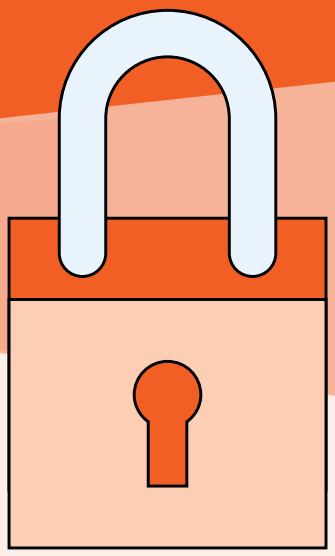
Trousse de cybersécurité pour nouveaux arrivants au Canada

Protection contre les cybermenaces



ASSOCIATION DES P QUIERS CANADIENS

En partenariat avec

SEZCYBERSECURITE.CA

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

D9N9FL?9J<= <= D9 HJN=FLAGF =L <= D9 <L=;LAGF <=K ;Q:=JE=F9;=K #DD=K ;GDD9:GJ=FL 9N=; D=K GJ?9FAKE=K <= J?D=E=FL9LAGF D=K >GJ;=K <= DGJ<J= =L LGMK D=K FAN=9MP <= ?GMN=JF=E=FL 9F <= HJGL?=J D= KQKLE= F9F;A=J 9AFKA IM= D=MJK ;DA=FLK ;GFLJ= D= ;Q:=J;JAE= .9J 9ADD=MJK NGMK HGMN=R HJ=F<J= <= KAEHD=K E=KMJ=K =F NM= <= <;=D=J D=K ;Q:=JE=F9;=K D=K HDMK =F ;GMJK 9M !9F9<9 =L <= NGMK HJGL?=J <= D9 >J9M<= F9F;AJ=A

Contenu

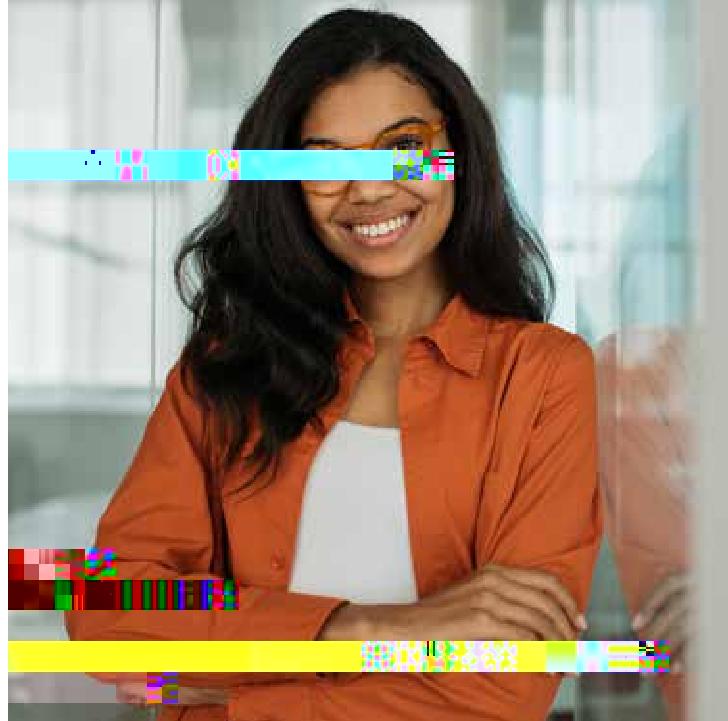
Abécédaire de la cybe)

'FL=JF=L 9 >9 ; ADALŭ <= >9ŢGF AFŭ<AL= D=K ; GFL9 ; LK 9N= ; D9 >9 EADD= =L D=K 9 EAKă 9AFKA I M= D=K 9 ; LANALŭK ; G E E=J ; A9D=K =L D9 ?=KLAGF <=K ūF9F ; =Kă I MA K= >GFL <ŭKGJ E 9AK HDMK J9HA<= E =FLă HDMK =ɣA ; 9 ; = E =FL =L HDMK ; GF>GJL9 : D= E =FLĂ

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, afn 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 profter 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.



