TELUS Averti

Conseils sur la sécurité et la protection de la vie privée en ligne.

TELUS Averti[MD] est un programme éducatif gratuit visant à donner aux Canadiens les outils nécessaires pour assurer leur sécurité dans le monde en ligne.

Sécurité d'Internet

1. **Protégez-vous :** utilisez un antivirus, un logiciel anti-espion et un coupe-feu. Et n'oubliez pas de faire une copie de sauvegarde de vos données régulièrement.
2. **Mettez à jour vos logiciels,** systèmes d'exploitation et navigateurs afin de vous protéger contre les plus récentes menaces.
3. **Choisissez des mots de passe difficiles à deviner et changez-les souvent.** Pour créer un mot de passe des plus sécuritaires, vous pouvez utiliser les premières lettres des mots d'une phrase au lieu d'un seul mot. Par exemple : JMSTDMMDP2*, pour « je me souviens toujours de mon mot de passe 2* ». Vous pouvez même utiliser une phrase complète et activer l'authentification à deux facteurs pour une sécurité accrue.
4. **Traitez les courriels avec un œil de lynx :** pièces jointes, liens suspects, demandes d'information, coquilles et fautes de grammaire, etc. Ce sont de bons indicateurs d'un courriel potentiellement nuisible.

Utilisation sécuritaire des téléphones intelligents et des tablettes

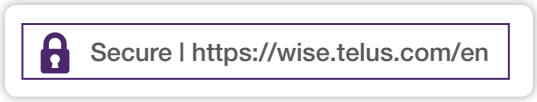
1. **Verrouillez votre téléphone :** programmez-le de manière à ce qu'il se verrouille automatiquement après une période d'inactivité. N'oubliez pas de modifier régulièrement les mots de passe.
2. **Utilisez un programme pour verrouiller et localiser l'appareil et supprimer des données :** utilisez une application qui verrouille et localise votre appareil et efface à distance l'information qu'il contient en cas de perte ou de vol, par exemple la fonction Localiser mon iPhone si vous avez un iPhone, ou l'application Localiser mon appareil sur certains appareils Android. N'oubliez pas d'effacer les données de votre appareil avant de l'échanger ou de le recycler.
3. **Faites les mises à jour** qui s'imposent pour vous protéger contre les menaces les plus récentes.
4. **Réglez les paramètres de localisation :** accordez l'accès à votre position seulement aux applications qui doivent la connaître, telles que la fonction GPS ou les applications de cartes routières. Les médias sociaux et bon nombre d'autres applications peuvent fonctionner sans connaître votre position.
5. **Méfiez-vous de l'hameçonnage par texto et examinez soigneusement vos textos.** Comme les courriels frauduleux, ces textos frauduleux visent à inciter les gens à cliquer sur des liens malveillants ou à fournir des renseignements personnels.
6. **Faites des recherches sur les applications** avant de les télécharger pour éviter d'installer des logiciels malveillants sur votre appareil.
7. **Faites preuve de prudence avec les réseaux Wi-Fi gratuits :** limitez votre activité à la navigation. Ne transmettez jamais de renseignements personnels ou financiers par réseau Wi-Fi public.
8. **Soyez conscients des risques associés à Bluetooth :** les pirates pourraient accéder aux renseignements personnels sur votre appareil muni d'une connexion Bluetooth ou établir une connexion non autorisée avec l'appareil. N'établissez des connexions qu'avec des appareils de confiance ou désactivez la fonction Bluetooth si vous n'en avez pas besoin.

