



TELUS Averti Or



Aider les personnes âgées
au Canada à naviguer dans
un monde numérique.

Contenu

Introduction.....	1
--------------------------	----------

Vous pourriez être plus connecté que vous le croyez.....	2
---	----------

Conseils pour l'utilisation sécuritaire d'Internet.....	4
--	----------

1. Créer des mots de passe difficiles à trouver	4
2. Mises à niveau logicielles.....	5
3. Créer une alerte Google	7
4. Surveiller son navigateur	7
5. Partager de l'information personnelle en ligne ...	8
6. Réfléchir avant de cliquer	9
7. Magasiner en ligne	10
8. Prendre et publier des photos	11

Conseils de sécurité sur les téléphones intelligents.....	12
--	-----------

1. Désactiver le géomarkage	12
2. Configurer les services de localisation, de verrouillage ou de suppression à distance	12
3. Faire preuve de prudence dans l'utilisation des réseaux Wi-Fi publics.....	13
4. Effacer le contenu de son appareil.....	14
5. GPS	14

Conseils de sécurité sur les réseaux sociaux.....	15
--	-----------

1. Surveiller ses paramètres de confidentialité et ses autorisations.....	15
2. Bien réfléchir avant d'entrer en contact avec quelqu'un ou de publier quelque chose.....	15
3. Choisir prudemment ses applications	16
4. Fermer une session	16
5. Mettre de l'ordre dans sa vie numérique.....	16

Se protéger contre le vol d'identité	17
---	-----------

1. Arnaques courantes pour le vol d'identité	18
2. Indices de vol d'identité :	19
3. Limitez le risque de vol d'identité en suivant ces conseils	20
4. Que faire si vous êtes victime de vol ou de fraude d'identité?	21

Conseils pour utiliser les sites de rencontre.....	22
---	-----------

1. Créer un deuxième compte de courriel	22
2. Visiter des sites web sans danger	22
3. Consulter les modalités et conditions	22
4. Créer un profil attrayant	22
5. Faire preuve de prudence si l'on donne rendez-vous à quelqu'un	23
6. Se méfier des escroqueries amoureuses.....	23

Conseils sur les jeux sociaux.....	24
---	-----------

1. Bien réfléchir avant de partager sa liste de contacts ou d'amis avec cette application	24
2. Clavarder avec précaution	24
3. Porter attention au temps d'écran	24
4. Prendre garde à la cyberintimidation.....	25

Centre de formation TELUS.....	26
---------------------------------------	-----------



Introduction

Ce guide a été créé à l'intention des aînés canadiens qui utilisent Internet et qui souhaitent participer à la société numérique en toute sécurité. Il peut servir de référence personnelle, mais il est aussi utilisé dans le cadre des ateliers TELUS Averti^{MD} Or.

Si vous souhaitez réserver un atelier TELUS Averti Or gratuit pour votre groupe communautaire ou si vous avez des questions au sujet du contenu du présent guide, veuillez communiquer avec **averti@telus.com**.

Pour connaître d'autres ressources qui vous permettront de naviguer en toute sécurité dans le monde numérique, visitez **telus.com/averti**.



Vous pourriez être plus connecté que vous le croyez.

Prenez quelques instants pour évaluer votre présence en ligne en répondant aux questions ci-dessous.

Utilisez-vous ce qui suit?

Adresse de courriel ☐ Qui ☐ Non

Twitter ☐ Qui ☐ Non

Facebook ☐ Qui ☐ Non

Instagram ☐ Qui ☐ Non

YouTube ☐ Qui ☐ Non

Envoyez-vous des **textos**? ☐ Qui ☐ Non

Téléchargez-vous des **applications**? ☐ Qui ☐ Non

Utilisez-vous des services **bancaires en ligne**? ☐ Qui ☐ Non

Magasinez-vous **en ligne**? ☐ Qui ☐ Non

Publiez-vous des **photos en ligne**? ☐ Qui ☐ Non

Participez-vous à des **concours en ligne**? ☐ Qui ☐ Non

Jouez-vous à **des jeux en ligne**? ☐ Qui ☐ Non

Utilisez-vous **Internet pour effectuer des recherches**? ☐ Qui ☐ Non

Que faites-vous d'autre en ligne?

.....

