[Marque de TELUS Averti]

[Introduction à Internet avec TELUS Averti]

[12. Gérer votre empreinte numérique]

[Un ordinateur portable et un téléphone portable apparaissent sur l'écran.]

[Voix d'une femme] : Lorsque vous visitez un site internet ou utilisez une application sur votre tablette ou téléphone intelligent…

[Des traces apparaissent sur l'écran de l'ordinateur et du téléphone portable.]

…vous laissez derrière-vous des traces de votre activité ou ce qu'on appelle une empreinte numérique.

[Un téléphone portable est en gros plan, affichant une photographie et des commentaires.]

Parfois nous savons que nous laissons ces empreintes numériques, comme quand nous partageons une photo ou un commentaire sur une publication de réseau social.

[Un point d'interrogation apparaît au-dessus du téléphone portable.]

Cependant, dans d'autre cas ce qu'un site internet ou une application sait à propos de nous une fois que nous l'utilisons, n'est pas toujours clair.

[Des traces apparaissent sur l'écran, en passant par des panneaux indiquant « Moteur de recherche », « Réseaux sociaux » et « Sites Internet ».]

En ce qui concerne l'Internet, une fois que quelque chose est en ligne, il l'est de manière permanente. Tout comme faire un pas dans du ciment frais, les empreintes que vous laissez derrière-vous, ils seront à jamais. Ce pourquoi il est important d'être prudents avec ce que vous partagez en ligne.

[Ne partagez jamais en ligne :

- Numéro de carte de crédit

- Information bancaires

- Mots de passe]

Par exemple, ne partagez jamais vos renseignements personnels, tel que le numéro de carte de crédit, informations bancaires ou mots de passe en ligne…

[Deux images du sites d'une banque et un site de confiance apparaissent sur l'écran. Chacun des deux sites à un symbole de cadenas.]

… sauf si vous êtes connectés à vos services bancaires en ligne ou que vous utilisez un site marchand auquel vous faites confiance et que vous considérez sécuritaire.

[Capture d'écran du site web Telus. Le « https » et le cadenas de la barre d'adresse sont en gros plan.]

Vous saurez qu'un site Internet est sécuritaire si son adresse web inclue « https » et non pas simplement « http » et qu'un symbole de cadenas apparaît dans la barre d'adresse.

[L'image d'une site internet générique apparaît sur l'écran. Un doigt tape sur le menu déroulant d'Utilisateur et puis sur « Se déconnecter ». Le message « Êtes-vous sur de vouloir vous déconnecter » apparaît. Le doigt tape sur « Oui ». L'écran revient à la page d'identification.]

Il est important aussi de vous assurer de vous déconnecter de vos comptes en ligne quand vous avez fini de les utiliser en particulier sur les appareils partagés, comme les ordinateurs de votre bibliothèque.

[Un ordinateur portable apparaît sur l'écran. Une page de courriel est affichée. La fenêtre est fermée sans que l'utilisateur se déconnecte. La fenêtre est ouverte encore un fois et la page d'accueil du courriel s'affiche encore une fois.]

Fermer l'onglet ou la fenêtre n'est pas suffisant. Si quelqu'un d'autre utilise le même appareil et se rend sur un page dont vous ne vous est pas déconnecté, il pourra accéder votre compte.

[La caméra de l'ordinateur portable est en gros plan.]

Vous pouvez également couvrir la caméra de vos ordinateurs portables et autres appareils quand vous ne les utilisez pas, pour réduire le risque d'accès non-autorisé.

[Une note autocollante couvre la caméra.]

Pour cela, vous pouvez utiliser une note autocollante ou quelque chose de similaire, facile à enlever quand vous souhaiterez utiliser votre caméra.

[Un micro apparaît au-dessous du portable et en dessous du téléphone portable.]

La plupart des ordinateurs et appareils portables ont aussi des micros intégrés. Vous ne pouvez pas simplement les couvrir comme c'est le cas avec votre caméra, mais il existe des solutions pour le garder en sécurité.

[Un Mac apparaît sur l'écran. Le doigt tape sur le lien Préférences Système du Mac. La fenêtre de préférences s'ouvre. Le doigt tape sur le diffuseur et puis change le réglage du volume.]

Sur un ordinateur de bureau ou portable, cliquez sur Paramètres sur un appareil Windows ou sur Préférences Système sur un Mac. Cliquez ensuite sur les réglages son et baissez le volume du micro jusqu'à zéro.

[Le doigt remonte le niveau du volume pour un appel vidéo.]

Souvenez-vous seulement que vous devrais le remonter quand vous souhaiterez utiliser à nouveau votre micro, par exemple pour un appel vidéo.

[Un téléphone portable Android apparaît sur l'écran, affichant le menu Paramètres. Le doigt tape sur Applications, puis sur les trois petits points à droite, sur le menu Gestionnaire d'autorisations et puis sur Microphone. Le doigt tape sur l'application Duolingo et change l'autorisation de « Autoriser uniquement lorsque l'appli est en cours d'utilisation » à « Refuser ».]

Sur un appareil portable, rendez-vous dans Réglages. Sur un appareil Android, tapez sur Applications, puis sur les trois petits points à droite et tapez sur autorisations.

À présent, tapez sur micro pour voir quelles applications sont autorisées à utiliser votre micro. Si vous trouvez une application qui à votre avis ne devrait pas l'utiliser, sélectionnez-la et modifiez ses réglages d'autorisation.