Sécurité sur les médias sociaux

1. **Gardez l'œil sur les autorisations et les paramètres de confidentialité :**
   - **Les autorisations permettent** aux réseaux sociaux et aux applications que vous utilisez d'accéder à du contenu qui vous concerne personnellement et de le communiquer (p. ex. listes de contacts, photos et profil).
   - **Les paramètres de confidentialité** déterminent qui peut voir votre profil et vos publications privées.
2. **Créez une alerte Google** associée à votre nom à google.com/alerts pour être avisé par courriel lorsque votre nom apparaît en ligne.
3. **Limitez ce que vous communiquez :** le fait de communiquer trop d'information, comme votre date de naissance, votre adresse et vos plans de voyage, peut augmenter le risque.
4. **Pensez-y à deux fois avant d'établir une connexion :** n'établissez la connexion en ligne qu'avec les gens que vous connaissez.
5. **Soyez vigilant dans le choix des liens sur lesquels vous cliquez :** ne cliquez pas sur une offre qui semble trop belle pour être vraie.
6. **Désactivez la géolocalisation :** les photos prises avec la plupart des téléphones intelligents contiennent une balise géographique indiquant l'endroit exact où elles ont été prises. Désactivez cette fonction pour assurer votre vie privée lorsque vous partagez des photos en ligne.
7. **Fermez les sessions :** si vous ne fermez pas les sessions de vos comptes de médias sociaux, d'applications ou de jeux lorsque vous ne les utilisez pas, vous vous exposez à des risques en matière de sécurité et de confidentialité.
8. **Entretenez vos comptes :** 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.

Magasinage en ligne sécuritaire

1. **Vérifiez la réputation du commerce :** notez la présence d'un énoncé concernant le respect de la vie privée, d'une adresse physique, d'un numéro de téléphone et d'une politique de retour sur le site web et consultez les commentaires positifs faits par d'autres clients.
2. **Assurez-vous que le site est sécurisé :** cherchez l'image du cadenas et confirmez la présence d'un « s » dans l'URL après « http » dans la barre d'adresse.



3. **Protégez vos renseignements :** n'utilisez pas un ordinateur public ou un réseau Wi-Fi pour faire votre magasinage. Refusez toujours l'option d'enregistrement de vos renseignements de carte de crédit.
4. **Si vous payez vos achats avec votre téléphone ou votre montre,** utilisez seulement l'application fournie avec l'appareil (Apple Pay ou Android Pay).

Prenez position contre la distraction au volant

Faites de la distraction au volant un phénomène socialement inacceptable! Suivez ces conseils pour garder les mains sur le volant et les yeux sur la route :

1. Gardez votre téléphone hors de votre portée
2. Activez le mode silencieux ou éteignez l'appareil
3. Demandez au passager de s'en occuper
4. Lisez vos messages et programmez le GPS avant de partir
5. Arrêtez-vous en lieu sûr si vous devez absolument utiliser le téléphone.

Utilisation sécuritaire de l'IdO

L'IdO, ou Internet des objets, fait référence aux appareils intelligents ou connectés, tels que les systèmes de sécurité à domicile, les moniteurs pour bébé et les montres intelligentes. Ces appareils se connectent entre eux par Internet. S'ils révolutionnent bon nombre d'aspects de notre vie, ils recueillent et transmettent des données, d'où l'importance de tenir compte de ce qui suit :

1. Soyez au fait des données recueillies et de leur utilisation.
2. Gérez les paramètres de confidentialité afin que seules les données que vous acceptez de partager le soient.
3. Éteignez les appareils lorsque vous ne les utilisez pas (surtout ceux qui comprennent une caméra ou un micro).
4. Gardez les appareils IdO sur un réseau distinct « invité ». Vous protégerez ainsi votre réseau personnel contre un éventuel piratage.

La cyberintimidation, mettez-y fin et soyez au-dessus de ça en suivant ces quatre étapes :

1. Cessez la discussion et quittez l'application en ligne immédiatement; argumenter ne fera qu'envenimer les choses.
2. Bloquez tous les messages, si possible, ou encore signalez ou bloquez la personne sur la plateforme de médias sociaux.
3. Enregistrez les messages, au cas où ils seraient importants dans le cadre d'une enquête. Gardez des saisies d'écran comme preuve.
4. Parlez-en à quelqu'un et décidez de la marche à suivre. Si vous ne parvenez pas à résoudre la situation ou si vous vous sentez menacé, communiquez avec la police.

Joignez-vous au mouvement #ZéroIntimidation pour rendre notre univers numérique sécuritaire. Rendez-vous à telus.com/engagement pour prendre l'engagement de bonne conduite en ligne de TELUS Averti.

Pour en savoir plus, visitez **telus.com/averti** ou écrivez à **averti@telus.com** pour demander un atelier. Joignez-vous à la conversation en ligne à **#TELUSAverti**

Appuyé par l'Association canadienne des chefs de police, TELUS Averti a sensibilisé plus de 200 000 Canadiens au moyen de ses ressources et de ses ateliers éducatifs et informatifs.

TELUS
le futur est simple