ce même thème, le criminel peut se faire passer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

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

Ces courriels ou messages utilisent un ton agressif et un langage menaçant afin de vous faire peur et vous forcer à payer les frais frauduleux ou la supposée dette, ou à révéler vos coordonnées de connexion. Par ailleurs, le message peut sembler provenir d'un membre de la famille dans une situation difficile qui demande de l'argent, ou encore d'une source vous annonçant que vous avez gagné un lot ou une admission à un forfait spécial.

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.

Conseils supplémentaires
Protégez vos renseignements personnels contre la fraude par usurpation d'identité : pensezcybersecurite.gc.ca/fr/blogues/protegez-vous-contre-escroqueries-usurpant-lidentite-dun-gouvernement-organismes-dapplication-loi

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. Voici comment reconnaître cette fraude et l'éviter.

Fonctionnement de ce stratagème

Généralement, la victime et le criminel se rencontrent sur les réseaux sociaux ou sur une appli 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 assister la personne malade.

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 du fraudeur.

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. Soyez vigilant(e).
- Si la personne a un profil public, vérifiez les incohérences entre ce qu'elle affiche et ce qu'elle vous dit. Faites de même pour ses profils sur d'autres plateformes.
- 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.

Éviter l'arnaque des jeux en ligne

Les cybercriminels profitent de la popularité de ces sites, applications et jeux afin de créer des arnaques qu'un adulte peine à reconnaître et à éviter. Qu'en sera-t-il d'un enfant! En tant que parent, ou gardien, vous disposez de nombreuses mesures que vous pouvez adopter afin de limiter l'exposition d'un enfant aux fraudes et aux arnaques.

Ne jamais utiliser dans le profil des renseignements personnels permettant l'identification

Il ne faut jamais utiliser les vrais noms, adresses et numéros de téléphone pour établir le profil de jeu en ligne. Les renseignements dans un profil peuvent être accessibles au public. Mieux vaut utiliser des données ou des noms fictifs, ou éviter tout simplement de remplir ces informations lorsque possible.

Protéger les renseignements du compte

Toujours choisir un mot de passe distinct et complexe pour chacun de vos comptes. S'il y a lieu, déclenchez l'authentification bifactorielle afin de protéger vos comptes de l'accès non autorisé.

Attention aux sites Web et aux appels téléphoniques frauduleux

N'effectuer des achats que sur les plateformes de jeu officielles – De nombreux jeux sont vendus sous forme d'achat intégré en vue de perfectionner l'expérience. La grande popularité des jeux en ligne incite les cybercriminels à façonner des escroqueries autour de ces applications. Les sites Web frauduleux paraissent très professionnels, mais contiennent des maliciels ou offrent de l'argent de jeu en échange de renseignements personnels. Les enfants doivent éviter toute offre du genre, que ce soit sur les réseaux sociaux ou par clavardage.

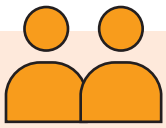
Ne jamais cliquer sur des liens suspects, même s'ils semblent provenir d'un « ami »

Les liens suspects, trouvés sur les sites Web, ou envoyés par texto, par clavardage sur les plateformes de jeu ou par courriel, peuvent télécharger des maliciels sur votre appareil, et voler ainsi vos coordonnées de connexion pour accéder à vos renseignements personnels et aux points de jeu que vous avez remportés, avant de les mettre en vente.

Ressources

Le site *Pensez cybersécurité*, du gouvernement canadien, décrit un nombre de ressources que les parents peuvent utiliser afin de protéger leurs enfants des cybermenaces.

La bande dessinée Branchés et futés : Internet et vie privée, du Commissariat à la protection de la vie privée du Canada, peut aider les enfants et les jeunes à mieux comprendre les questions de renseignements personnels pour en tenir compte en tout temps.



Parents et gardiens

Expliquer que les renseignements du compte sont personnels

Faites comprendre à votre enfant l'importance de ne jamais donner les coordonnées de son compte à quiconque, même pas à ses amis. Le compte de votre enfant peut contenir des renseignements personnels confidentiels comme le numéro de votre carte de crédit. Par ailleurs, les entreprises de jeu ne demanderont jamais des renseignements personnels du genre numéro du compte bancaire, mot de passe ou numéro d'assurance sociale. Une demande de renseignements personnels de cette sorte est une indication claire de fraude.

