



TELUS AVERTI Or



Guide pour aider les aînés canadiens
à naviguer dans un monde numérique

Table des matières

Introduction.....1

À quel point êtes-vous connecté?.....2

Conseils de sécurité généraux sur
Internet et les téléphones intelligents.....4

1. Création de mots de passe sécuritaires4

2. Mises à niveau logicielles de vos appareils.....5

3. Création d'une alerte Google liée à votre nom.....7

4. Maîtrise du navigateur7

5. Prudence par rapport aux renseignements
personnels communiqués en ligne.....8

6. Réfléchir avant de cliquer9

7. Magasinage en ligne10

8. Prise et publication de photos.....11

Conseil de sécurité pour les
téléphones intelligents.....12

1. Désactivez les balises GPS12

2. Installez ou activez un logiciel de localisation,
de verrouillage et de suppression des données
à distance13

3. Soyez prudent lorsque vous utilisez un réseau
Wi-Fi gratuit dans un lieu public13

4. Effacez le contenu de votre appareil avant de
le recycler ou de le donner15

5. GPS.....15

Conseils de sécurité pour les réseaux
sociaux.....16

1. Gardez un oeil sur vos autorisations.....17

2. Consultez vos paramètres de confidentialité17

3. Réfléchissez bien avant de communiquer ou
de publier quelque chose.....18

4. Choisissez prudemment vos applications18

5. Pensez à vous déconnecter19

6. Mettez de l'ordre dans vos profils numériques ...19

Protégez-vous contre le vol d'identité.....20

- Les cyberfraudeurs trouvent leurs victimes sur
Internet sans trop d'efforts.21

- Protéger votre vie privée et vos renseignements
personnels en ligne19

Rencontres en ligne.....23

1. Créez un compte de courriel séparé23

2. Choisissez un site web approprié.....23

3. Lisez les modalités et les conditions
des sites web23

4. Créez un profil intéressant.....24

5. Soyez prudent si vous prévoyez une rencontre ..24

Jeux sociaux.....25

Ressources additionnelles.....27

Comment participer au programme
TELUS AVERTI.....30



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 et de cahier d'exercices aux participants des ateliers TELUS AVERTI Or qui sont organisés un peu partout au pays.

Si vous souhaitez organiser un tel atelier pour votre groupe communautaire, veuillez communiquer avec nous à **averti@telus.com**. Tous les éléments du programme sont gratuits et offerts à tous les Canadiens.

Pour obtenir des ressources supplémentaires, **visitez telus.com/averti**. Pour recevoir une copie électronique de ce guide, visitez **telus.com/averti**. Si vous avez des questions, n'hésitez pas à nous les envoyer par courriel à **averti@telus.com**.



À quel point êtes-vous connecté?

Prenez quelques instants pour évaluer votre présence en ligne.

Utilisez-vous ce qui suit?

Courriel ☐ Oui ☐ Non

Twitter ☐ Oui ☐ Non

Facebook ☐ Oui ☐ Non

Instagram ☐ Oui ☐ Non

YouTube ☐ Oui ☐ Non

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

Téléchargez-vous des applis (p. ex. jeux, cartes)

sur votre ordinateur, votre tablette ou votre
téléphone intelligent? ☐ Oui ☐ Non

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

Magasinez-vous en ligne? ☐ Oui ☐ Non

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

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

Jouez-vous en ligne avec

d'autres personnes (jeux sociaux)? ☐ Oui ☐ Non

Utilisez-vous **Internet pour effectuer des**

recherches (p. ex. voyage, soins de santé)? ☐ Oui ☐ Non

Additionnez maintenant vos comptes de courriel, de réseaux sociaux (p. ex. Twitter, Facebook, Instagram), d'institutions bancaires en ligne et de magasinage en ligne, ainsi que les applications mobiles que vous utilisez.

