TELUS Averti

TELUS Averti Or

Assurer votre sécurité dans le monde numérique.

telus.com/**averti**

Contenu

Introduction

Ce guide a été élaboré pour les personnes âgées qui utilisent déjà Internet et qui souhaitent en savoir plus sur la façon de participer à notre société numérique en toute sécurité.

La technologie numérique est-elle nouvelle pour vous?

Consultez telus.com/**Techno101Averti**

Conçu en partenariat avec HabiloMédias, l'atelier Techno 101 de TELUS Averti permet aux personnes qui commencent à utiliser la technologie numérique d'acquérir des compétences de base utiles au quotidien. Cette série de vidéos gratuites destinées aux personnes âgées, aux nouveaux arrivants et aux personnes qui n'ont pas grandi dans le monde numérique, traite de différents sujets : comment se connecter à Internet, utiliser un moteur de recherche, se protéger sur les médias sociaux, et bien plus encore.

Si vous souhaitez réserver un atelier TELUS Averti Or gratuit pour votre groupe communautaire, ou obtenir des ressources supplémentaires pour vous aider à assurer votre sécurité dans le monde numérique, visitez telus.com/**averti**.

Tout au long de ce guide, vous verrez une série de codes QR comme celui ci-dessous. Les codes QR vous permettent d'accéder rapidement à des sites web sans avoir à saisir ni mémoriser une adresse web. Vous pouvez utiliser l'application Appareil photo de votre téléphone pour balayer le code QR.

1. Ouvrez l'application Appareil photo depuis l'écran d'accueil, le centre de contrôle ou l'écran de verrouillage.
2. Choisissez l'appareil photo arrière. Tenez votre appareil de sorte que le code QR apparaisse dans le viseur de l'application Appareil photo. Votre appareil reconnaîtra le code QR et affichera une notification vous permettant d'accéder au site associé au code QR.
3. Appuyez sur la notification pour ouvrir le lien associé au code QR.

Essayez vous-même!

Vous protéger contre les fraudes et le vol d'identité

Dans le 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 renseignements personnels d'une personne à des fins criminelles.
- **La fraude d'identité** désigne l'usage trompeur de l'identité de quelqu'un.

Quelles sont les répercussions potentielles sur les victimes de vol d'identité et de fraude d'identité?

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

Quels sont les renseignements recherchés par les cybercriminels?

- 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
- Numéro de permis de conduire
- Numéros de compte bancaire
- Numéro d'identification personnel (NIP)
- Renseignements sur la carte de crédit
- Signature
- Numéro de passeport

1

Fraudes courantes

Les escrocs et les fraudeurs sont de plus en plus opportunistes. Voici les principales fraudes à surveiller :

Fraude sentimentale : L'escroc établit une relation virtuelle avec sa victime, lui donne beaucoup d'attention et d'affection, gagne sa confiance, puis lui demande de lui envoyer de l'argent ou de recevoir pour lui de l'argent que la victime doit ensuite lui transmettre. Ça peut sembler difficile à croire, mais les fraudes sentimentales sont bien réelles et elles fonctionnent dans bien des cas.

Cryptomonnaie : Les escrocs, qui se présentent souvent comme des professionnels de l'investissement, vous proposent d'investir dans de la cryptomonnaie et vous font miroiter un rendement élevé en peu de temps. Avant d'investir dans de la cryptomonnaie ou d'envoyer de l'argent en ligne à quiconque, effectuez des recherches et gardez à l'esprit que récupérer son argent après un envoi en ligne peut être difficile.

Faux comptes de médias sociaux : Les escrocs utilisent de faux comptes de médias sociaux pour se faire passer pour quelqu'un d'autre (ou pour une organisation) à des fins personnelles. Pour y arriver, les escrocs copient parfois la photo de profil de la victime, créent un nouveau compte Facebook ou Instagram et commencent à envoyer des messages ou des liens dangereux en se faisant passer pour quelqu'un d'autre.

Hameçonnage (courriel) et hameçonnage par message texte (texto) : Si vous êtes la cible de cette fraude, vous recevez un courriel ou un message texte de ce qui semble être une entreprise réputée ou connue vous demandant de cliquer sur un lien (qui est malveillant et installe souvent un virus ou un logiciel malveillant sur votre appareil) ou de lui fournir des renseignements personnels ou financiers. Il devient de plus en plus complexe de détecter ces messages.

Saviez-vous?

Si vous recevez un hameçonnage par message texte,transférez le message texte au code court **7726** en incluant le mot « **SPAM** » (pourriel) dans le corps du message.