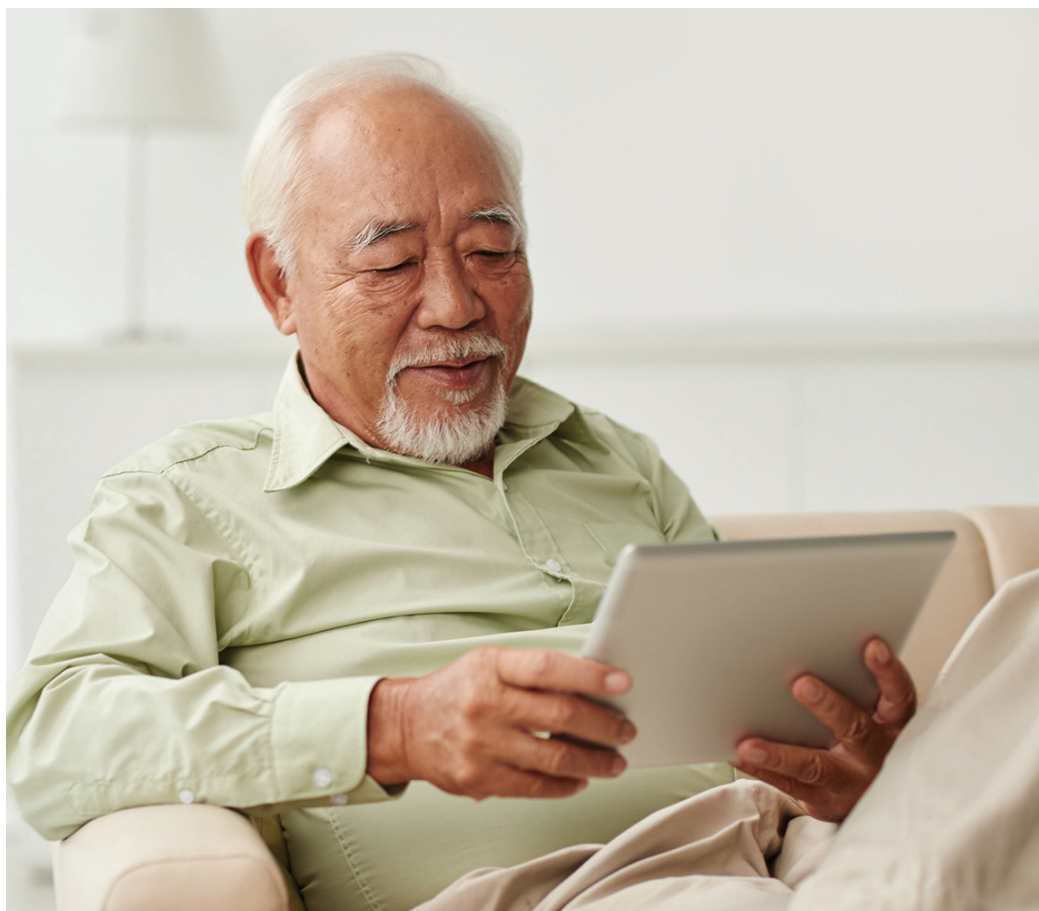
.....

.....

.....

En faisant cet exercice, vous avez peut-être découvert que vous étiez plus connecté que vous le croyiez au départ. Cependant, même si vous n'avez qu'un compte de courriel et que vous vous contentez de naviguer sur le web, vous faites toujours partie d'une société numérique en progression.

Ce guide offre des conseils pour protéger votre vie privée et assurer votre sécurité en ligne.



Conseils pour l'utilisation sécuritaire d'Internet



1. Créer des mots de passe difficiles à trouver

Un mot de passe difficile à deviner peut empêcher les autres de pirater vos comptes de médias sociaux ou de courriel, entre autres. Il devrait comporter au moins huit caractères, dont des nombres, des lettres et des symboles.

Pour créer un mot de passe sécuritaire, vous pouvez utiliser une phrase secrète ou remplacer les mots de la phrase par leur première lettre. Par exemple : « Je n'oublie jamais mon mot de passe 2* » peut devenir JNOJMMDP2*

Authentification à deux facteurs : Cette fonction de sécurité vous oblige à vous authentifier avec un élément de plus que votre nom d'utilisateur et votre mot de passe. Il peut s'agir d'un code unique envoyé par texto à votre appareil ou d'une vérification biométrique comme une empreinte digitale. **Pour une sécurité optimale, il est recommandé d'activer l'authentification à deux facteurs dans tous vos comptes en ligne.**

N'utilisez pas le même mot de passe pour votre ordinateur, votre téléphone intelligent, votre courriel et vos applis (p. ex. compte bancaire en ligne ou Facebook). Autrement, c'est tout un trésor pour les pirates informatiques.