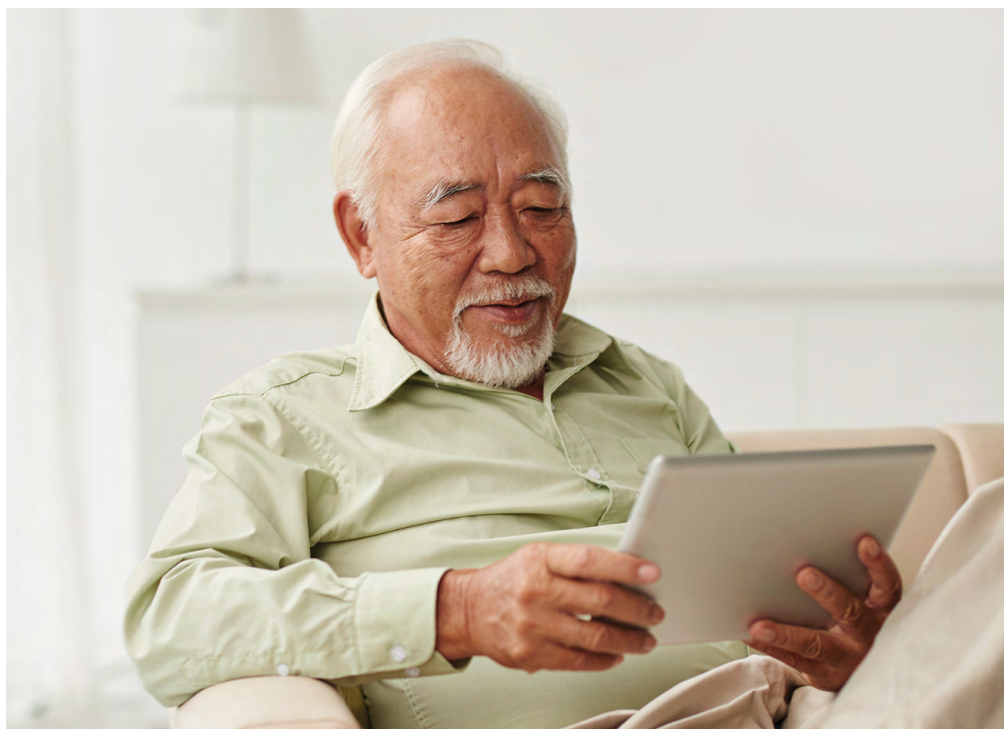
Combien en avez-vous?.....Inscrivez votre total ici :

Combien d'appareils pouvant accéder à Internet utilisez-vous? Calculez les téléphones intelligents, les ordinateurs de bureau et portatifs, les tablettes, les consoles de jeux vidéo et les iPod.

Combien en avez-vous?.....Inscrivez votre total ici :

Même si vous n'avez qu'un compte de courriel et que vous vous contentez de naviguer sur le web, **vous êtes connecté et vous faites partie d'une société numérique** qui progresse à toute vitesse.

Dans ce guide, nous vous donnerons notamment des conseils pour vous aider à protéger votre vie privée et votre identité.



Conseils de sécurité généraux sur Internet et les téléphones intelligents



1. Création de mots de passe sécuritaires

Un bon mot de passe peut empêcher les gens de pirater vos comptes de courriel ou de réseaux sociaux, par exemple. **Un bon mot de passe comprend au moins huit caractères, dont des chiffres, des lettres et des symboles.**

Vous pouvez rendre votre mot de passe plus sécuritaire en utilisant les premières lettres d'une phrase au lieu d'un mot. Par ex. **JMSTDMMDP2*** pour « Je me souviens toujours de mon mot de passe 2* ».

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).

Voici les six pires mots de passe de 2016, selon SplashData : qui publie annuellement une liste des pires mots de passe

1. 123456
2. password
3. 12345
4. 12345678
5. football
6. qwerty

Visit goo.gl/teu0vJ for the full list.



2. Mises à niveau logicielles de vos appareils

Notes

Pour protéger votre téléphone intelligent, votre tablette ou votre ordinateur des virus, il faut accepter les mises à niveaux 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. BlackBerry, 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.

Il en va de même pour **votre ordinateur**, toutes les mises à jour logicielles doivent provenir du fabricant du logiciel. Par exemple, Microsoft et Apple gèrent la majorité des correctifs de vos appareils.



Se protéger des demandes de mises à jour logicielles illégitimes.

Les fausses mises à jour logicielles, même si elles semblent légitimes, peuvent causer beaucoup de dommages si vous cliquez dessus. **Rappelez-vous de toujours prendre une pause et de bien regarder de quoi il s'agit. Dans le doute, ne la téléchargez pas.**

