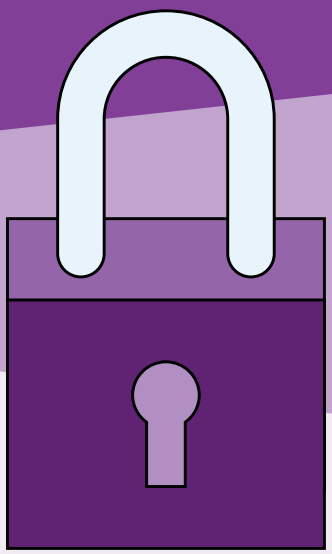
# Trousse de cybersécurité

## Protection contre les cybermenaces



ASSOCIATION DES BANQUIERS CANADIENS

En partenariat avec

PENSEZCYBERSECURITE.CA

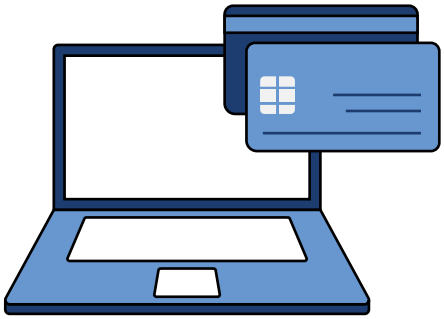
# L'Association des banquiers canadiens et PensezCybersécurité ont conçu cette trousse afin de vous aider à vous protéger en vous expliquant les menaces à la cybersécurité et l'importance d'adopter une habitude de cyberhygiène.

Nous sommes tous concernés. 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

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 essayer 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, pour commettre des activités de fraude.

Notre monde devient de plus en plus interconnecté, ce qui augmente l'exposition de nos renseignements personnels aux risques 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 et ainsi se protéger.



## 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.

# Cyberhygiène

## Liste de vérification pour protéger contre les cyberattaques vos renseignements et vos appareils

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

Au Canada, les banques utilisent une technologie de pointe et des niveaux de sécurité complexes pour protéger leurs clients contre la fraude. Néanmoins, les clients sont également responsables de leur propre protection, et donc de l'adoption de certaines mesures dans ce sens.

### 1. Installation de logiciels de protection

Installez des logiciels antivirus et anti-maliciels ainsi qu'un pare-feu sur tous vos appareils connectés, et mettez-les à jour régulièrement.

### 2. Mises à jour et correctifs

Installez toutes les versions mises à jour, aussitôt lancées, sur tous vos appareils connectés. Ne retardez pas l'installation des nouvelles versions, car elles contiennent d'importants correctifs de sécurité qui protègent les appareils contre les vulnérabilités connues. Les études montrent que 42 %[1] des propriétaires de téléphones intelligents mettent à jour leur système d'exploitation aussitôt la nouvelle version disponible, et que 56 %[2] des Canadiens mettent à jour leur logiciel antivirus au moins une fois par semaine.

### 3. Mots et phrases de passe forts et singuliers

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

### 4. Sauvegardes périodiques des données

Sauvegardez fréquemment vos fichiers sur des plateformes externes. Pour les fichiers très importants, envisagez une sauvegarde sur un support externe, un disque dur externe ou une clé USB. Vous protégerez ainsi vos données des cybermenaces, comme les rançongiciels. Également, instaurez des procédures claires pour récupérer les fichiers ainsi sauvegardés et prévoyez une liste de vérification de ces sauvegardes régulières. Toujours tester vos copies de sauvegarde afin de vous assurer de leur fonctionnement.

### 5. Désactivation des réseaux de partage de fichiers

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

[1] Pew Research Centre, 2017
[2] Sécurité publique Canada, 2018

# Cyberhygiène
(Suite)

### 6. Pas de téléchargement d'applications, de fichiers, de programmes et de logiciels gratuits

Une logique malveillante, comme un rançongiciel qui verrouille vos appareils et vos fichiers, un logiciel espion qui surveille secrètement vos activités en ligne, ou un espion de clavier qui enregistre secrètement les touches frappées sur votre clavier, peut être cachée dans le téléchargement et servir à accéder à des renseignements personnels, comme vos mots de passe et vos renseignements financiers.