Voici les six pires mots de passe de 2018 selon SplashData :

- | | | |
|-------------|--------------|-----------|
| 1. 123456 | 3. 123456789 | 5. 12345 |
| 2. password | 4. 12345678 | 6. 111111 |



2. Mises à niveau logicielles

Pour protéger votre téléphone intelligent, votre tablette ou votre ordinateur des virus, il faut accepter les mises à niveau logicielles, qui comprennent d'importants correctifs de sécurité. **Installez ces mises à niveau dès qu'elles sont disponibles pour minimiser les risques.**

Dans le cas des téléphones intelligents, les fabricants (p. ex. Apple et Android) offrent tous leur propre programme de mise à niveau logicielle ainsi que des gestionnaires de logiciel qui vous indiquent s'il existe une nouvelle version du logiciel pour votre appareil ou une application installée sur votre appareil. Les mises à niveau logicielles se trouvent dans l'application des paramètres, Apple () et Android () , par exemple.

Il en va de même pour votre ordinateur; toutes les mises à jour logicielles doivent provenir du fabricant du logiciel.



Se protéger des demandes de mises à jour logicielles illégitimes.

Les mises à jour logicielles frauduleuses peuvent causer beaucoup de tort si vous cliquez dessus. N'oubliez pas de toujours prendre le temps de bien regarder de quoi il s'agit. **Dans le doute, évitez de cliquer dessus ou de la télécharger.**

- Ne répondez pas aux demandes de mises à jour logicielles à partir d'un réseau **Wi-Fi public**.
- Téléchargez les mises à jour uniquement à partir du **site web du fabricant** du logiciel (Microsoft ou Apple, par exemple).
- **Ne cliquez jamais sur les liens dans les courriels qui vous demandent de mettre à niveau votre logiciel.** Si vous vous interrogez sur la légitimité d'un lien, passez le pointeur au-dessus pour voir l'adresse de destination. Si vous ne reconnaissez pas le site web, ne cliquez pas.

<http://this.is/scam/donot/click&1256abc>



- Examinez soigneusement les demandes de mise à jour logicielles, surtout si elles semblent venues de nulle part ou d'un expéditeur inconnu. Vérifiez s'il y a des **fautes de grammaire et d'orthographe**.
- Configurez votre ordinateur et votre téléphone intelligent pour qu'ils **appliquent automatiquement les mises à jour** du système d'exploitation et des applications, dès qu'elles sont disponibles.



3. Créer une alerte Google

Créez une alerte Google associée à votre prénom et à votre nom à **google.com/alerts** pour être avisé par courriel lorsque votre nom apparaît en ligne. Vous pouvez préciser la recherche en ajoutant la province ou la ville où vous habitez.

Même si cela n'offre pas une garantie à toute épreuve, c'est un bon début pour suivre votre empreinte numérique. Vous pourriez ainsi détecter les signes précurseurs d'un vol d'identité.

Pour en savoir plus sur les alertes Google, visitez **<https://goo.gl/Kh01N4>**

4. Surveiller son navigateur

Le navigateur web que vous utilisez (p. ex. Internet Explorer, Firefox, Google Chrome ou Safari) est votre passerelle Internet et votre premier point de défense contre les activités malveillantes. **Employez toujours la plus récente version du navigateur** et configurez-en les paramètres en fonction de votre sécurité et de la protection de votre vie privée. Pour plus de confidentialité, vous pouvez également vous servir du navigateur en mode incognito ou privé.

Il est également recommandé de vider l'historique et la mémoire cache de votre navigateur au moins une fois par mois.

Recherchez les instructions concernant votre navigateur sur google.com (« comment supprimer l'historique dans Internet Explorer », par exemple).



5. Partager de l'information personnelle en ligne

En toutes circonstances, **limitez la quantité de renseignements personnels que vous partagez en ligne.**

Ainsi, vous pourrez mieux protéger votre vie privée et réduire la possibilité d'être victime de vol d'identité ou de fraude.

Pensez-y à deux fois avant de publier les renseignements personnels suivants sur une plateforme publique (un profil dans les médias sociaux, par exemple) :

- Vos coordonnées (numéro de téléphone, adresse de courriel, etc.)
- Votre nom complet et votre date de naissance
- Votre adresse résidentielle
- Le nom complet de vos enfants ou des membres de votre famille
- Les dates et les détails de vos voyages, de vos vacances et des périodes que vous passez à l'extérieur de la maison

Réfléchissez bien également avant de remplir des questionnaires en ligne sur les médias sociaux. Les renseignements personnels que vous fournissez alors peuvent révéler les réponses aux questions de sécurité qui protègent vos comptes en ligne.