- Ne répondez pas aux demandes de mise à jour logicielle lorsque vous êtes sur un point d'accès **Wi-Fi public** ou lorsque vous **navigatez sur un média gratuit (comme les nouvelles) ou sur un site de téléchargement**.
- Dans le doute, **téléchargez les mises à jour dont vous avez besoin directement** à partir du site web du fabricant du logiciel (p. ex. Microsoft, Apple).
- **Ne cliquez jamais sur les liens** dans les courriels qui vous demandent de mettre à jour votre logiciel.
- Habituez-vous à **examiner attentivement les demandes de mise à jour logicielle**, particulièrement si elles semblent venir de nulle part. Vérifiez s'il y a des fautes de grammaire et d'orthographe.
- Configurez votre ordinateur pour qu'il **mette automatiquement à jour votre système d'exploitation** et vos applications.
- **Placez votre curseur au-dessus des liens.** La meilleure façon de déterminer si un courriel est valide ou non consiste à simplement placer le curseur de votre souris sur les liens suspects. Vous pourrez ainsi voir si le courriel provient d'un domaine reconnaissable lié au nom de l'expéditeur. La première partie de l'adresse (URL) est le « nom de domaine » (après le http:// et le sous-domaine). De nombreux polluposteurs exploitent le nom de domaine lorsqu'ils essaient de vous faire cliquer sur un lien malveillant.





3. Création d'une alerte Google liée à votre nom

Allez à google.com/alerts.

Entrez votre nom dans le champ de recherche pour voir le contenu associé à votre nom. Vous pouvez préciser la recherche en ajoutant la province ou la ville où vous habitez.

Si vous avez un compte Google, vous pouvez créer une alerte Google permanente liée à votre nom. Vous recevrez alors des alertes Google par courriel chaque fois que votre nom apparaîtra en ligne. Ce n'est pas une garantie totale, mais c'est un bon départ pour suivre votre empreinte numérique et détecter rapidement les vols d'identité, etc.

Visitez <https://goo.gl/Kh01N4> pour trouver de l'information sur la façon de créer des alertes Google.



4. Maîtrise du 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. Assurez-vous d'avoir installé la version la plus récente du navigateur et que celui-ci est configuré pour fournir le bon niveau de sécurité et de confidentialité.

Assurez-vous aussi de nettoyer votre historique de navigation et votre mémoire cache une fois par mois.

Visitez <https://goo.gl/Q0cMuZ> pour apprendre comment supprimer l'historique de votre navigateur. Vous y trouverez de l'information concernant les navigateurs web les plus populaires.



5. Prudence par rapport aux renseignements personnels communiqués en ligne

Pour limiter **la quantité des renseignements potentiellement confidentiels à votre sujet** et pour réduire les **risques de vol ou d'abus**, pensez-y bien avant de publier :

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

Lorsqu'on vous demande des renseignements personnels en ligne, **posez-vous les questions suivantes** :

1. À quel effet ces renseignements seront-ils utilisés?
2. Pourquoi ont-ils besoin de ces renseignements?
3. Qui aura accès à ces renseignements?

Comment ces renseignements seront-ils protégés?
N'oubliez pas qu'il s'agit de VOS renseignements.

Créez un compte de courriel séparé pour les activités en ligne (p. ex. Gmail) autres que vos communications avec votre famille et vos amis. Ainsi, si le compte de courriel que vous utilisez pour vos activités en ligne est compromis, votre compte de courriel personnel restera intact.



6. Réfléchir avant de cliquer

Notes

- **Ne cliquez jamais sur une pièce jointe ou sur un lien suspect**, même s'il semble intéressant. Les liens, les pièces jointes et les applications indésirables sont à l'origine de beaucoup d'escroqueries (comme l'hameçonnage) et de problèmes causés par des logiciels malveillants sur les réseaux sociaux.
- **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 ou les banques **ne** communiqueront **pas** avec vous pour vous demander de fournir ou de vérifier vos renseignements personnels par des moyens non sûrs comme le courriel.
- **Si vous avez des doutes ou que cela semble être trop beau pour être vrai**, c'est probablement le cas, alors prenez le téléphone et appelez directement votre fournisseur de services ou votre institution financière pour vérifier la validité de l'offre ou de la demande de renseignements sur votre compte.
- **Examinez bien vos relevés mensuels** dès que vous les recevez pour vous assurer que toutes les transactions qui y figurent sont authentiques et que toutes les transactions prévues y figurent aussi.
- **Microsoft ou d'autres entreprises** ne vous appelleront pas pour vous dire que vous avez un problème lié à votre ordinateur. Comment pourraient-ils le savoir si vous n'avez pas communiqué avec eux? Nous vous conseillons de raccrocher le plus rapidement possible. N'acceptez pas de visiter un site web que la personne au téléphone vous propose pour vous aider à réparer votre ordinateur; c'est une arnaque!!