Extorsion : Un escroc obtient illégalement de l'argent, des biens ou des services par la contrainte.

Mystification : La mystification est une tactique utilisée par des escrocs pour obtenir des renseignements personnels en faisant croire qu'ils représentent une source digne de confiance ou une entreprise reconnue.

Fraude des petits-enfants en situation d'urgence : Une personne âgée reçoit un appel d'une personne se faisant passer pour l'un de ses petits-enfants dans le but de gagner la confiance de la victime. La personne qui appelle prétend avoir un problème et demande à la victime de lui envoyer de l'argent sur-le-champ.

Fraudes par téléphone : Les escrocs appellent en se faisant passer pour des sociétés de services financiers ou de téléphonie, des fournisseurs d'assurance ou pour offrir un soutien technique, une aide à l'immigration ou d'autres services. Leur objectif est d'obtenir vos renseignements financiers ou d'obtenir un paiement pour des services qui ne seront pas fournis.

Numéro d'assurance sociale : Les escrocs prétendent appeler au nom d'agences gouvernementales et disent aux victimes potentielles que leur NAS a été bloqué, compromis ou suspendu. Ils demandent ensuite des renseignements personnels pour corriger le problème.

Les fraudes par courriel sont de plus en plus fréquentes et sophistiquées. **Regardez cette vidéo de TELUS Averti pour apprendre comment repérer les fraudes courantes par courriel**.

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 quelques 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 courriers 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.
- Activités douteuses dans votre dossier de crédit, notamment des enquêtes de crédit ou des demandes de création de nouveaux comptes.

3

Réduire les risques grâce à ces conseils

- Utilisez des mots de passe difficiles à deviner et l'authentification à deux facteurs. Évitez de partager vos mots de passe, modifiez-les régulièrement et n'utilisez pas le même mot de passe pour tous vos comptes.
- Utilisez une adresse de courriel distincte pour les questions financières.
- Effacez tout ce qui se trouve sur votre appareil avant de le vendre ou de le recycler.
- Évitez de partager des renseignements personnels ou privés en ligne.
- Faites preuve de discernement quant aux courriels non sollicités vous demandant de fournir ou de valider vos renseignements personnels. Méfiez-vous des courriels (et des appels) indiquant que vous avez remporté un prix ou sollicitant une aide financière.
- Vérifiez toujours que vous êtes sur un site web sécurisé avant de fournir vos renseignements bancaires ou liés au paiement.
- Contentez-vous de naviguer sur Internet lorsque vous utilisez un Wi-Fi public.

Voici des mesures supplémentaires pour protéger votre identité hors ligne :

- Relever régulièrement votre courrier.
- Protéger votre NIP bancaire, surveiller que personne ne vous observe lorsque vous le saisissez à un guichet automatique ou pendant vos achats.
- Détruire tout document sur lequel figurent des renseignements personnels dès que vous n'en avez plus besoin.

4

Que faire si vous êtes victime d'une fraude

Étape 1 : Communiquez avec votre service de police local 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 d'identité.

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 à votre service de police local et informez le Centre antifraude du Canada au **1 888 495-8501**
antifraudcentre-centreantifraude.ca

Retrouvez des renseignements supplémentaires sur les fraudes ainsi que la marche à suivre si vous êtes victime d'une fraude sur le site web du Centre antifraude du Canada à : **antifraudcentre-centreantifraude.ca**

Pour en savoir plus, consultez telus.com/**Techno101Averti** et regardez l'épisode 11 : Votre sécurité : Éviter les fraudes en ligne

Conseils de sécurité sur Internet

1

Définir des mots de passe difficiles à deviner

Un mot de passe difficile à deviner peut empêcher quelqu'un de pirater vos comptes de médias sociaux ou de courriel, entre autres. Il devrait comporter au moins **12 caractères, dont des nombres, des lettres et des symboles**.

Pour que votre mot de passe soit plus sécuritaire, vous pouvez utiliser une **phrase passe ou les premières lettres des mots de la phrase au lieu d'un seul mot**.