Avant de partager des renseignements, demandez-vous toujours :

1. Comment ces renseignements seront-ils utilisés?
2. Pourquoi ont-ils besoin de ces renseignements?
3. Qui aura accès à ces renseignements?
4. Comment ces renseignements seront-ils protégés?



6. Réfléchir avant de cliquer

- **Ne cliquez jamais sur une pièce jointe ou sur un lien suspect, même s'ils semblent intéressants.** Les liens, les pièces jointes et les applications indésirables sont à l'origine de beaucoup d'escroqueries et de problèmes causés par des logiciels malveillants.
- **Ne répondez pas aux appels ou aux courriels vous demandant des renseignements personnels ou financiers,** surtout si une forme de pression est exercée sur vous ou si on cherche à vous faire peur.
- Les véritables fournisseurs de services, comme TELUS, l'Agence du revenu du Canada, les banques, etc., **ne vous demanderont pas de fournir ou de confirmer vos renseignements personnels par des moyens non sécuritaires** comme le courriel.
- Apple, Microsoft et les autres entreprises reconnues **ne vous appelleront jamais pour vous dire que vous avez un problème lié à votre ordinateur** ou à votre appareil. N'acceptez pas de vous rendre sur un site web que vous propose la personne au téléphone sous prétexte de vous aider à réparer votre ordinateur. C'est une arnaque!
- **Si c'est trop beau pour être vrai, dites-vous que c'est sans doute trop beau pour être vrai!** Si vous recevez une offre douteuse par courriel, appelez votre fournisseur de services ou votre institution financière pour la vérifier ou pour confirmer la demande d'information sur le compte. **Ne composez jamais le numéro indiqué dans l'offre par courriel.**

Conseil de TELUS Averti : Créez-vous un compte de courriel réservé aux médias sociaux, aux jeux en ligne, aux concours, aux listes d'envoi, etc. Conservez-en un autre pour une utilisation plus professionnelle comme les services bancaires en ligne, les réservations de voyage, les communications avec les amis et la famille, etc.



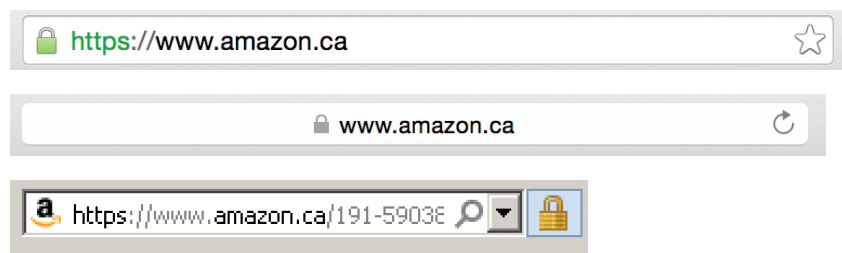


7. Magasiner en ligne

Pour magasiner en ligne, allez sur des sites web reconnus. Consultez vos amis, les membres de votre famille ou les références en ligne (non affiliées au site) pour connaître la réputation de l'entreprise.

Vérifiez si le site web sur lequel vous magasinez utilise le chiffrement. Au début de la barre d'adresse, assurez-vous qu'il y a un « s » au bout de **http** et, plus loin, une **icône de cadenas**; ce qui indique que le site web utilise le chiffrement pour protéger les renseignements sur le paiement.

Prenez par exemple l'adresse du site web amazon.ca ci-dessous. Elle commence par **https://** et une icône de cadenas apparaît dans la barre d'adresse.



N'acceptez pas qu'on enregistre les renseignements de votre carte de crédit pour faciliter de futurs achats.

Même si cela peut sembler pratique pour la prochaine fois, les données enregistrées peuvent être compromises si l'entreprise est victime de piratage.



8. Prendre et publier des photos

Nombreux sommes-nous à aimer prendre des photos pour les partager en ligne avec nos amis et les membres de notre famille, mais il faut tenir compte des enjeux concernant la protection de la vie privée et la sécurité.

Avant de publier des photos en ligne :

- **Demandez la permission des personnes qui y figurent.**
Cela s'applique aussi aux petits-enfants et aux enfants qui vous entourent. Demandez d'abord la permission aux parents avant de publier une photo dans laquelle figurent des enfants.
- **Pensez à votre public cible.** Ajustez les paramètres de sécurité des comptes de médias sociaux pour que seules les personnes auxquelles vous n'hésitez pas à montrer ces photos puissent les voir. Autrement, servez-vous d'un service de stockage infonuagique reconnu pour télécharger et ranger vos photos avant de configurer les dossiers pour les partager directement avec certaines personnes.