### 7. Limite du partage en ligne de renseignements personnels importants

Les cybercriminels n'ont besoin que d'une infime quantité de vos renseignements personnels pour voler votre identité en ligne et commettre des crimes financiers. Faites attention à quels renseignements vous saisissez en ligne. Ne fournissez donc jamais votre date de naissance, votre numéro d'assurance sociale ou tout autre renseignement personnel ou financier, à moins d'avoir vous-même initié le contact ou de bien connaître votre correspondant.

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

Vérifiez les paramètres de sécurité et de confidentialité sur tous vos comptes de réseautage social et changez les paramètres par défaut. Limitez l'accès à ces comptes et rappelez-vous que ce vous y mettez restera pour toujours. 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.

## Votre liste de vérification de la cyberhygiène

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

# Déceler les arnaques les plus fréquentes

- Courriels frauduleux et hameçonnage
- Arnaque téléphonique ou vocale
- Échange de la carte SIM
- Fraude des jeux en ligne
- Faux sites et applications

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 de fonds.

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

**Signes que le courriel reçu est un hameçon**

## Exigences et menaces

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

## Expéditeur douteux

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

## Pièces jointes et liens douteux

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

## Avertissements

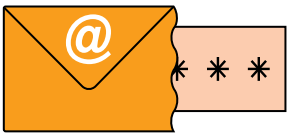
Avertissements que votre compte sera fermé ou l'accès à votre compte sera limité si vous ne répondez pas aux demandes dans le courriel.

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

# Arnaque par mot de passe à usage unique

Parmi les actions les plus efficaces que vous devez prendre afin de bien vous protéger en ligne : choisir un mot de passe distinct pour vos comptes confidentiels, éviter le partage excessif de renseignements personnels sur les réseaux sociaux et, lorsque cette option est offerte, utiliser l'authentification multifactorielle (AM) qui fait appel à un mot de passe à usage unique pour accéder à tous vos comptes en ligne.

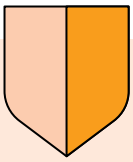
**Voici quelques conseils pour vous aider à éviter les arnaques axées sur le code à usage unique.**




## Fonctionnement de l'arnaque

Le processus d'authentification multifactorielle d'un grand nombre de sites Web nécessite un mot de passe à usage unique (OTP de son acronyme anglais), qui est en fait un code numérique à court temps d'expiration envoyé une fois, que vous pouvez recevoir soit par message texte soit par courriel. Cette étape est destinée à 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, 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.



## 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.
- 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.

## 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.

# Protection contre l'hameçonnage vocal

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

## Fonctionnement de l'arnaque

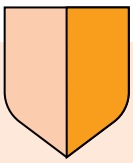
Vous recevez un appel d'un criminel qui se fait passer pour un représentant d'une agence gouvernementale ou des forces de l'ordre. Le message affirme que vous devez de l'argent, que vous avez une dette impayée ou que vous faites l'objet d'un mandat d'arrestation. Dans une variation sur ce même thème,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

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

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

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

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



### Protégez-vous!

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

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

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

# ATTENTION à la fraude sentimentale

La fraude sentimentale se trouve dans le peloton de tête des arnaques les plus fréquentes, selon le Centre antifraude du Canada. Cette fraude a coûté aux Canadiens plus de 59 millions de dollars en 2022, comparativement à 28 millions en 2020.

## Fonctionnement de ce stratagème

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

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

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

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

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

## Protégez-vous

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

- Votre interlocuteur ne perd pas son temps. Les escrocs veulent développer une relation rapidement. Ne vous laissez pas prendre.
- Votre interlocuteur vous demande de lui envoyer de l'argent, plus spécifiquement sous forme de carte cadeau, en cryptomonnaies ou par transfert électronique. Soyez vigilant(e).
- Si la personne a un profil public, vérifiez les incohérences entre ce qu'elle affiche et ce qu'elle vous dit. Vous pouvez faire une recherche d'image de sa photo de profil pour voir si la photo existe dans un autre contexte sur Internet.
- 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 dont vous pouvez lire les détails sur le site de l'ABC.

# 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.

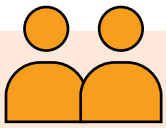
### Ne jamais cliquer sur des liens suspects, même s'ils semblent provenir d'un « ami »

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 cette sorte de renseignements personnels 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 l'enfant

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 votre enfant en ligne. Profitez des paramètres de sécurité afin de gérer l'accès en ligne de votre enfant, y compris les types de sites Web auxquels il peut accéder, les personnes qui peuvent communiquer avec lui et les façons dont il peut 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.