1. Protection de vos appareils

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

2. Mises à jour et correctifs

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

3. Choix de phrases et de mots de passe distincts et complexes

Créez un mot ou une phrase de passe distincts pour chaque compte en ligne et chaque site, et déclenchez l'authentification multifactorielle. C'est très important vu que l'atteinte à la sécurité des données dans un site Web pourra entraîner l'acquisition de vos coordonnées de connexion par de [illegible]
des do l, [illegible]

Cyberhygiène

ÿ1MAL=ÿ

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

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

7. Limite du partage en ligne de renseignements personnels importants

Les cybercriminels n'ont besoin que d'une infme quantité de vos renseignements personnels pour voler votre identité en ligne et commettre des crimes fnanciers. Attention aux renseignements saisis en ligne.

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

8. Rafermissement des paramètres de sécurité et de confdentialité des réseaux sociaux

Vérifez les paramètres de sécurité et de confdentialité sur tous vos comptes de réseautage social et changez les paramètres par défaut. Choisissez soigneusement qui peut accéder à vos réseaux sociaux ou les consulter, et limitez le type de renseignements que vous y afchez.

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

Votre liste de vérifcation 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 fchiers
- ☐ Attention au téléchargement d'applications, de fchiers, de programmes et de logiciels
- ☐ Limite du partage en ligne de renseignements personnels importants
- ☐ Rafermissement des paramètres de sécurité et de confdentialité des réseaux sociaux

4GA;A MF= DAKL= <Ä9JF9IM=K ;GMJ9FL=K IM= NGMK <=N=R ;GFF9€LJ= Ä

&9E=ŢGFF9?= =L ;GMJJA=DK >J9M<MD=MP

!G<= ń MK9?= MFAIM=

&9E=ŢGFF9?= NG;9D

JF9IM= <= D9 K9AKGF <=K AEHżLK

-ɣJ=K <Ä= EHDGA >J9M<MD=MK=K

HHDA;9LAGFK =L KAL=K 5=: >J9M<MD=MP

09FŢGF?A;A=DK

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

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,

Hameçonnage et courriels frauduleux

L=FL9LAN=K <@9E=TGFF9?= =PAKL=FL <=HMAK IM= D= ;GMJJA=D =PAKL=Å !=IMA 9 ;@9F?uă ;=KL D9 F9LMJ= HDMK J9yAFu= <= ;=K 9JF9IM=K yD=K >9ML=K DAF?MAKLAIM=K =L ?J9EE9LA;9D=K F=F KGFL HDMK MF KA?F= JuNuD9L=MJya ;=IMA Fu;=KKAL= MF= NA?AD9F;=KGML=FM=Å

Signes que le courriel reçu est un hameçon

Exigences et menaces

La demande de renseignements provient-elle d'une source légitime? Votre banque ne vous enverra jamais de courriel menaçant ni ne vous appellera pour exiger la divulgation de renseignements personnels, comme votre mot de passe, le numéro de votre carte de débit ou de crédit ou le nom de jeune fille de votre mère. Par ailleurs, les banques et le gouvernement au Canada jamais ne vous demanderont un paiement par carte cadeau ou carte prépayée, par cryptomonnaie ou par transfert de fonds.

Expéditeur douteux

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

Pièces jointes et liens douteux

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

Avertissements

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

Code à usage unique

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

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

Les appels ou messages comportent des menaces de vous signaler à la police qui

Arnaques axées sur les contribuables

"MJ9FL D9 K9AKGF <=K AEHzLKă <=K >J9M<=MJK MKMJH=FL DÏA<=FLALŭ <Ï=EHDGQŭK <= DÏ ?=F;= <M J=N=FM <M !9F9<9 ÿ 0!ÿ=L NGMK D=MJJ=FL 9AFKA 9N=; <=K <=LL=K >9;LA;=K HGMJ NGMK KGMLAJ=J <= DÏ9J?=FL GM <=K J=FK=A?F=E=FLK H=JKGFF=DK IMÏADK HGMJJGFL MLADAK=J 9MP ūFK <Ï9MLJ=K 9;LANALŭK >J9M<MD=MK=KĂ