Conseil de TELUS Averti : Choisissez soigneusement les applications auxquelles vous accordez un accès à votre dossier Pellicule. Lisez toujours les conditions pour connaître l'utilisation que l'on fera de vos photos.



Conseils de sécurité sur les téléphones intelligents



1. Désactiver le géomarquage

Bien que la plupart des sites de médias sociaux suppriment le géomarquage ou les données de localisation des photos, n'oubliez pas que des détails de l'emplacement demeurent associés aux images partagées par courriel ou par texto.

Vous pouvez **désactiver le géomarquage** sur votre appareil si vous ne voulez pas que l'information sur l'emplacement accompagne vos images. Recherchez les instructions concernant votre appareil sur [google.com](https://www.google.com) (« comment désactiver le géomarquage sur un iPhone », par exemple).



2. Configurer les services de localisation, de verrouillage ou de suppression à distance

Servez-vous de ces services intégrés pour **verrouiller votre téléphone intelligent, le localiser ou supprimer les données à distance en cas de perte ou de vol**. Ces services vous permettent également d'afficher un message à distance sur votre téléphone intelligent pour indiquer comment vous joindre s'il est retrouvé. Vous pouvez aussi faire en sorte qu'il émette un son si vous l'avez tout simplement égaré aux alentours.

Sur les appareils Apple, cette fonction s'appelle **Localiser mon iPhone**, alors que si vous avez un appareil Android, c'est **Localiser mon appareil**. Vous pouvez configurer ces services dans les Paramètres de votre appareil.





3. Faire preuve de prudence dans l'utilisation des réseaux Wi-Fi publics

Les pirates informatiques peuvent accéder aux données personnelles des autres utilisateurs en passant par les réseaux Wi-Fi publics (dans un café, par exemple). Voici quelques conseils à suivre pour réduire les risques :

- **Confirmez toujours la légitimité d'un réseau Wi-Fi avant de vous y connecter.** Ne vous fiez pas uniquement à son nom. S'il existe de multiples réseaux Wi-Fi pour le même endroit, demandez au personnel lequel vous devriez utiliser. Lisez aussi les modalités de service du lieu en question pour savoir à quoi vous consentez avant de vous connecter.
- Servez-vous des Wi-Fi publics uniquement pour **consulter des sites web sur lesquels vous ne devez pas ouvrir de session** (notamment des sites web généraux). Si vous devez accéder à des données sensibles ou entrer vos identifiants de connexion en vous servant d'un Wi-Fi public, allez uniquement sur les sites web dont l'adresse commence par https (consultez la page 10 pour en savoir plus sur les sites web sécurisés).
- **N'installez jamais de logiciel et ne faites jamais de mises à jour au moyen d'un Wi-Fi public**, car cela pourrait introduire des virus dans votre ordinateur. Par exemple, une des attaques courantes consiste à informer l'utilisateur que la version de son navigateur n'est plus à jour et à le rediriger vers un faux site web qui installera un virus.



4. Effacer le contenu de son appareil avant de le recycler ou de le donner

La technologie progresse à un rythme étonnant et bien des gens changent souvent de téléphone intelligent.

Vous êtes-vous déjà demandé ce qu'il advenait des appareils dont vous vous débarrassez? Et surtout, ce qu'il advient de tous les renseignements personnels qui y sont stockés, comme les coordonnées, les mots de passe, les photos et plus encore?

Avant de vous défaire de vos appareils mobiles, assurez-vous d'en effacer tout le contenu.

Pour savoir comment vous départir de votre appareil mobile en toute sécurité, visitez un Centre de formation TELUS.



5. GPS

Gérez les paramètres de localisation de vos applications en saisissant bien quelles sont les applications qui ont besoin de savoir où vous êtes. Posez-vous la question : est-ce que Facebook ou Twitter a vraiment besoin de savoir où je me trouve pour bien fonctionner?

Désactivez le GPS (ou les paramètres de localisation) et le Bluetooth lorsque vous ne les utilisez pas. Ainsi, vous pourrez mieux protéger votre vie privée et économiser la pile!

Vous trouverez le GPS ou la localisation et le Bluetooth dans la section « paramètres » de votre téléphone intelligent.