L'Agence de la consommation en matière financière du Canada donne des conseils pouvant vous aider à reconnaître les sites Web 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.
- Vous ne parvenez pas à connaître l'adresse civique ou le numéro de téléphone de l'entreprise.
- Les politiques relatives aux ventes, aux retours et à la confidentialité sont difficiles à repérer ou ne sont pas claires.
- Le bouton « Retour » ne fonctionne pas. En d'autres termes, vous n'arrivez pas à quitter une page ou à retourner à la page précédente.
- On vous demande des informations sur votre carte de crédit à un moment où vous n'achetez rien.

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

## Moyen de se protéger en magasinant en ligne

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

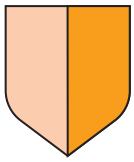
## Quelques signes révélateurs d'une fausse appli mobile

- 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.
- 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.

# Rançongiciels : protégez vos fichiers

Un rançongiciel est un logiciel malveillant, ou maliciel.

Une fois que le maliciel est installé sur votre ordinateur, rien n'arrivera jusqu'à ce que des pirates informatiques s'en emparent et cryptent vos fichiers. Lorsque les fichiers sont cryptés (verrouillés), les fraudeurs exigeront le paiement d'une rançon pour les décrypter et les déverrouiller. Toutefois, rappelez-vous que, 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. Prenez le temps d'installer la plus récente version de vos systèmes d'exploitation et de vos applications. Sauvegardez fréquemment vos fichiers sur des systèmes de stockage externes, comme un disque dur externe ou une plateforme infonuagique, qui ne sont pas reliés à votre ordinateur.

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

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

## Que faire si vous en êtes victime?

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

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

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

**Changez vos mots de passe.**
Changez tous vos mots de passe en ligne, 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.

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

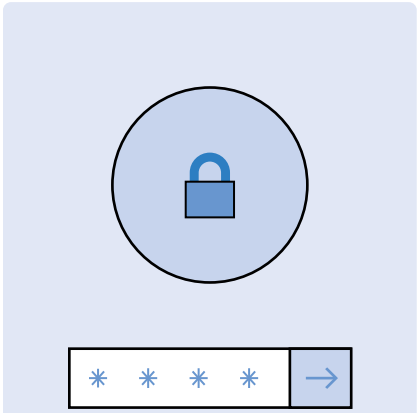
Votre institution financière pourrait avoir ses propres exigences pour les mots de passe sécurisés. Voici quand même un moyen facile de choisir un mot de passe difficile à deviner, mais qui est assez facile pour vous en souvenir.

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

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 8 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 mettez-les à jour régulièrement. Installez les mises à jour et les correctifs aussitôt lancés. 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!

### 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)

## Protction 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.

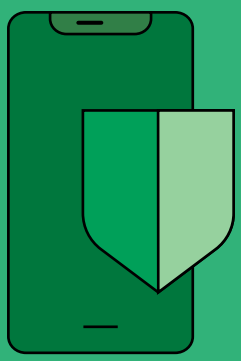
## Sécurité du WiFi à domicile

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.

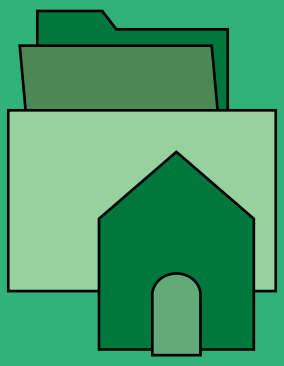
## Détails

Trouvez plus de conseils sur
https://cba.ca/staying-safe-while-working-from-home?l=fr



**Protection des appareils**

**Sécurité du WiFi**



**Distinction entre professionnel et personnel**

# Ressources additionnelles

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

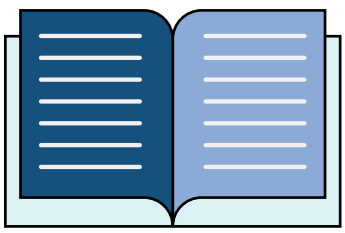
Questionnaires de sensibilisation à la cybersécurité :
https://abccybersecurite.ca

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

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

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

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



ASSOCIATION DES BANQUIERS CANADIENS

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

PENSEZCYBERSECURITE.CA

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