[Marque de TELUS Averti]

[Introduction à Internet avec TELUS Averti]

[9. Maintenir vos appareils et comptes en sécurité : NIPs et mots de passe]

[Des images d'un ordinateur portable, d'un téléphone cellulaire et d'une tablette apparaissent à l'écran.]

[Voix d'une femme] L'étape la plus importante en ce qui concerne votre protection de vol d'identité est de vous assurer que vous soyez la seule personne à utiliser vos appareils et avoir accès à vos comptes.

[Un verrou apparaît sur tous les écrans]

Les téléphones, tablettes et certains ordinateurs peuvent être verrouillés à l'aide d'un NIP ou d'un mot de passe.

[Gros plan du téléphone cellulaire

Un mot de passe est tapé dans le champ NIP]

En général, un NIP est une suite de chiffres ....

[Gros plan de l'ordinateur portable.

Le mot « $M0tdepa$$etrèsf0rt » est tapé dans le champ du mot de passe]

... alors qu'un mot de passe est un mélange de lettres, de chiffres et de caractères spéciaux comme le signe du dollar, les points d'exclamation ou les points d'interrogation.

[Gros plan de la tablette.

« Commençons » apparaît à l'écran]

Créer un NIP ou d'un mot de passe est la première chose à faire lorsque vous utilisez un nouvel appareil. Sans quoi, n'importe qui pourrait accéder à tout son contenu.

[« Choisissez un numéro d'identification personnel » apparaît à l'écran.]

Une fois crée, vous devrez entrer votre NIP ou votre mot de passe afin d'utiliser votre appareil.

[Gros plan du téléphone portable, affichant le menu des paramètres.

Un doigt défile vers le haut dans le menu.]

Sur les appareils Apple comme les iPhones, allez dans Réglages, puis appuyez sur « Touch ID et code »

[« Tapez votre mot code » s'affiche à l'écran.

Le doigt tape six chiffres inconnus.]

« Code » signifie ici NIP.

[Les options de Code alphanumérique personnalisé, Code numérique personnalisé, Code à 4 chiffres et Annuler apparaissent à l'écran.]

On vous demandera alors de créer un NIP à six chiffres, mais vous pouvez aussi en choisir un plus court ou utiliser des lettres.

[Un téléphone Android apparaît.
Le doigt appuie sur Paramètres, puis fait défiler jusqu'à Verrouiller screen.
Les options de l'écran de verrouillage s'affichent. Le doigt appuie sur le type de verrouillage d'écran. Les options Type de verrouillage d'écran s'affichent.]

Sur les appareils Android, utilisez l'application paramètres, puis faites défiler jusqu'à « Verrouillage de l'écran ». Appuyez sur « Type de verrouillage de l'écran » et choisissez le type de verrouillage que vous désirez : un NIP, un mot de passe ou un chemin à tracer sur l'écran. Peu importe l'option que vous choisissez, pour vue que vous puissiez verrouiller votre appareil.

[L'ordinateur portable apparaît à l'écran.
Une page « S'inscrire » s'affiche.]

Vous aurez également besoin de choisir un mot de passe, lorsque vous ouvrirez un compte en ligne comme un compte courriel ou de réseaux sociales.

Souvent, on utilise des mots faciles à retenir, et on choisit le même pour différents comptes.

[Divers mots de passe simples sont tapés dans le champ de mot de passe d'une page d'inscription].

Certains des mots de passe les plus courants sont par exemple 123456, QWERTY - les six premières touches de la rangée de haut de votre clavier, 11111, le terme « mot de passe » ou une phrase courante comme « J'aime mon chien ».

Les mots de passe comme ceux-ci ne sont pas recommandés car ils sont faciles à deviner. Il arrive aussi qu'on utilise des mots de passe que toute personne nous connaissant pourrait deviner, comme le nom de notre animal de compagnie ou notre date de naissance.

Voici trois conseils pour créer des mots de passe forts :

[1. Utilisez un mélange de lettres, de chiffres et de caractères spéciaux.]

Tout d'abord, utilisez à la fois de lettres, de chiffres et de caractères spéciaux.

[Simulation d'un programme de piratage générant divers mots de passe dans le champ de mot de passe d'une page de connexion utilisateur, jusqu'à ce que le bon mot de passe soit entré.]

La plupart des pirates informatiques ou ceux qui pénètrent dans les systèmes ou les comptes d'autres individus utilisent des programmes qui testent différents mots de passe, y compris les plus communes. Puis que ce sont des programmes informatiques, ils peuvent faire ça rapidement et facilement.

Choisir un mélange de lettres, de chiffres et d'autres symboles comme des signes de ponctuation, rend ce processus plus difficile. Vous pouvez commencer avec un mot normal et remplacer certaines lettres avec des chiffres et autres caractères spéciaux comme on vous le montre ici.

[Le mot « bananes » est remplacé par « B4n4n3$"]

Utilisez des lettres majuscules et minuscules, mais ne mettez pas toujours la majuscule au début.