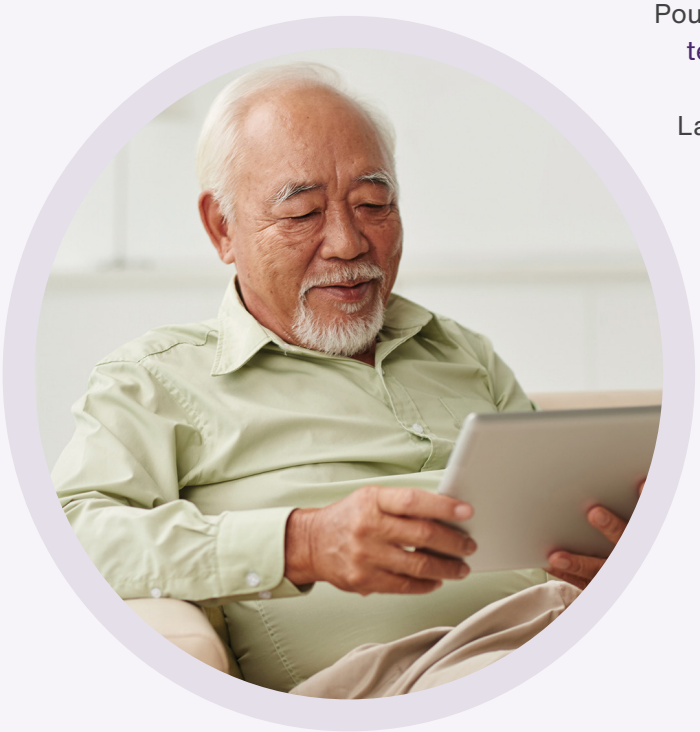
Par exemple : « Jenesaisplusoùj'aimismescléshiermaisjem'ensouviensaujourd8! » ou plus simplement JNSPOJMMCHMJMSA8!

Authentification à deux facteurs (2FA) et multifacteurs (MFA) : Cette fonction de sécurité du compte exige que vous vous authentifiiez à l'aide d'un facteur supplémentaire, en plus de votre nom d'utilisateur et de votre mot de passe, comme un code unique envoyé par message texte à votre appareil ou une vérification biométrique comme une empreinte digitale. **Il est recommandé d'activer l'authentification à deux facteurs et multifacteurs pour une sécurité optimale de tous vos comptes en ligne**.

N'utilisez pas le même mot de passe pour votre ordinateur, votre téléphone intelligent, votre compte de courriel et toutes vos applications (p. ex. compte bancaire et Facebook). **Autrement, cela facilite la vie des pirates informatiques!**

Selon Cybernews, **les 6 mots de passe les moins sécuritaires en 2023** sont :

- motdepasse
- 123456
- 123456789
- 12345
- qwerty
- qwerty123



Pour en savoir plus, consultez telus.com/**Techno101Averti** et regardez l'épisode 9 : La sécurité de vos appareils et de vos comptes : NIP et mots de passe.

2

Effectuer les mises à niveau de logiciel

Il est important d'accepter les mises à niveau de logiciel, qui comprennent des correctifs de sécurité, pour protéger votre téléphone intelligent, tablette ou ordinateur contre les virus. **Installez ces mises à niveau dès que possible pour réduire au minimum les risques auxquels vous vous exposez**.

Pour les téléphones intelligents, les fabricants (p. ex. : Apple et Android) proposent leurs propres programmes de mise à niveau de logiciel et disposent tous de gestionnaires de logiciel qui vous informent s'il existe une nouvelle version de logiciel disponible pour votre appareil ou une application sur votre appareil. Retrouvez les mises à niveau de logiciel dans l'application Réglages de vos appareils Apple ( ) et Android ( ).

De même, sur votre ordinateur, toutes les mises à niveau de logiciel doivent provenir directement du fabricant du logiciel.

Demandes de mises à niveau de logiciel non autorisées

Les mises à niveau de logiciel frauduleuses peuvent causer beaucoup de dommages si vous cliquez dessus. N'oubliez jamais de vous arrêter, de regarder de près et, **si vous avez un doute, de ne pas télécharger ni cliquer**.

- Ne cliquez pas sur les demandes de mise à niveau de logiciel lorsque vous **utilisez un Wi-Fi public**.
- Téléchargez uniquement les mises à niveau directement depuis le **site web du fabricant du logiciel** (p. ex. : Microsoft, Google et Apple).
- **Ne cliquez jamais sur des liens dans des courriels qui vous demandent de mettre à niveau votre logiciel**. Si vous avez des doutes quant à la légitimité d'un lien, passez le pointeur dessus pour voir l'adresse IP de destination. Si vous ne reconnaissez pas le site web, ne cliquez pas.
- Examinez attentivement les demandes de mise à niveau de logiciel, surtout si elles semblent être apparues de nulle part ou provenir d'un expéditeur inconnu. Regardez également s'il y a des **erreurs de grammaire et des fautes d'orthographe**.
- Configurez votre ordinateur ou votre téléphone intelligent de manière à **mettre à niveau automatiquement** votre système d'exploitation et vos applications dès que des mises à niveau sont disponiblese.