[Un iPhone apparaît sur l'écran, affichant le menu Réglages. Le doigt tape sur « Confidentialité », puis sur Micro. Le doigt désélectionne plusieurs applis.]

Sur un iPhone or iPad, tapez sur Confidentialiser, puis, sur micro et refusez l'accès à toutes les applications qui, selon vous, ne devraient pas utiliser votre micro.

[Le même processus est présenté pour la caméra.]

Vous pouvez faire la même chose pour votre caméra et refuser l'accès aux applications qui n'ont en pas besoin pour fonctionner.

[La page d'accueil de Google apparaît sur l'écran. Le doigt tape sur le menu Fichier, puis sur le lien Nouvelle fenêtre de navigation privée. Une fenêtre noire apparaît sur l'écran, affichant le message « Vous êtes passé en mode navigation privée ».]

Vous pouvez également contrôler ce que votre navigateur enregistre à propos de sites que vous visitez et de l'utilisation que vous en faites, en utilisant le mode de navigation incognito ou privée.

[Le même processus est présenté pour Mac. Le doigt tape sur le menu Fichier, puis sur le lien « Nouvelle fenêtre privée ».]

De cette façon, votre navigateur ne gardera aucune trace de sites que vous visitez et ne se souviendra d'aucun renseignement du compte ou mot de passe que vous entrerais.

[La page d'accueil d'Amazon apparaît. Une liste de produits consultés récemment s'affiche.]

Souvenez-vous que cet réglage n'empêche généralement pas les sites internet eux-mêmes d'enregistrer votre activité.

[Un profil en ligne, avec une photo et des renseignements apparaît sur l'écran, puis la page d'un réseau social et des messages pub personnalisés est affichée.]

Cela est important car les sites internet et les publicitaires utilisent ce qu'ils savent de vos activités en ligne pour vous créer un profil. Ils utilisent ensuite ce profil pour choisir quelle publicité vous montrer.

[Des billettes de banque et un contracte apparaissent sur l'écran, au droit du profil en ligne.]

Votre profil en ligne peut également être utilisé pour influencer tout ce que vous faites : du prix que vous payez pour des produits et services, à votre aptitude à obtenir une assurance.

[Limiter ce que les applications et sites savent de vous.]

Il existe des moyens de limiter la quantité des informations que les applications et les sites web et les entreprises qui en sont propriétaires peuvent obtenir sur vous.

[Choix de navigateur :

Firefox

Brave]

Pour commencer, vous pouvez utiliser un navigateur créé pour protéger d'avantage votre vie privée, come Firefox ou Brave. Vous pouvez aussi utiliser des extensions à cet effet :

[La page d'accueil de Google dans le navigateur Firefox apparaît sur l'écran. Le doigt tape sur le menu « Outils » et puis sur le lien « Extensions et thèmes ». L'écran se déroule. Le doigt tape sur « Découvrir davantage de modules ». La page de Firefox Add-Ons s'ouvre.]

Lex extensions sont des mini-applications qui fonctionnent avec votre navigateur. Pour trouver des extensions sur Firefox cliquez sur module complémentaire. Puis, chercher l'extension que vous souhaitez à installer.

[Le même processus est présenté pour Chrome. Le doigt tape sur le menu « Fenêtre » et puis sur le lien « Extensions ».]

Sur Chrome et Edge, cliquez sur Extensions.

[La page d'accueil du Safari s'ouvre. Le doigt tape sur le menu « Safari » et puis sur le lien « Extensions de Safari ».]

Sur Safari cliquez sur « Extensions de Safari ».

[Une page de résultats pour extensions pour « confidentialité » apparaît sur l'écran. Les extensions Disconnect Premium et Ghostery Lite sont en gros plan.]

Privacy badger, Ghostery et Disconnect sont es extensions qui empêcheront la plupart des sites internet d'enregistrer votre activité en ligne.

[Un téléphone portable apparaît sur l'écran. Les applis mobiles de Disconnect et de Ghostery sont affichées.]

Il existe également un version application mobile du Disconnect, Ghostery et d'autres, que vous pourrez télécharger pour vos appareils iOS et Android.

[Un ordinateur portable et un ordinateur de bureau apparaissent sur l'écran. Les mots « Ordinateur d'un ami » et « Ordinateur public » apparaissent au-dessous des ordinateurs.]

Si vous utilisez un ordinateur qui ne vous appartient pas, comme celui d'un ami ou un ordinateur public à la bibliothèque…

[La page d'accueil d'une bibliothèque apparaît sur l'écran. Le doigt tape sur le lien « Nouvelle fenêtre privée ».]

… utilisez toujours la navigation privée quand vous le pouvez.

[Le message « Voulez-vous que cet ordinateur se souvienne de votre mot de passe pour la prochaine fois? » est affiché sur l'écran. Le doigt tape sur « Non ».]

Si c'est impossible, assurez-vous de cliquer sur « Non » à chaque fois que le navigateur demande votre permission d'enregistrer votre compte ou mot de passe pour la prochaine fois.

[Marque de TELUS Averti]

Pour poursuivre votre introduction à Internet, consultez les autres vidéos de cette série. Visitez notre site, telus point com barre oblique techno cent un averti.

[telus.com/Techno101Averti]