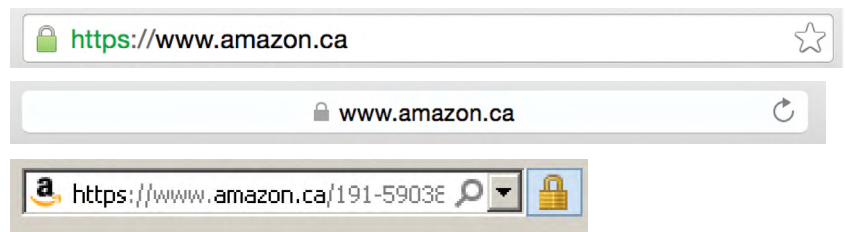


7. Magasinage en ligne

Essayez d'utiliser des sites web réputés pour votre magasinage en ligne. Consultez vos amis ou des références en ligne (non affiliées au site) pour connaître la réputation de l'entreprise.

Ensuite, assurez-vous que le site auquel vous fournissez les renseignements de votre carte de crédit chiffre vos données. **Vérifiez si l'adresse HTTP se termine par un « S » ou si la barre d'adresse comporte l'icône d'un cadenas indiquant que le chiffrement est utilisé.**

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.



Aussi, lorsque vous magasinez en ligne, **n'acceptez pas que votre ordinateur ou un autre appareil électronique se souvienne de votre mot de passe.** Refusez toujours cette option.



8. Prise et publication de photos

Notes

Nous aimons en général prendre des photos et les envoyer à nos parents et amis. Toutefois, il faut tenir compte de certaines choses avant de prendre et de publier des photos en ligne.

- **Demandez toujours aux gens leur permission** avant de prendre et de publier leur photo. Et assurez-vous que l'on vous demande aussi la vôtre avant de prendre et de publier votre photo. Cela s'applique aussi aux petits-enfants et aux enfants qui vous entourent; demandez d'abord la permission à leurs parents avant de publier une photo dans laquelle ils figurent.
- **Assurez-vous que les balises GPS sont désactivées** sur votre appareil (p. ex. votre téléphone intelligent) ou dans l'application p. ex. Instagram) lorsque vous prenez des photos et les publiez. Reportez-vous au conseil n° 1 dans la section suivante pour en savoir plus sur la désactivation de la fonction de géobalisateur.



Conseil de sécurité pour les téléphones intelligents



1. Désactivez les balises GPS

Désactivez les balises GPS de votre téléphone intelligent et de votre tablette, ou même celles des réseaux sociaux, comme Instagram et Facebook, pour protéger votre vie privée. Lorsqu'elles sont activées, la latitude et la longitude exactes de l'endroit où vous vous trouvez sont indiquées sur les photos ou les vidéos que vous prenez, publiez sur un réseau social ou envoyez par courriel. Les balises GPS se trouvent dans les paramètres de l'appareil photo ou de la position.

La meilleure façon d'apprendre à désactiver les balises GPS consiste à visiter google.com et à entrer dans le champ de recherche : « comment désactiver la géolocalisation sur un iPhone » ou « comment désactiver la localisation sur Instagram ».



2. Installez ou activez un logiciel de localisation, de verrouillage et de suppression des données à distance sur votre téléphone intelligent

Vous pouvez aussi installer le logiciel qui vous permet de localiser, de verrouiller ou de supprimer le contenu de votre appareil à distance en cas de perte ou de vol. Pour l'iPhone, le logiciel s'appelle **Localiser mon iPhone**, pour BlackBerry, il s'appelle **Blackberry Protect** et pour Android, cela dépend du fabricant. Pour Samsung par exemple, le logiciel s'appelle **Traçage du mobile**.

Ces programmes vous permettent même d'écrire un message à distance sur l'écran de l'appareil pour demander à la personne qui le trouve de vous rappeler, le trouve de vous rappeler.





3. Soyez prudent lorsque vous utilisez un réseau Wi-Fi gratuit dans un lieu public

Notes

Soyez vigilant lorsque vous utilisez le réseau Wi-Fi « gratuit » d'un lieu public. Ce type de réseau permet aux pirates informatiques d'accéder facilement à vos renseignements personnels. Vous courez toujours un certain risque en vous connectant à un point d'accès Wi-Fi public, Vous courez toujours un certain risque en vous connectant à un Wi-Fi public, mais vous pouvez prendre quelques mesures pour vous protéger :