Conseils de sécurité sur les réseaux sociaux

Notes



1. Surveiller ses paramètres de confidentialité et ses autorisations

Lisez toujours les paramètres de confidentialité et les autorisations avant d'ouvrir un nouveau compte dans un média social ou de télécharger une nouvelle application. Ne les acceptez pas aveuglément.

- **Autorisations;** elles déterminent, parmi vos renseignements personnels, ceux auxquels un site de réseautage social ou une application mobile peut ou non accéder et ceux qu'il lui est possible de communiquer à votre sujet. (Votre liste de contacts, vos photos, l'endroit où vous êtes, etc.)
- **Paramètres de confidentialité;** ils déterminent qui est autorisé ou non à voir votre profil et vos publications en ligne (par exemple, est-ce que seuls les amis de votre liste peuvent les consulter ou si le grand public y a aussi accès?)



2. Bien réfléchir avant d'entrer en contact avec quelqu'un

En règle générale, vous devriez **communiquer et partager en ligne uniquement avec les personnes que vous connaissez vraiment**. En devenant « ami » avec des étrangers en ligne, vous vous exposez à des risques en matière de sécurité et de protection de la vie privée. Faites également **attention à ce que vous publiez en ligne**. Par exemple, publier des photos de vous en vacances peut indiquer à d'autres qu'il n'y a personne à la maison.

Le saviez-vous? Selon Facebook, 1 pour cent des 2,38 milliards de profils d'utilisateur actifs sont faux et ont peut-être été créés par des polluposteurs





3. Choisir prudemment ses applications

N'achetez ou ne téléchargez des applis qu'à partir de la boutique d'applications de votre téléphone intelligent.

Avant de télécharger une application, lisez des évaluations et faites des recherches pour vous assurer de sa légitimité.



4. Fermer une session

N'oubliez pas de vous déconnecter des comptes de médias sociaux quand vous ne les utilisez pas. Si vous ne le faites pas, vous vous exposez à des risques en matière de sécurité et de protection de la vie privée.

De plus, vous devriez toujours vous **désabonner des comptes et des applications que vous n'utilisez plus et les désactiver**. Les comptes inactifs risquent d'être piratés; ce qui peut vous exposer à des vols d'identité.

Par exemple, un criminel a communiqué avec des adolescents en ligne en utilisant le compte Facebook inactif piraté d'un jeune de Calgary.



5. Mettre de l'ordre dans sa vie numérique

Tous les trois à six mois, prévoyez un moment pour vérifier vos paramètres de confidentialité et vos autorisations, modifier vos mots de passe, épurer vos listes d'amis et désactiver les comptes que vous n'utilisez plus.

Se protéger contre le vol d'identité

Dans ce monde numérique, les risques de vol de renseignements personnels pour utilisation à des fins criminelles (vol d'identité, fraude) augmentent sans cesse. Vous devriez prendre des précautions pour vous protéger.

- **Le vol d'identité** consiste à acquérir les données personnelles de quelqu'un à des fins criminelles.
- **La fraude d'identité** désigne l'usage trompeur de l'identité de quelqu'un.

Quelles sont les répercussions possibles du vol et de la fraude d'identité sur les victimes?

- Effets négatifs sur le dossier de crédit
- Refus de crédit (hypothèques, prêts)
- Usurpation d'identité (casier judiciaire)

Quels renseignements les cybercriminels recherchent-ils?

- Nom complet
- Date de naissance
- Numéro d'assurance sociale
- Adresse complète du domicile
- Nom de jeune fille de la mère
- Nom d'utilisateur et mot de passe
- Numéro de permis de conduire
- Numéros de comptes bancaires
- Numéros d'identification personnels (NIP)
- Coordonnées de carte de crédit
- Signature
- Numéro de passeport



1. Arnaques courantes pour le vol d'identité

- **Courriels/textos de hameçonnage** : Tentative d'accéder à des renseignements confidentiels en envoyant des courriels/messages illégitimes semblant provenir d'organisations reconnues. L'objectif consiste à amener les destinataires à cliquer sur des liens ou à répondre au courriel en fournissant des renseignements personnels.
- **Détournement de domaine** : Technique consistant à changer le nom de domaine d'un site web légitime, pour vous rediriger vers un site frauduleux, où vos renseignements, n'étant pas sécurisés, pourraient être utilisés à des fins illicites.
- **Vol de formulaire ou « formjacking »** : Situation où des renseignements transmis dans un formulaire en ligne (des renseignements personnels comme le numéro de carte de crédit) sont interceptés avant d'être soumis au site web.