Fonctionnement de l'arnaque

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

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

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

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

Si vous êtes victime de cette arnaque

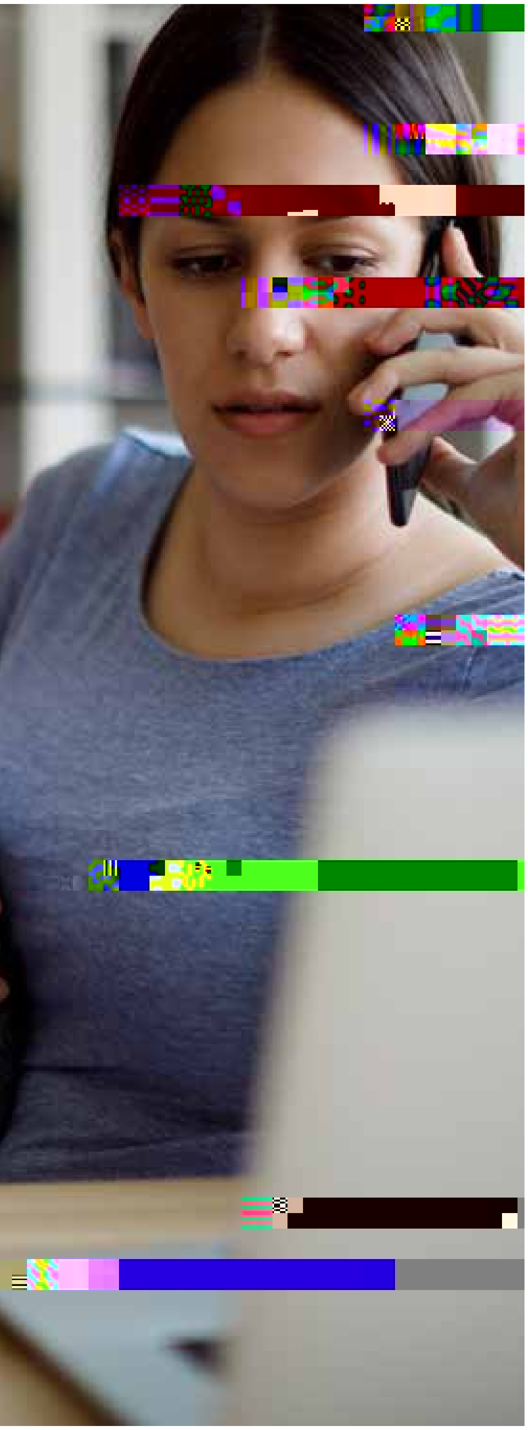
Si vous recevez un appel déclarant que vous devez de l'argent à l'ARC, communiquez directement avec Revenu Canada pour voir, ou consultez « Mon dossier » sur son site Web. Si vous croyez avoir donné accidentellement vos informations financières à des cybercriminels, communiquez sans tarder avec votre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

Jamais l'ARC...

- ne vous enverra un courriel avec un lien vous demandant de révéler vos renseignements personnels ou financiers;
-

Offres d’emploi frauduleuses

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



Fonctionnement de l’arnaque

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

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

Protégez-vous

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

& Ƭ
qtrife ɥ l’ sŷ Ş pedrop o
fe W f rentreprise
qeoeӟntreprisedW'emploi i W ɞ ӟ ntpon Ꝁ Ꝁ t ud

Ressources

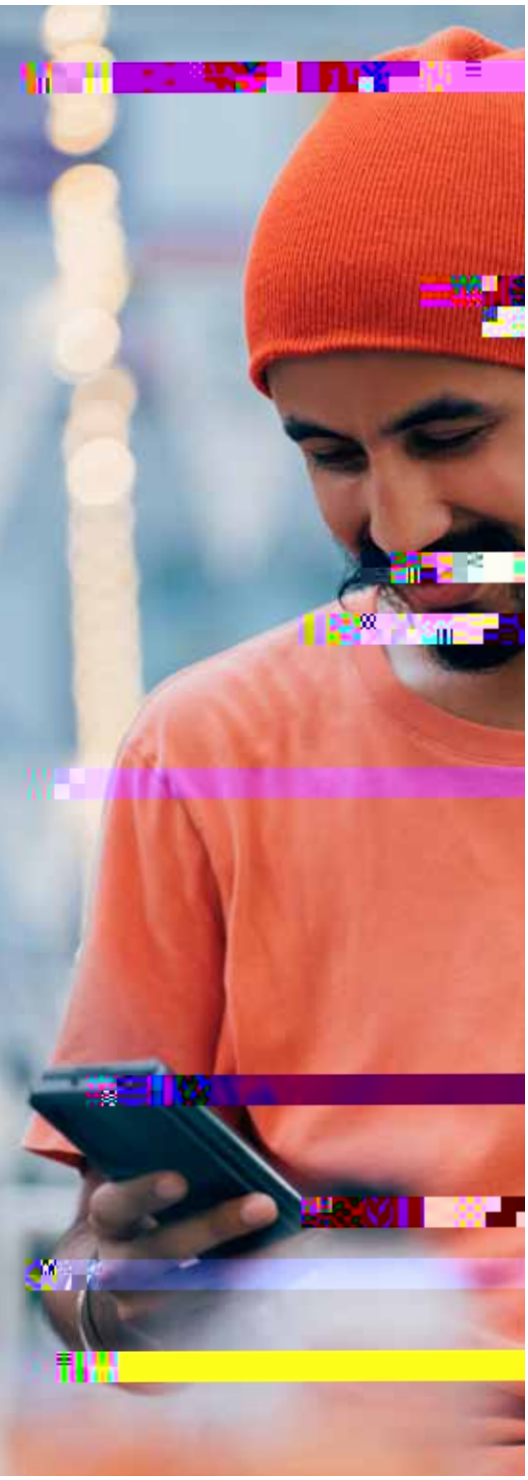
Le Centre antifraude du Canada expose les formes les plus courantes de l’offre d’emploi frauduleuse sur son site Web.