Le saviez-vous?

TELUS propose des solutions de sécurité en ligne offrant une protection tout-en-un.

3

Maintenir votre navigateur sous contrôle

Le navigateur web que vous utilisez (p. ex. : Edge, Firefox, Chrome ou Safari, etc.) est votre passerelle vers Internet et le premier rempart contre les activités malveillantes. Utilisez toujours la version la plus récente du navigateur et configurez les paramètres du navigateur en tenant compte de votre sécurité et de votre vie privée. Vous pouvez également utiliser votre navigateur en mode incognito ou navigation privée pour plus de confidentialité.

Extensions et hygiène du navigateur

Les extensions du navigateur ajoutent des fonctions à votre navigateur (p. ex. : extensions de vérification orthographique ou grammaticale) et requièrent le téléchargement de logiciels. Souvent, les extensions peuvent être malveillantes ou représenter un risque pour votre vie privée. Pour protéger votre sécurité, il est préférable d'éviter de télécharger des extensions. Si vous en téléchargez une, assurez-vous qu'elle provienne d'une source réputée, consultez les avis et prenez le temps de rechercher les informations que l'extension collectera depuis votre navigateur.

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

Effectuez une recherche sur Google.com pour obtenir des instructions spécifiques à votre navigateur (p. ex. : « Comment supprimer l'historique de navigation dans Chrome »).

4

Partager des renseignements personnels en ligne

Veillez toujours à limiter la quantité de renseignements personnels que vous partagez en ligne. Cela contribuera à protéger votre vie privée et à réduire le risque de vol d'identité et de fraude d'identité.

Réfléchissez à deux fois avant de publier les renseignements personnels suivants sur un forum public (p. ex. : profil sur un média social) :

- vos coordonnées (p. ex. : numéro de téléphone, adresse de courriel);
- votre nom complet et votre date de naissance;
- votre adresse résidentielle;
- le nom complet de vos enfants ou d'autres membres de votre famille;
- les dates et les détails de vos voyages, de vos vacances et des périodes que vous passez loin de chez vous.

Réfléchissez également à deux fois avant de répondre à des questionnaires en ligne sur des médias sociaux. Les informations que vous partagez à votre propos par le biais de ces questionnaires peuvent révéler les réponses à des questions de sécurité liées à vos comptes en ligne.

Avant de partager une quelconque information en ligne, demandez-vous toujours :

1. Comment mes renseignements seront-ils utilisés?
2. Pourquoi ces renseignements sont-ils nécessaires?
3. Qui aura accès à mes renseignements?
4. Comment mes renseignements personnels seront-ils protégés?

5

Réfléchir avant de cliquer

- **Ne cliquez jamais sur des liens ou des pièces jointes de courriel qui vous semblent suspects**, aussi intéressants puissent-ils sembler. Plusieurs escroqueries et logiciels malveillants se propagent par le biais de liens, de pièces jointes et d'applications frauduleuses.
- **Ne répondez pas aux courriels vous demandant des informations personnelles ou financières**, surtout à ceux qui emploient des tactiques de pression ou exploitent la peur.
- Les fournisseurs de services légitimes comme TELUS, l'Agence du revenu du Canada, les banques, etc. **ne vous demanderont jamais de fournir ou de vérifier des informations sensibles par des moyens non sécurisés comme le courriel**.
- Apple, Microsoft, Google et d'autres entreprises réputées **ne vous appelleront jamais pour vous dire qu'il y a un problème avec votre ordinateur** ou votre appareil. Ne vous rendez pas sur un site web qui vous est fourni par un interlocuteur afin de vous aider à réparer votre ordinateur, c'est une fraude!
- **Si c'est trop beau pour être vrai... c'est probablement trop beau pour être vrai!** Si vous recevez une offre par courriel suspecte, appelez directement votre fournisseur de services ou votre institution financière pour vérifier l'offre ou la demande d'informations sur le compte. **Ne composez jamais le numéro figurant dans le courriel de l'offre**.

Conseil TELUS Averti :
Créez un compte de courriel pour les médias sociaux, les jeux en ligne, les concours, les bulletins d'information, etc., et ayez un compte de courriel distinct pour des utilisations plus professionnelles comme la gestion de vos comptes en ligne, la réservation de vos voyages et la communication avec vos amis et votre famille.