Se servir de la fonction du contrôle parental qui se trouve sur les appareils, les sites et les plateformes utilisés par les enfants

La plupart des appareils, des sites Web, des plateformes de jeu et des fournisseurs de service Internet ont prévu des outils pour que vous puissiez protéger vos enfants en ligne. Profitez des paramètres de sécurité afin de gérer l'accès en ligne de vos enfants, y compris les types de sites Web auxquels ils peuvent accéder, les personnes qui peuvent communiquer avec eux et les façons d'effectuer des achats.

Comment déceler les applications mobiles et les sites Web frauduleux

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 quelques conseils pour vous aider à reconnaître les sites Web frauduleux.

Les cybercriminels créent de faux sites et applications de magasinage qui ressemblent à s'y méprendre aux vrais dans l'objectif de voler les données financières et les renseignements personnels des consommateurs.

Quelques conseils pour vous aider à déceler ces applications et ces sites frauduleux.

Signes qu'un site Web est frauduleux

- Le site Web est mal conçu, ne présente pas une image professionnelle et contient des hyperliens rompus.
- Les rabais sont trop beaux pour être vrais, et les modes de paiement demandés sont inusuels : cryptomonnaie, transferts électroniques ou cartes-cadeaux.
- L'adresse électronique du site ne correspond pas à l'adresse officielle. Même une seule lettre ou un signe fait la différence.
- Vous ne parvenez pas à trouver l'adresse civique ou le numéro de téléphone de l'entreprise sur ce site.
- 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, ou on vous demande des renseignements qui ne sont pas nécessaires pour l'achat (comme votre numéro d'assurance sociale).

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.

Moyen de se protéger en magasinant en ligne

- Magasinez auprès de détaillants connus et fiables. Vérifiez les évaluations des produits.
- 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.
- 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.

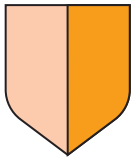
Quelques signes révélateurs d'une fausse appli mobile

- 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 ni aucune évaluation.
- 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, ou commence à partager des informations avec de tierces parties.

Rançongiciels : protégez vos fichiers

Un rançongiciel est un logiciel malveillant, ou maliciel, capable de verrouiller votre ordinateur et vos fichiers contre une rançon.

Une fois le maliciel propagé sur votre ordinateur ou appareil, vous ne pourrez plus y accéder, en partie ou entièrement. Les fraudeurs exigeront le paiement d'une rançon pour décrypter les fichiers et déverrouiller l'appareil. Ne payez surtout pas la rançon. Leurs menaces visent à vous effrayer et à vous intimider. Mais une fois la rançon payée, rien ne garantit 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, y compris les correctifs de sécurité.

Prenez le temps d'installer la plus récente version de vos systèmes d'exploitation et de vos applications. **Activez l'authentification multifactorielle.**

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?

Ne payez pas la rançon.
Le paiement de la rançon vous exposera à de nouvelles attaques et à de nouvelles demandes d'argent.

Déconnectez tous vos appareils.
Les rançongiciels peuvent se propager entre appareils et réseaux. Utilisez un réseau privé différent afin de limiter la propagation de petentiels rancongiciels dormants. Nettoyez, réinitialisez et mettez à jour tous vous appareils.

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, en particulier ceux qui donnent accès à vos comptes bancaires 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.

Conseils pour choisir des mots de passe complexes pour vos comptes en ligne

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

Il est essentiel d'utiliser un mot de passe distinct pour chaque compte en ligne, surtout que les criminels utilisent la technique de tentatives d'infiltration simultanées, ou bourrage d'identifiants, où ils téléchargent les 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.

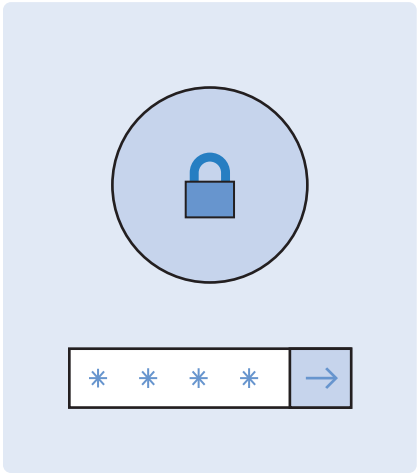
Votre institution financière peut avoir ses propres exigences pour les mots ou phrases de passe sécurisés. Voici quand même un moyen facile de choisir une phrase de passe difficile à deviner, mais qui est assez facile pour vous en souvenir.