- **Confirmez toujours la légitimité d'un réseau Wi-Fi** avant de vous y connecter; ne vous fiez pas au nom. S'il existe de multiples points d'accès pour le même endroit (p. ex. un café), demandez au personnel lequel vous devriez utiliser. Lisez aussi les modalités de service du lieu en question afin de vous assurer que votre vie privée reste protégée.
- Idéalement, nous vous conseillons **d'utiliser seulement les Wi-Fi publics pour consulter des sites web sur lesquels vous ne devez pas ouvrir de session** (notamment des sites web généraux). Cependant, si vous devez accéder à des données confidentielles ou entrer vos authentifiants (pour accéder à vos courriels par exemple), limitez-vous aux sites web qui commencent par HTTPS (« S » = sécurisé, soit une version plus sécurisée du protocole web HTTP standard). Cependant, même si un site web utilise le protocole HTTPS pour la majorité de son contenu, il se peut que les images de ce site web soient tout de même distribuées au moyen du protocole HTTP puisque les liens ne sont habituellement pas chiffrés. Heureusement, la plupart des navigateurs web actuels vous aviseront si le contenu du lien n'est pas sécurisé ou si le certificat d'un site HTTPS sécurisé n'est pas valide ou ne peut pas être vérifié.
- **N'installez jamais de logiciel 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 au lieu du vrai logiciel.



4. Effacez le contenu de votre appareil avant de le recycler ou de le donner

La technologie progresse très rapidement et de nouveaux appareils mobiles présentant de nouvelles caractéristiques sont offerts chaque mois. Bien des gens remplacent donc leur téléphone intelligent ou leur tablette presque chaque année.

Avez-vous déjà pensé à ce qui arrive à votre ancien appareil lorsque vous vous en débarrassez? Et surtout, ce qu'il advient de vos renseignements personnels? Lorsque vous utilisez vos appareils chaque jour pendant une longue période de temps, ceux-ci accumulent de nombreuses données très confidentielles.

Avant de vous départir de votre appareil mobile, assurez-vous donc de bien supprimer toute l'information qu'il contient.

Vous trouverez toute l'aide dont vous avez besoin au Centre de formation TELUS.
Visitez : goo.gl/g8WZJ2



5. GPS

Gérez les paramètres de localisation de vos applications en comprenant 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 vous vous trouvez?

Désactivez le GPS (ou les paramètres de localisation), le Wi-Fi et le Bluetooth lorsque vous ne les utilisez pas. Cela protégera votre vie privée et vous permettra d'économiser la pile!

Vous trouverez le GPS ou la localisation, le Wi-Fi et le Bluetooth dans la section « paramètres » ou « réglages » de votre téléphone intelligent.

Conseils de sécurité pour les réseaux sociaux

Il est très important que les autorisations et les paramètres de confidentialité des comptes de réseaux sociaux auxquels vous vous inscrivez et des applications que **vous téléchargez soient réglés selon vos besoins**. Vous devez lire attentivement les modalités concernant la confidentialité et les autorisations – ne les acceptez pas sans les lire.

- **Les autorisations déterminent** le contenu auquel il est possible ou non d'accéder ou le contenu pouvant être communiqué ou non à votre sujet (p. ex. vos listes de contacts, vos photos et autres fichiers et votre profil) sur un réseau social ou par une application mobile à laquelle vous êtes abonné.
- **Les paramètres de confidentialité** déterminent qui peut ou non voir votre profil et vos publications.

Avant de lire nos conseils, dressez la liste des réseaux sociaux (p. ex. LinkedIn, Twitter, Instagram ou Facebook) auxquels vous êtes inscrit et des applis (p. ex. météo ou cartes) que vous avez téléchargées.



1. Gardez un oeil sur vos autorisations

Chaque fois que vous téléchargez une application sur votre téléphone intelligent, votre tablette ou votre ordinateur ou que vous vous inscrivez à un nouveau réseau social, vous permettez peut-être à ses concepteurs de voir et même de prendre vos renseignements personnels, comme votre carnet d'adresses, les renseignements de votre compte Facebook ou Twitter, l'endroit où vous vous trouvez et même vos photos.





2. Consultez vos paramètres de confidentialité

Vérifiez bien quels sont les renseignements partagés publiquement – et ceux auxquels les applications ont accès. Vous communiquez peut-être plus d'information que vous ne le pensez.



3. Réfléchissez bien avant de communiquer ou de publier quelque chose

Règle générale, vous devriez seulement communiquer avec des gens que vous connaissez dans la vraie vie. En devenant « ami » avec des étrangers en ligne, vous vous exposez à des risques pour votre confidentialité et votre sécurité. Selon Facebook, 1 pour cent des 1,86 milliard de profils d'utilisateur actifs sont faux et ont peut-être été créés par des concepteurs de logiciels malveillants ou des polluposteurs. De plus, prenez garde à ce que vous publiez et communiquez. Par exemple, publier des photos de vous ou d'autres personnes dans des situations inappropriées pourrait nuire à votre carrière ou anéantir vos rêves!