6

Magasiner en ligne

Allez sur des sites web réputés pour magasiner en ligne et demandez à vos amis et à votre famille s'ils connaissent ces sites ou lisez des avis en ligne (non affiliés au site) pour avoir une idée de leur réputation.

Assurez-vous que le site web utilise le chiffrement. Vérifiez la présence du « s » dans la partie « http » tout à gauche dans la barre d'adresse ainsi que la présence du **symbole de cadenas**. Ces deux éléments indiquent que le site web utilise le chiffrement pour protéger vos renseignements liés au paiement.

À titre d'exemple, voici l'adresse web d'Amazon.ca ci-dessous. Elle commence par **https://** et comporte également un cadenas dans la barre d'adresse du site web.

Refusez systématiquement l'option d'enregistrer vos renseignements de carte de crédit pour des achats ultérieurs. Bien que cela puisse être pratique lors de votre prochain achat, vos données enregistrées sont exposées à des risques en cas de violation des données de l'organisation.

Pour en savoir plus, consultez telus.com/**Techno101Averti** et regardez l'épisode 20 : Magasiner en ligne.

7

Prendre et partager des photos

Si vous partagez des photos en ligne :

- **Demandez l'autorisation avant de publier des photos d'autres personnes.** Cela s'applique également à vos petits-enfants et enfants. Assurez-vous d'avoir l'autorisation des parents avant de publier ou de partager en ligne une photo sur laquelle figure un enfant.
- **Pensez à votre public.** Ajustez les paramètres de confidentialité de vos médias sociaux de manière à restreindre votre public aux personnes avec qui vous êtes à l'aise de partager vos photos. Sinon, utilisez un service de stockage infonuagique réputé pour conserver vos photos, et créez des dossiers pour partager directement vos photos avec des personnes en particulier.

Conseil TELUS Averti : Choisissez avec soin les applications auxquelles vous accordez l'accès à votre galerie de photos. Lisez toujours les modalités afin de comprendre comment vos photos seront utilisées.

Conseils de sécurité pour téléphone intelligent et tablette

1

Configurer les services de localisation, de verrouillage et de suppression à distance

Utilisez ces services intégrés pour **verrouiller votre appareil, le localiser ou effacer à distance les informations qu'il contient s'il est perdu ou volé**. Ces services vous permettent également d'afficher à distance un message sur l'écran de l'appareil, indiquant comment vous contacter si quelqu'un trouve votre appareil, ou de faire émettre un son à votre appareil si vous l'avez simplement égaré à proximité.

Sur les appareils Apple, ce service porte le nom de **Localiser**, tandis que sur la plupart des Android, il porte le nom de **Localiser mon appareil**. Vous pouvez configurer ces services dans les paramètres de votre appareil.

2

Faire preuve de prudence lors de l'utilisation du Wi-Fi public

Les pirates informatiques peuvent accéder aux renseignements personnels d'autres utilisateurs par le biais d'un Wi-Fi public (p. ex. : dans un café) Voici quelques mesures que vous pouvez prendre pour faire réduire au minimum le risque :

- **Vérifiez toujours le réseau Wi-Fi avant de vous y connecter**, ne vous fiez pas seulement au nom du réseau. Si plusieurs réseaux Wi-Fi sont répertoriés pour un même lieu, demandez lequel utiliser à un membre du personnel. De même, prenez le temps de lire les modalités de service du lieu, afin de savoir à quoi vous vous engagez avant de vous connecter.
- Utilisez uniquement le Wi-Fi public pour **naviguer sur des sites web qui ne requièrent pas vos informations de connexion** (p. ex. : sites web généraux pour la navigation).
- **Vous ne devriez jamais installer de logiciel ou faire de mise à niveau de logiciel lorsque vous utilisez un Wi-Fi public**, car cela pourrait introduire des logiciels malveillants dans votre ordinateur. Par exemple, une attaque courante consiste à informer l'utilisateur que son navigateur utilise un logiciel obsolète et le rediriger ensuite vers un faux site web qui installera un virus sur son appareil.

3

Effacer tout ce qui se trouve sur votre téléphone avant de le recycler ou de le donner

La technologie progresse à un rythme effréné et de nombreuses personnes changent souvent de téléphone intelligent.