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

L'usage d'une expression ou d'une phrase associée au site serait plus facile pour vous en souvenir. 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 12 caractères et ne dépasse pas la limite spécifiée.

KiNaPAmVi1/2!

Des 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.

Télétravail en toute sécurité

Il importe de palier les lacunes de sécurité de votre bureau à domicile.

Voici des conseils simples à suivre afin d'instaurer des protocoles de sécurité chez vous, même si votre bureau à domicile ne consiste qu'en un ordinateur portatif et un sofa.

Consultez régulièrement les portails de communications internes de votre entreprise pour les mises à jour des récentes cybermenaces et des pratiques que vous devez suivre afin de garder vos appareils en sécurité.

Protection des appareils

Si vous utilisez votre ordinateur et votre cellulaire personnels pour le travail, assurez-vous de prendre les précautions nécessaires.

- Si possible, n'utilisez que les appareils fournis par votre employeur. Vous profiterez ainsi des mesures de sécurité déjà prévues contre les cybermenaces et le vol de renseignements relatifs à votre travail.
- Veillez à ce que vos appareils soient protégés grâce à un mot de passe complexe et distinct.
- Améliorez la protection en installant des logiciels antivirus et anti-espions ainsi qu'un pare-feu sur tous vos appareils connectés, et déclenchez les mises à jour automatiques. De plus, vous devez permettre l'autorisation multifactorielle et utiliser un VPN.

Conseil : Gardez l'aide à portée de la main!

Gardez le numéro de téléphone du service informatique de votre entreprise accessible pour pouvoir facilement signaler un incident ou obtenir de l'aide.

Télétravail en toute sécurité (Suite)

Protection de vos renseignements personnels et de ceux d'autrui

Il est essentiel de séparer vos affaires professionnelles de vos affaires personnelles pour mieux protéger vos données, pour vous conformer aux règles de votre employeur et pour protéger l'intimité de votre famille.

- Séparez le professionnel du personnel. Ne sauvegardez pas des documents ou des données du travail sur vos appareils personnels. Gardez votre travail à part et ne laissez aucun membre de votre ménage utiliser les appareils de votre entreprise.
- N'imprimez que les documents dont vous avez absolument besoin. Déchiquetez tous ce qui contient vos renseignements personnels, ou ceux de vos clients ou de votre employeur.
- Assurez-vous de faire fréquemment des copies de sauvegarde de vos fichiers personnels sur une source externe sécurisée. Également, vous devez savoir comment récupérer ces copies de sauvegarde et vous devez établir une liste de vérification, ou des sauvegardes automatiques, afin que ce soit fait régulièrement.

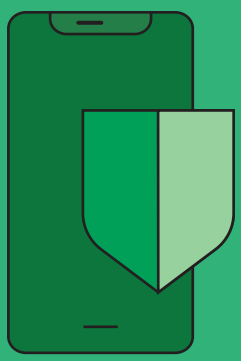
Sécurité du WiFi à domicile

Les fraudeurs savent que de nombreuses personnes travaillent à domicile de nos jours et ils essaient d'en profiter.

- Modifiez le nom et le mot de passe par défaut de votre routeur à quelque chose de difficile à deviner. Et veillez à automatiser l'installation des mises à jour et des correctifs du routeur afin de vous protéger contre les menaces.
- Établissez un réseau visiteur.

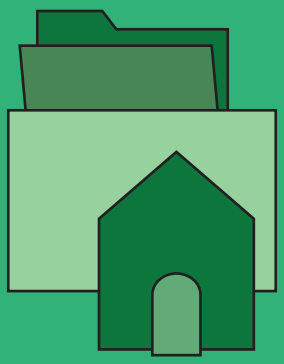
Détails

Trouvez plus de conseils sur
cba.ca/article/teletravail-en-toute-securite



Protection des appareils

Sécurité du WiFi



Distinction entre professionnel et personnel

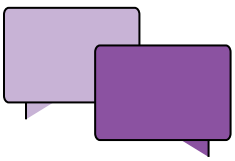
Signaler la fraude

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

Coalition canadienne antifraude
EnsembleContrelaFraude.ca

Gouvernement du Canada
Pensez Cybersécurité
pensezcybersecurite.gc.ca

Agence de la consommation en matière financière du Canada
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.

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