Applications et sites Web frauduleux

*=K ;Q:=J;JAEAF=DK ;Jŭ=FL <=K 9HHDA;9LAGFK =L <=K KAL=K 5=: <= E9?9KAF9?= >J9M<MD=MPă I MA J=KK=E:D=FL ń KŭQ EŭHJ=F<J= 9MP NJ9AKĂ

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

Voici quelques astuces pour pouvoir les déceler.



Signes d'un site Web de magasinage frauduleux

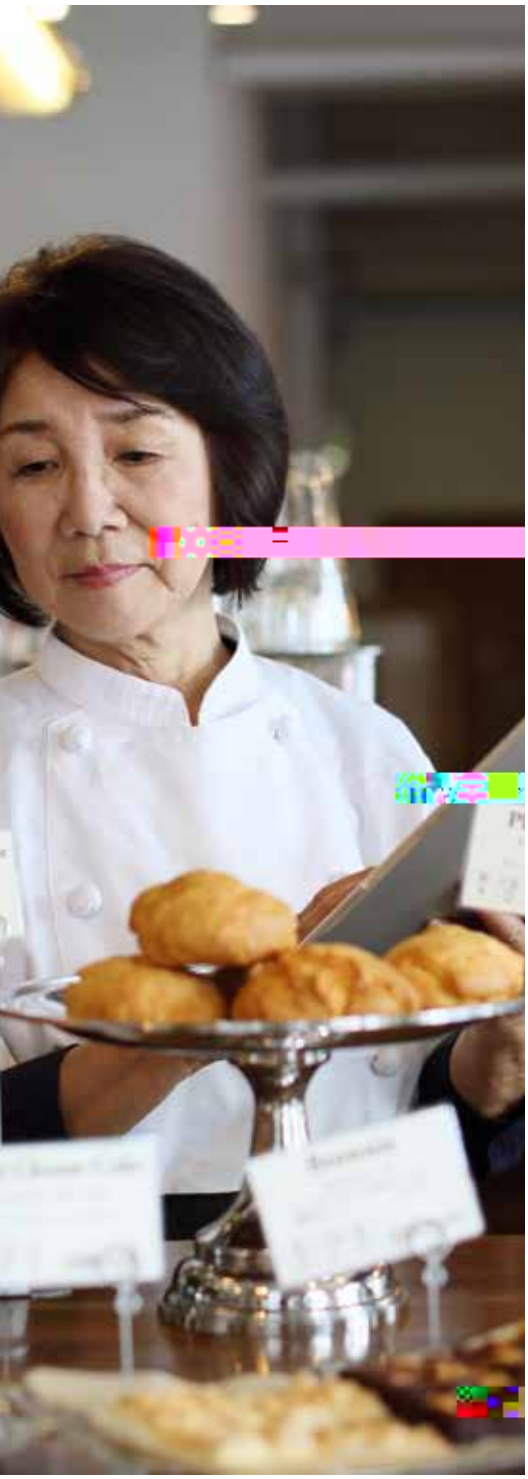
- Le site Web est mal conçu, ne présente pas une image professionnelle et contient des hyperliens rompus.
- L'adresse du site contient des acronymes et des termes qui n'ont pas leur place sur ce site.
- Le site affiche un cadenas déverrouillé ou utilise le format http (et non https), ce qui signifie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

Signes d'une application frauduleuse

- Le nom du diffuseur de l'application (habituellement affiché sous le nom de l'application) ressemble au nom du diffuseur légitime, mais quelque chose cloche.
- La description de l'appli est mal rédigée ou n'affiche aucun commentaire.
- Il faut un nombre d'autorisations excessif pour l'installation.
- L'application produit beaucoup de fenêtres de publicité ou de demandes de saisie de renseignements personnels.
- L'application utilise une quantité énorme de données ou utilise des données même quand elle est fermée.