4. Choisissez prudemment vos applications

N'achetez ou ne téléchargez des applis qu'à partir de la « boutique d'applications » de votre téléphone intelligent ou de votre fournisseur de services. Évitez de télécharger des applications pouvant accéder à vos données comme votre carnet d'adresses, vos photos, etc. Règle générale, avant de télécharger une application, faites une recherche pour vous assurer de sa légitimité.



5. Pensez à vous déconnecter

Ne laissez pas vos comptes de médias sociaux (p. ex. Twitter ou Instagram) ou vos applis et vos jeux (p. ex. Angry Birds) ouverts si vous ne les utilisez pas. Si vous ne fermez pas votre session, vous vous exposez à des risques pour votre sécurité et votre confidentialité.

De plus, désabonnez-vous des sites et des applications que vous n'utilisez pas. Pensez-y, un criminel a communiqué avec des adolescents en ligne en utilisant le compte Facebook d'un adolescent de Calgary qui avait cessé de s'en servir depuis longtemps parce qu'il avait déjà été piraté.



6. Mettez de l'ordre dans vos profils numériques

Tous les trois à six mois, prévoyez un moment dans votre calendrier pour que les membres de votre famille et vous procédiez à la vérification de vos paramètres de confidentialité et de vos autorisations sur les réseaux sociaux et dans les applications que vous avez téléchargées. Désabonnez-vous aussi des comptes de courriel et des applications que vous n'utilisez plus.



Protégez-vous contre le vol d'identité

Qu'est-ce que le vol d'identité?

Le vol d'identité renvoie au processus initial consistant à acquérir les données personnelles de quelqu'un à des fins criminelles.

Qu'est-ce que la fraude d'identité?

La fraude d'identité est l'usage trompeur des renseignements d'identification d'une personne relativement à différentes fraudes.

Quelles sont les répercussions potentielles sur les victimes?

- **Effets négatifs sur le dossier de crédit**
- **Refus de crédit** (hypothèques, prêts)
- **Usurpation d'identité** (les fraudeurs peuvent faire l'objet d'un casier judiciaire ou de mandats)

Quelles sont les données recherchées par les fraudeurs?

- Nom complet
- Date de naissance
- Numéro d'assurance sociale
- Adresse complète
- Nom de jeune fille de la mère
- Noms d'utilisateur et mots de passe des services en ligne
- Numéro de permis de conduire
- Numéros de comptes bancaires
- Numéros d'identification personnels (NIP)
- Données de carte de crédit
- Signature
- Numéro de passeport



À quoi servent vos renseignements personnels?

- Accéder à vos comptes bancaires
- Ouvrir de nouveaux comptes bancaires
- Virer des fonds
- Faire des demandes de prêts, de cartes de crédit ou d'autres biens et services
- Louer des voitures ou des appartements
- Camoufler des activités criminelles
- Obtenir un passeport
- Toucher des prestations du gouvernement



Les cyberfraudeurs trouvent leurs victimes en ligne sans trop d'efforts.

Voici les deux moyens les plus courants :

- **Hameçonnage** : fraude en ligne visant à soutirer les renseignements personnels et financiers d'un titulaire de compte en prétendant être une entreprise légitime.
- **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.



Voici quelques moyens de protéger votre vie privée et vos renseignements personnels en ligne

1. Effacer le contenu de l'appareil

Les ordinateurs et les téléphones intelligents renferment un éventail de renseignements que les pilleurs de données aimeraient bien avoir. Supprimer vos fichiers et vider votre corbeille ne suffisent pas : nettoyez ou effacez votre disque dur avant de vous départir de votre appareil.

2. Être attentif à ce qui se passe autour

Les épieurs regardent par-dessus l'épaule de leurs victimes pendant qu'elles entrent leur mot de passe ou leur NIP.

Vous devez :

- être attentif à ce qui se passe autour de vous et garder à l'esprit que les fraudeurs cherchent activement des occasions d'espionner par-dessus l'épaule des gens.
- bloquer vos données; masquez le clavier numérique pour que personne ne puisse voler votre NIP.

3. Porter attention aux courriels

Soyez particulièrement prudent en ce qui concerne les courriels non sollicités, y compris ceux vous annonçant que vous avez gagné un prix ou vous demandant de l'aide financière.

4. Bien gérer les mots de passe

- Choisissez des mots de passe difficiles à découvrir.
- Utilisez des mots de passe différents pour tous vos comptes.
- Changez souvent vos mots de passe et vos NIP.
- Mémorisez vos mots de passe et vos NIP.