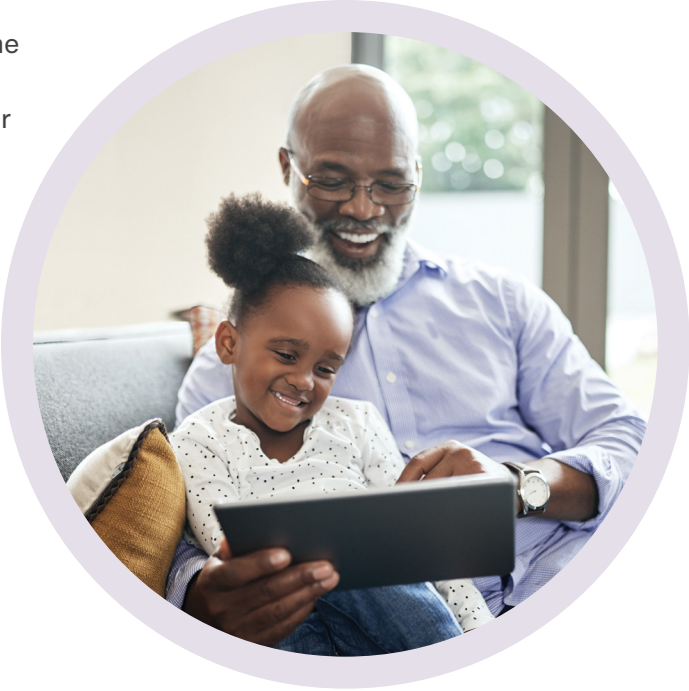
Avez-vous déjà pensé à ce qu'il advient de votre ancien appareil lorsque vous vous en débarrassez? Et surtout, à ce qu'il advient de toutes les informations privées conservées sur votre appareil, comme les coordonnées, les mots de passe et les photos?

Avant de vous débarrasser de tout appareil mobile, veillez à effacer toutes les informations qui s'y trouvent en effectuant un rétablissement des paramètres d'usine sur votre appareil.

4

Gérer les paramètres des services de localisation

Gérez les paramètres des services de localisation sur vos applications en comprenant pourquoi certaines applications requièrent votre localisation. Demandez-vous si des applications comme Facebook ou Instagram ont réellement besoin de connaître votre localisation pour fonctionner correctement?



Désactivez les services de localisation et la fonction Bluetooth lorsque vous ne les utilisez pas. Cela contribuera à protéger votre vie privée et vous permettra d'économiser de la batterie.

Retrouvez les services de localisation et la fonction Bluetooth dans la section Paramètres de votre téléphone intelligent.

5

Bien choisir ses applications

Achetez et téléchargez uniquement des applications directement depuis la boutique d'applications de votre téléphone intelligent. Avant de télécharger une application, lisez des avis et effectuez des recherches pour vous assurer que cette dernière est légitime.

Pour en savoir plus, consultez telus.com/**Techno101Averti** et regardez l'épisode 10 : La sécurité de vos appareils : Télécharger et installer des applications.

6

Désactiver le géomarquage

Bien que la plupart des sites de médias sociaux suppriment les données de géomarquage ou de localisation des photos, gardez à l'esprit que les informations de localisation demeurent associées aux images partagées par courriel ou par message texte.

Vous pouvez **désactiver le géomarquage** sur votre appareil si vous ne souhaitez pas que vos informations de localisation soient associées à vos images. Effectuez une recherche sur Google.com pour obtenir des instructions spécifiques à votre appareil (p. ex. : « Comment désactiver le géomarquage sur un iPhone »).

Conseil TELUS Averti :
Avant de publier des photos ou des vidéos en ligne, examinez-les pour vous assurer que ces dernières ne comportent pas d'informations privées que vous partageriez alors par inadvertance. Il peut s'agir de panneaux de signalisation pouvant révéler votre localisation ou de panneaux scolaires indiquant l'établissement scolaire de votre petit-enfant.

Conseils de sécurité sur les médias sociaux

1

Garder l'œil sur vos paramètres de confidentialité et vos autorisations

Prenez toujours le temps de lire les paramètres de confidentialité et les autorisations lorsque vous créez un nouveau compte sur les médias sociaux ou téléchargez une nouvelle application. N'acceptez pas les modalités aveuglément.

- Les **autorisations** définissent quelles informations personnelles peuvent être consultées et partagées par un site de réseau social ou une application mobile (p. ex. : vos listes de contacts, vos photos, votre localisation, etc.) et lesquelles sont restreintes.
- Les paramètres de confidentialité définissent qui peut ou ne peut pas voir votre profil et vos publications (p. ex. : votre profil est-il visible par vos amis uniquement ou également par le grand public?).