Protégez-vous

-



Comment éviter le téléchargement de rançongiciels

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

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

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

Sauvegardez fréquemment vos fichiers sur des systèmes de stockage externes, comme un disque dur externe ou une plateforme infonuagique, qui ne sont pas reliés à votre ordinateur. Conservez vos données confidentielles sur une plateforme externe non connectée à Internet, comme une clé USB ou un disque dur externe portatif, car si jamais votre système est verrouillé, les

Choisir un mot de passe complexe

CANADIAN BANKE

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'in f ltration simultanées, ou bourrage d'identi f ants, 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.

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 chi f res et des caractères spéciaux, modi f ez 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 spéci f ée.

KiNaPAmVi1/2!

Un mot de passe solide n'est qu'une première ligne de défense pour vos renseignements personnels importants. Servez-vous donc de l'authenti f cation multifactorielle (sécurité à deux étapes)

Signaler la fraude

! = F=KL H9K NGLJ= >9ML= KA NGMK LG E : =R NA ; LA E = <MF= 9JF9 I M=Å 2GML=>GAKå NGMK HGMN=R NGMK 9A<=J =L 9A<=J 9MLJMA =F 9?AKK9FL K9FK L9J<=JÅ

Contactez votre institution financière

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

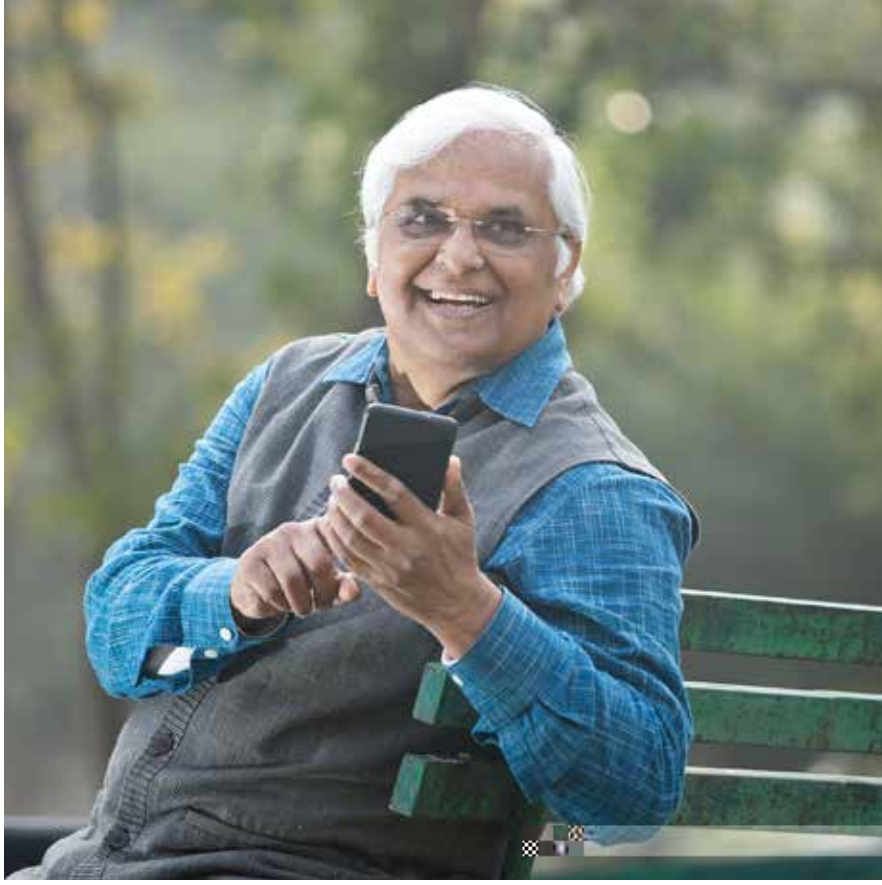
Contactez la police

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

Signalez l'incident

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

.



Association des banquiers canadiens
.JŭN=FLAGF <= D9 >J9M<= Ä
; : 9Ä; 9Ţ>J9M<=

Questionnaires de sensibilisation à la cybersécurité :
9 : ; ; Q : =JK= ; MJAL=Ä; 9

Bulletin gratuit *Conseils pour la protection contre la fraude* :
'FK ; JAHLAGF =F DA?F=Ä