Que faire si vous êtes victime d'un vol 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.

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

Étape 4 : Signalez toujours le vol d'identité et la fraude. Communiquez avec le Centre antifraude du Canada. Numéro sans frais : **1-888-495-8501**
antifraudcentre-centreantifraude.ca

Rencontres en ligne

1. Créez un compte de courriel séparé

Vous ne rencontrerez pas nécessairement la compagne ou le compagnon idéal du premier coup. Il est donc préférable d'avoir un compte séparé plus anonyme que celui que vous utilisez pour vos proches et vos amis.

2. Choisissez un site web approprié

La plupart des sites web de rencontre traditionnels comme **eHarmony**, offrent maintenant leurs services aux personnes de 55 ans et plus. Il existe aussi des sites web de rencontre qui s'adressent spécialement aux aînés, comme **Senior Friend Finder**, **Senior Match** et **Senior People Meet**.

3. Lisez les modalités et les conditions 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 le moment venu si vous souhaitez continuer d'utiliser le service ou non. Bien souvent, les sites web payants renouvellent automatiquement votre abonnement. Vérifiez s'il est possible de vous désinscrire.

4. Créez un profil intéressant

L'honnêteté est la meilleure politique. Votre profil sera plus populaire si vous publiez une photo; les sites web suggèrent même d'opter pour une photo sur laquelle vous êtes actif. Assurez-vous que votre profil est à jour et indiquez précisément quels sont vos intérêts et vos passe-temps. Il est difficile de parler de soi, alors demandez de l'aide à vos amis.

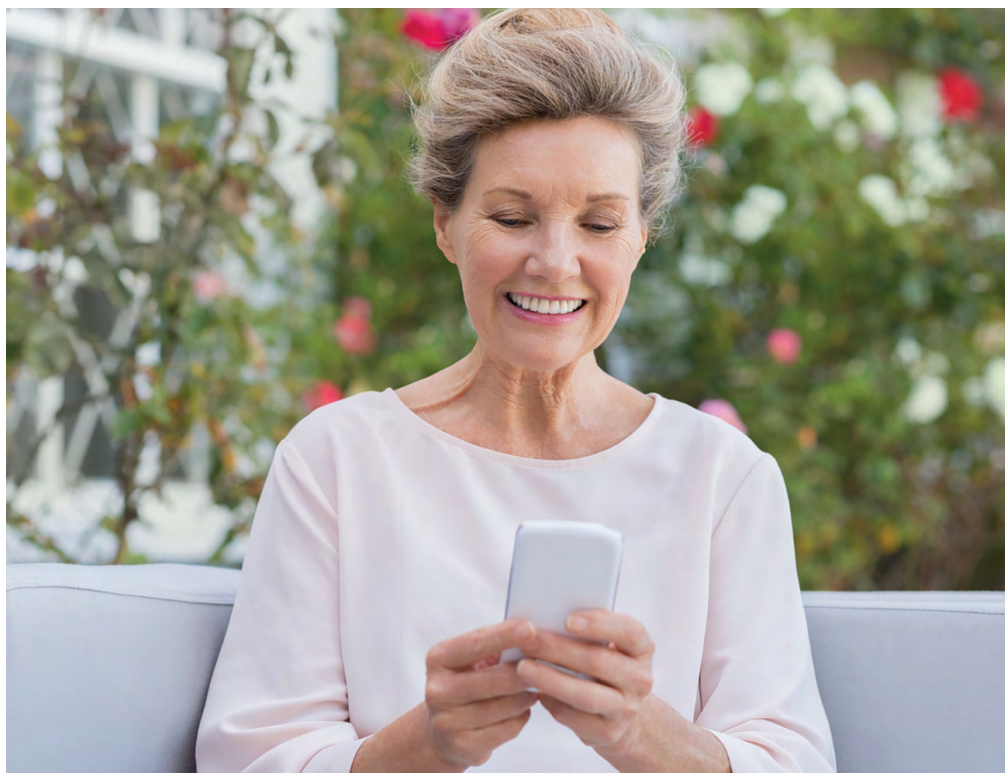
Enfin, n'indiquez pas trop de renseignements personnels, car vous pourriez ainsi divulguer votre adresse, par exemple.



5. Soyez prudent si vous prévoyez une rencontre

Si vous décidez de rencontrer quelqu'un, montrez-vous futé. Rencontrez la personne dans un endroit public et ne lui dites pas où vous habitez. Vous ne l'avez pas encore réellement rencontrée, alors soyez conscient des risques que cela pose pour votre sécurité. Écoutez votre intuition.