Les escroqueries par courriel sont de plus en plus répandues et sophistiquées. Regardez cette vidéo TELUS Averti sur la façon de les repérer.

<https://bit.ly/2yS9MMu>





2. Indices de vol d'identité :

De nombreuses victimes de vol d'identité ne se rendent pas compte que cela leur est arrivé. Elles peuvent parfois le découvrir seulement lorsqu'on leur refuse le crédit malgré un bon historique.

Voici des indices à surveiller :

- Transactions ou frais inhabituels dans vos relevés bancaires ou de carte de crédit
- Avis provenant de votre institution financière au sujet de modifications dans votre compte
- Interruption des courriels ou des relevés que vous recevez habituellement ou réception de nouveaux relevés de comptes que vous ne possédez pas
- Appels de créanciers au sujet de comptes et de prêts qui vous sont étrangers
- Mystérieuses activités dans votre rapport de crédit, comme des enquêtes de crédit ou des demandes de nouveaux comptes.



3. Limitez le risque de vol d'identité en suivant ces conseils

- Utilisez des **mots de passe difficiles à deviner et l'authentification à deux facteurs**. Ne divulguez pas vos mots de passe, changez-les souvent. N'utilisez pas le même mot de passe pour tous vos comptes.
- Créez une **adresse de courriel distincte pour les sujets financiers**.
- **Effacez les données de votre appareil** avant de le vendre ou de le recycler.
- **Examinez attentivement les courriels non sollicités** où l'on vous demande de fournir ou de confirmer des renseignements personnels. Méfiez-vous des courriels (et des appels) qui vous annoncent que vous avez gagné un prix ou qui sollicitent un soutien financier.
- **Limitez les renseignements personnels et confidentiels fournis en ligne**.
- **Vérifiez toujours si vous êtes sur un site web sécurisé** avant de fournir de l'information bancaire ou sur les paiements.
- **Lorsque vous utilisez une connexion de réseau Wi-Fi public, contentez-vous de naviguer sur le web**.
- Créez une alerte **Google liée** à votre nom.

Autres mesures à prendre pour **protéger votre identité hors ligne** :

- vider votre boîte de réception régulièrement.
- protéger votre NIP bancaire en vous assurant que personne n'essaie de le voir lorsque vous l'entrez dans un guichet ou en faisant des achats.
- déchiqueter tout document dont vous n'avez plus besoin **et qui contient des renseignements personnels**.



4. Que faire si vous êtes victime de vol ou de fraude d'identité?

Étape 1 : Communiquez avec le service de police de votre quartier pour remplir un rapport.

Étape 2 : Communiquez avec votre institution bancaire ou financière et avec la société émettrice de votre carte de crédit pour signaler le vol.

Étape 3 : Communiquez avec les deux agences nationales d'évaluation du crédit pour qu'un avis de fraude soit inscrit à votre dossier et demandez une copie de vos rapports de crédit

- Equifax Canada, numéro sans frais :
1-800-465-7166
- TransUnion Canada, numéro sans frais :
1-877-525-3823

Étape 4 : Signalez le vol ou la fraude au service de police de votre quartier et avisez le Centre antifraude du Canada au 1-888-495-8501

antifraudcentre-centreantifraude.ca

Vous trouverez d'autres informations sur le site web de la GRC (<http://www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-fra.htm>)



Rencontres en ligne

De plus en plus, les aînés canadiens cherchent des compagnons ou même un nouveau ou une nouvelle partenaire de vie sur les sites et les applications de rencontre en ligne. Ce n'est peut-être pas le cas pour tous les aînés célibataires, mais ceux qui cherchent l'amour en ligne devraient se méfier des escroqueries amoureuses répandues sur le web. Ils devraient porter très attention à la protection de leur vie privée et à leur sécurité.



1. Créer un deuxième compte de courriel

Nous vous avons déjà conseillé de créer un compte de courriel distinct pour les médias sociaux, les jeux, etc. Il est recommandé de vous servir de ce compte lorsque vous vous inscrivez à un site web de rencontre.



2. Choisir des sites web sans danger

De nombreux sites web de rencontre classiques, comme **eHarmony**, répondent maintenant aux besoins des plus de 55 ans. Il en existe également d'autres qui s'adressent tout particulièrement aux personnes âgées, comme **Senior Friend Finder**, **Senior Match** et **OurTime**.



3. Vérifier les conditions d'utilisation des sites web

Lisez les petits caractères avant de vous inscrire. S'il y a une période gratuite, inscrivez un rappel dans votre calendrier pour que vous puissiez décider, à la fin de cette période, si vous souhaitez continuer d'utiliser le service ou non. Parfois, les essais gratuits se renouvellent automatiquement et des frais inattendus pourraient vous être facturés.