2

Réfléchir à deux fois avant d'établir un lien

En règle générale, vous devriez **communiquer et partager en ligne uniquement avec des personnes que vous connaissez**. En devenant « ami » avec des étrangers en ligne, vous vous exposez à des risques de confidentialité et de sécurité, à des fraudes et bien plus encore. De plus, **faites attention à ce que vous publiez en ligne**. Par exemple, publier une photo de vous en vacances peut indiquer aux autres que votre maison est vide.

Le saviez-vous?
Selon les estimations de Facebook, environ 1,3 milliard d'utilisateurs actifs sont en réalité de faux comptes, potentiellement créés par des personnes qui envoient du pourriel.

3

Se déconnecter

N’oubliez pas de vous déconnecter des sites de médias sociaux lorsque vous avez terminé. Si vous ne le faites pas, vous vous exposez à des risques de sécurité et de confidentialité.

De plus, vous devriez toujours **vous désabonner de comptes et d’applications que vous n’utilisez plus et les désactiver**. Les comptes inactifs peuvent être piratés et cela peut compromettre votre identité.

4

Mettre de l’ordre dans votre vie numérique

Tous les trois à six mois, prenez 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.

Pour en savoir plus, consultez telus.com/**Techno101Averti** et regardez :

La sécurité de vos appareils :

Épisode 11 : Éviter les fraudes en ligne
Épisode 12 : Gérer votre empreinte numérique
Épisode 13 : Vie privée sur les réseaux sociaux
Épisode 14 : Paramètres de confidentialité sur les réseaux sociaux
Épisode 15 : Prendre de bonnes décisions de confidentialité
Épisode 16 : Votre sécurité : Vie privée sur les réseaux sociaux

Sites de rencontres en ligne

Les personnes âgées utilisent de plus en plus les sites web et les applications de rencontres à la recherche de compagnie ou même d'un nouveau partenaire de vie. Les personnes en quête d'amour en ligne doivent avoir conscience des fraudes sentimentales courantes et redoubler de vigilance pour protéger leur vie privée et leur sécurité.

1

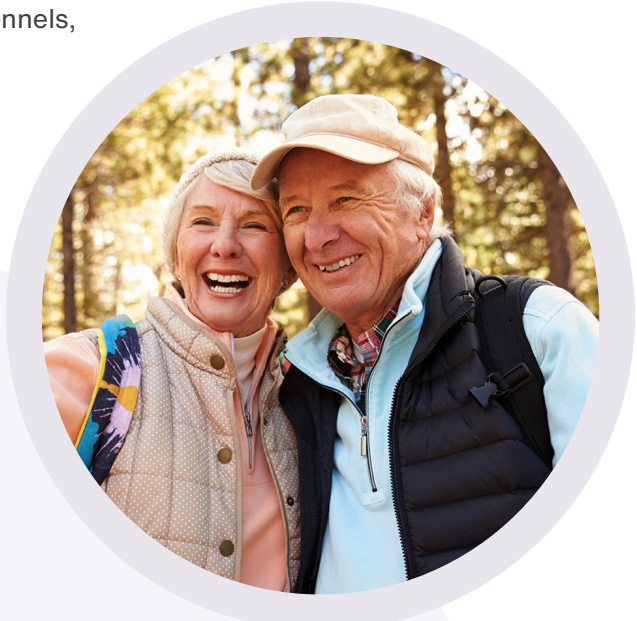
Créer un compte de courriel distinct

Dans la même lignée que le conseil prodigué précédemment quant à la création d'un compte de courriel distinct pour les réseaux sociaux, les jeux, etc., il est recommandé d'utiliser un autre compte de courriel lors de votre inscription sur un site de rencontres en ligne.

2

Choisir un site web approprié

Plusieurs sites de rencontres en ligne traditionnels, comme eHarmony, ont désormais une catégorie pour les plus de 55 ans. Il existe également des sites de rencontres en ligne spécifiquement dédiés aux personnes âgées, comme Silver Singles.



3

Rechercher les modalités de sites web

Lisez les petits caractères avant de vous inscrire. Si vous bénéficiez d'un essai gratuit, ajoutez un rappel à votre calendrier à la fin de la période d'essai, et décidez à ce moment-là si vous souhaitez conserver votre abonnement. Parfois, les essais gratuits se renouvellent automatiquement, ce qui peut entraîner des dépenses inattendues.

4

Se méfier des fraudes sentimentales

Voici quelques signes révélateurs indiquant que vous êtes la cible d'une fraude sentimentale :

- La personne dit vivre proche de chez vous, mais se trouver actuellement à l'étranger.
- La personne annule des rendez-vous de vidéoclavardage ou en personne.
- La personne vous déclare son amour rapidement avant même de vous avoir rencontré en personne.
- La personne vous demande de lui envoyer de l'argent pour l'aider à faire face à une situation d'urgence ou pour couvrir ses frais de voyage pour venir vous voir.