Source: '5 online dating tips for seniors looking for love in Canada', <http://goo.gl/RtJ98t> — en anglais seulement.



Conseils sur les jeux sociaux

Les jeux sociaux sont des jeux en ligne qui permettent des interactions entre les joueurs. Ils sont devenus très populaires, car ils donnent la possibilité de jouer sur un téléphone intelligent ou une tablette grâce à des applications ou à des réseaux sociaux, souvent gratuitement! Bien que les jeux sociaux offrent de nombreuses façons de s'amuser avec proches et amis, il faut appliquer les mêmes règles de sécurité en ligne si l'on veut réduire les risques.

Si une application que vous téléchargez vous demande accès à vos données, comme l'endroit où vous vous trouvez ou votre liste de contacts, demandez-vous pour quelles raisons elle en a besoin et quels renseignements vous vous apprêtez à lui donner.

Généralement, les joueurs sociaux jouent directement contre leurs amis ou participent au classement général de l'application ou du réseau social. La possibilité d'entrer en contact avec des gens de partout dans le monde signifie qu'il est important de savoir comment protéger sa vie privée et de faire preuve de gentillesse envers les autres joueurs.

Heureusement, la plupart des jeux et des appareils comprennent des outils de sécurité pour protéger les joueurs. Si vous jouez sur un réseau social, **apprenez comment bloquer les autres joueurs et signaler les problèmes** si vous en rencontrez. Lorsque vous clavardez ou communiquez des renseignements, assurez-vous de ne jamais donner de renseignements personnels, envoyer des photos ou accepter de rencontrer quelqu'un en personne. Pensez attentivement à la personne à laquelle vous parlez et aux renseignements que vous communiquez. Généralement, il est préférable de parler seulement aux gens que vous connaissez dans la vraie vie et de protéger vos renseignements personnels, comme votre adresse de courriel et vos mots de passe.



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 conserver un style de vie sain et équilibré tout en jouant à des jeux, ils doivent prendre de nombreuses pauses.

Les jeux sociaux et Internet font partie intégrante de la vie de bien des gens, mais pour connaître une expérience sécuritaire et positive, ils doivent se rappeler que les choses peuvent mal tourner et savoir quoi faire dans un tel cas.

Malheureusement, en raison de la nature des jeux sociaux, vous pourriez être victime de cyberintimidation. **En cas de harcèlement, signalez ce comportement au réseau social sur lequel vous jouez et bloquez l'utilisateur concerné. Soyez toujours attentif à la personne à qui vous parlez et ne divulguez pas de renseignement personnel.** Voici quelques conseils :

1. Lorsqu'une application vous demande d'accéder à vos données, comme l'endroit où vous vous trouvez, demandez-vous pourquoi.
2. Portez attention aux personnes avec lesquelles vous parlez et aux renseignements que vous leur donnez. **Ne divulguez aucun renseignement personnel** aux gens que vous connaissez seulement en ligne. Soyez prudent lorsque vous donnez rendez-vous à quelqu'un.
3. **Montrez-vous aimable et respectueux** avec tous les gens à qui vous parlez et suivez les règles du jeu.
4. **Prenez des pauses.** Il est amusant de jouer à beaucoup de jeux, mais il faut aussi faire de nombreuses pauses.
5. **Prenez garde à ce sur quoi vous cliquez**, car certaines applications peuvent coûter de l'argent!
6. Sachez que certains jeux publicitaires sont conçus pour promouvoir et vendre un produit.
7. Vérifiez les paramètres de confidentialité et les autorisations. Les applis de jeu pourraient publier des données sur vos activités dans les réseaux sociaux et inviter vos contacts à participer.



Ressources additionnelles

Voici quelques ressources additionnelles pour assurer votre sécurité en ligne :

- Visitez **telus.com/averti**
- Pour en savoir plus sur les fonctions de votre téléphone intelligent, réservez une séance individuelle avec un spécialiste d'un Centre de formation TELUS près de chez vous. Pour prendre un rendez-vous en ligne, visitez **<http://goo.gl/g8WZJ2>**.

Notes complémentaires



Comment participer au programme TELUS AVERTI

- Visitez-nous à telus.com/averti si vous avez des questions ou si vous voulez réserver une séance TELUS AVERTI en personne gratuite pour la classe de votre enfant ou votre groupe de parents.
- Vous pouvez nous joindre à averti@telus.com
- Participez à la conversation [@TELUSfr](https://twitter.com/TELUSfr) ou sur Twitter en utilisant [#TELUSAVERTI](https://twitter.com/hashtag/TELUSAVERTI)