4. Créer un profil attrayant

L'honnêteté est la meilleure politique qui soit. Assurez-vous que votre profil soit à jour et exact. Faites tout de même attention de ne pas fournir trop de renseignements personnels, comme votre date de naissance exacte.



5. Faire preuve de prudence si l'on donne rendez-vous à quelqu'un

Si vous avez fait une rencontre en ligne et que vous avez envie de prendre rendez-vous avec cette personne, choisissez toujours un endroit public. N'oubliez pas que vous ne l'avez pas encore vraiment rencontrée et que vous ne pouvez pas savoir avec certitude à qui vous avez affaire. Vous devez donc être conscients des risques. Fiez-vous toujours à votre intuition.



6. Se méfier des escroqueries amoureuses

Voici certains signes pouvant indiquer que vous êtes en train de vous faire charmer par un fraudeur ou une fraudeuse :

- la personne prétend qu'elle habite non loin de chez vous, mais qu'elle est actuellement à l'étranger
- elle annule des rendez-vous par clavardage vidéo ou en personne
- elle vous déclare son amour très vite, avant même une rencontre en personne
- elle vous demande de lui envoyer de l'argent pour la dépanner dans une situation urgente ou pour payer ses frais de voyage pour venir vous voir

N'envoyez jamais d'argent, en aucun cas, à quelqu'un que vous avez rencontré en ligne.

Centre antifraude du Canada, plus de 22 M\$ de pertes en lien avec les escroqueries amoureuses ont été signalées au Canada en 2018.



Conseils sur les jeux sociaux

La popularité des jeux en ligne permettant l'interaction sociale entre les joueurs ne cesse d'augmenter.



1. Bien réfléchir avant de partager sa liste de contacts ou d'amis avec cette application.

Souvent, les développeurs de l'application ou du jeu vous demanderont de leur donner accès à vos listes d'amis pour pouvoir participer au jeu. De plus, les conditions peuvent autoriser les développeurs à expédier à tous vos contacts des messages associés au jeu.



2. Clavarder avec précaution.

Lorsque vous jouez en ligne, vous avez l'occasion de clavarder avec d'autres joueurs de partout dans le monde. Prenez garde aux amitiés que vous créez en ligne et aux renseignements personnels que vous partagez. Demandez-vous bien à qui vous parlez. La personne de l'autre côté de l'écran n'est pas nécessairement celle que vous croyez. En règle générale, il vaut mieux clavarder uniquement avec les gens que vous connaissez dans la vraie vie.



3. Porter attention au temps d'écran.

Comme il est possible de jouer aux jeux sociaux en déplacement, il arrive que les joueurs le fassent régulièrement et durant de longues périodes. Pour que ces jeux puissent faire partie d'une relation saine et équilibrée avec la technologie, il importe de prendre des pauses et de consacrer du temps à d'autres activités hors ligne.





4. Prendre garde à la cyberintimidation.

Même si de nombreuses personnes vivent une expérience positive avec les jeux sociaux, il est bon de savoir comment réagir si les choses s'enveniment. Malheureusement, en raison de la nature de plusieurs jeux sociaux, vous pourriez être victime de cyberintimidation. En cas de harcèlement, signalez ce comportement au réseau social et bloquez l'utilisateur concerné.

Voici quelques conseils additionnels :

1. Prenez garde à ce sur quoi vous cliquez. Certains achats que vous faites dans les applications ou sur les sites de jeu peuvent **coûter de l'argent!**
2. Prendre garde à la **promotion**. Certains jeux publicitaires sont conçus pour promouvoir et vendre un produit.

Mon plan d'action

Indiquez de 1 à 3 choses que vous ferez différemment après l'atelier d'aujourd'hui.

•

•

•

Centre de formation TELUS

Obtenez du soutien direct pour vos appareils mobiles.

Les représentants du Centre de formation TELUS^{MD} peuvent vous montrer à tirer le maximum de votre téléphone intelligent ou de votre tablette. Réservez une séance individuelle gratuite dans un Centre de formation TELUS. Trouvez-en un près de chez vous en consultant **telus.com/formation**.



En savoir plus sur la sécurité dans le monde numérique.

- Réservez un atelier TELUS Averti à **telus.com/averti**
- Écrivez-nous à **averti@telus.com**
- Joignez-vous à la conversation en ligne à **#TELUSAverti**