[2. Les mots de passe plus longs sont plus sûrs.]

Deuxièmement, choisissez un mot de passe long, ne vous limitez pas à un seul mot. Les programmes qui tentent de deviner les mots de passe passent souvent en revue tout le dictionnaire. Aussi, même si vous remplacez quelques lettres par des chiffres ou des symboles, ils peuvent quand même le deviner.

[« lesbananessontjaunes » apparaît dans le champ de mot de passe.]

Afin d'éviter cela, remplacez votre mot par une phrase. Par exemple, au lieu du « bananes » choisissez « lesbananessontjaunes» ou « J'aime les bananes ».
La plupart des mots de passe n'acceptent pas les espaces, vous devez donc écrire la phrase tout attachée comme ceci.

[Les mots « lesbananessontjaunes » se transforment en « l3sb4n4n3$$0ntjaunes »]

Ensuite, remplacez certaines lettres dans les nouveaux mots par des chiffres ou autres caractères.

[3. Utilisez différents mots de passe pour différents comptes.]

Enfin, utilisez différents mots de passe pour différents comptes et sites Internet.

[Trois sites différents apparaissent : courriel, réseaux sociaux, Banque.
Le mot « Compromis » apparaît sous chacun d'eux.]

Il arrive souvent que des sites du compagnie se fassent piratées elles-mêmes, plutôt que des comptes individuels. Dans ces cas, quand un grand nombre de données sont volées, les pirates peuvent accéder aux renseignements personnels des utilisateurs, y compris leurs mots de passe.
En utilisant toujours le même mot de passe pour différents sites, vous permettez aux pirates d'accéder à vos autres comptes.
Se souvenir de différents mots de passe pour différents sites peut être difficile.
Une solution simple est d'ajouter la première et la dernière lettre du nom du site à votre mot de passe.

[La page de connexion Facebook s'affiche. Le mot « l3sb4n4n3$$0ntj4un3S! » devient « Fl3sb4n4n3$$0ntj4un3S!k »

Par exemple, pour votre compte Facebook, vous pourriez ajouter un F avant votre mot de passe et un K à la fin, ou vous pouvez faire l'inverse.

[La page de connexion Amazon s'affiche.
Le mot de passe « Nl3sb4n4n3$$0ntj4un3S!a » est tapé dans le champ de mot de passe.]

Pour Amazon, ajoutez un N au debut du mot de passe et un a à la fin.

Vous n’avez pas à suivre cette méthode à la lettre.

[Le mot de passe devient « l3sb4n4n3aN0ntj4un3S!a »]

Vous pouvez ajouter des lettres au milieu ou les inverser, peu importe, pour vous que ce soit un système dont vous vous souviendrez.

[Le mot de passe devient « NAl3sb4n4n3$$0ntj4un3S! »]
[Une page de connexion pour courriel s’affiche. Le mot de passe « Lespommessontrouges » est tapé.]

Vous pouvez utiliser cette méthode pour tous vos mots de passe, à l’exception de votre courriel. Dans la mesure où vous utilisez votre adresse courriel pour créer la plupart de vos autres comptes, il s’agit d’un mot de passe dont la confidentialité est la plus importante.

[Le mot de passe devient « LespoMMe$$ontrouGe$! ».]

Vous pouvez utiliser la même méthode pour trouver un mot de passe, mais assurez-vous qu’il soit complètement différent de ceux de tous vos autres comptes.

[Les pages de connexion pour différents sites Web, banque et courriel apparaissent.]

À présent, vous n’avez besoin de vous souvenir que de deux mots de passe.

[Divers mots de passe forts comme ceux illustrés précédemment sont tapés dans plusieurs fenêtres de connexion.]

Celui que vous utilisez pour votre adresse courriel et l’autre que vous modifiez légèrement pour chacun de vos autres comptes.

[Un verrou et les mots « Gestionnaire de mots de passe » apparaissent à l’écran]

Une autre alternative est d’utiliser un gestionnaire de mots de passe.

[Divers mots de passe apparaissent à l’écran]

Il s’agit d’un programme qui gère les mots de passe pour différents comptes. Il crée un mot de passe différent, presque indéchiffrable pour chaque compte que vous créez, puis leur registre se charge de tous vos connexions automatiquement.

[La page d’accueil du site Web « LastPass » apparaît.]

Un gestionnaire de mots de passe populaire offrant une version gratuite de base est LastPass.

[La page des paramètres de Chrome s’affiche.]

Certains navigateurs web, comme Chrome, ont également un gestionnaire de mots de passe intégré.

[La page de connexion du gestionnaire de mots de passe s'affiche.]

Les gestionnaires de mots de passe peuvent être utiles, mais ils ne règlent que le problème d'avoir différents mots de passe pour différents comptes. Vous devez quand même vous assurer que vous créez un mot de passe fort pour le gestionnaire de mots de passe lui-même, car n'importe qu'individu pouvant l'accéder, aura accès à tous vos comptes.

[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]