N'envoyez jamais d'argent, quelle que soit la situation, à une personne que vous avez rencontrée en ligne et faites preuve de prudence si vous envisagez de rencontrer quelqu'un en personne.

Selon le Centre antifraude du Canada, les fraudes sentimentales ont coûté aux Canadiens plus de 59 millions de dollars en pertes déclarées en 2022.

Conseils pour les jeux sociaux

Les jeux en ligne qui permettent l'interaction sociale entre les joueurs sont de plus en plus populaires.

1

Bien réfléchir avant de partager votre liste de contacts ou d'amis avec l'application

Souvent, les développeurs de l'application ou du jeu demanderont l'accès à vos listes d'amis pour vous permettre de jouer au jeu. De plus, les modalités peuvent autoriser les développeurs à envoyer des messages liés au jeu à vos contacts.

2

Clavarder avec prudence

De nombreux jeux offrent la possibilité de clavarder avec d'autres joueurs du monde entier. Méfiez-vous des amitiés en ligne et du partage de renseignements personnels, et réfléchissez attentivement à qui vous parlez. La personne de l'autre côté de l'écran pourrait ne pas être exactement celle que vous imaginez. De manière générale, il est préférable de clavarder uniquement avec des personnes que vous connaissez.

3

Avoir conscience du temps passé devant un écran

Pour veiller à ce que les jeux en ligne fassent partie d'une relation saine et équilibrée avec la technologie, il est important de prendre des pauses et d'équilibrer le temps passé devant un écran avec des activités hors ligne.

4

Faire attention à la cyberintimidation

Bien que la plupart des personnes aient une expérience positive liée aux jeux sociaux en ligne, il est bon de savoir quoi faire si les choses tournent mal. Si vous êtes victime de harcèlement ou d'intimidation en ligne, signalez ce comportement au réseau social et bloquez l'utilisateur.

De plus :

- Faites attention à ce sur quoi vous cliquez. Ce que vous achetez dans les applications ou sur les sites de jeu en ligne peut réellement vous coûter de l'argent!
- Attention aux publicités. Certains « publidivertissements » sont conçus pour promouvoir et vendre un produit.

Remarques

Remarques

Remarques

Agir pour les personnes âgées du pays

À TELUS, nous ne ménageons aucun effort pour que tous aient accès aux technologies et aux soins de santé de pointe grâce à nos **programmes Connectés pour l'avenir**MD.

Technologies pour l'avenir

Le programme Technologies pour l'avenirMD vise à rendre le monde en ligne accessible à tous. Il offre ainsi aux personnes handicapées l'aide spécialisée et le soutien (p. ex. des technologies d'assistance) dont elles ont besoin pour utiliser leur téléphone intelligent ou leur tablette en toute autonomie.

Mobilité pour l'avenir, Internet pour l'avenir et Santé pour l'avenir

Si vous êtes une personne âgée à faible revenu, vous pourriez être admissible à ces autres **Connectés pour l'avenir**MD :

Mobilité pour l'avenirMD

- 25 $ par mois (taxes en sus)
- 3 Go de données haute vitesse par mois et données illimitées à vitesse réduite
- Appels et textos illimités au Canada Apportez votre appareil ou profitez d'un rabais de 75 $ à l'achat du téléphone de votre choix auprès de Mobile Klinik
- Sans entente de service ni frais de résiliation

Internet for Good®

- À partir de 10 $ par mois (taxes en sus) en Colombie-Britannique, en Alberta et dans certaines régions du Québec
- Option d'acheter un ordinateur remis à neuf à bas prix
- Sans entente de service ni frais de résiliation

Santé pour l'avenirMD : pendentif d'alerte médicale

- Vivez plus sereinement en sachant qu'une assistance d'urgence en tout temps est disponible à la simple pression d'un bouton. À partir de 10 $ par mois

En savoir plus à propos des **programmes Connectés pour l'avenir**MD.

Découvrez comment mieux assurer votre sécurité dans le monde numérique.

- Réservez un atelier TELUS Averti pour votre groupe local de personnes âgées à telus.com/**averti**.
- Consultez telus.com/**AteliersTelusAverti** pour suivre l'atelier en ligne destiné aux personnes âgées.
- Consultez telus.com/**Techno101Averti** pour regarder des vidéos et apprendre les bases et les aptitudes numériques de tous les jours.

telus.com/**averti**