Sécurité technologique Canada

Conseils de sécurité pour les ordinateurs

Une note sur la langue

Dans cette trousse, nous utiliserons parfois le mot femme et les pronoms féminins par souci de simplicité et pour reconnaître l'impact significatif de la violence facilitée par la technologie sur les femmes et les filles. Nous reconnaissons que la VFGFT a également un impact sur les personnes trans, non binaires et bispirituelles. Nous espérons que toutes les personnes touchées par la VFGFT trouveront ces documents utiles.

De nos jours, rares sont les foyers qui ne possèdent pas d'ordinateur. Les enfants s'en servent pour faire leurs devoirs et vous l'utilisez régulièrement pour vos courriels ou pour payer des factures. Au bureau, on l'allume chaque matin et on l'éteint chaque soir.

Les ordinateurs sont une technologie vulnérable que les auteurs de violence, connus ou non, peuvent exploiter pour obtenir des informations sur une femme. Si un ordinateur n'est pas aussi familier qu'un téléphone, il contient néanmoins beaucoup d'informations personnelles: courriel, historique de navigation sur le web, formulaires et documents ou informations importantes dignes de sauvegarde.

La seule façon de couper complètement l'accès à votre ordinateur est de le déconnecter du Web ou d'un autre réseau (comme un réseau domestique, non connecté à Internet) et de créer un code d'accès que vous êtes seule à connaitre. Si vous craignez que quelqu'un ne s'introduise dans votre ordinateur et que le déconnecter d'Internet ne pose pas problème, cette solution peut vous convenir. Pour la plupart des gens, cependant, la déconnexion d'Internet peut compliquer la vie de tous les jours. Que vous soyez en train de configurer un nouvel appareil ou de revoir les paramètres, voici quelques conseils de sécurité et de confidentialité.

Prévention et protection

Voici quelques moyens de minimiser les risques.

Employez une protection pare-feu

Sur la plupart des ordinateurs, tablettes et appareils mobiles, des pare-feu sont déjà installés. Les pare-feu surveillent ce qui entre et sort de l'appareil. Lorsqu'ils détectent des données suspectes, ils les empêchent de parvenir à votre ordinateur. Essentiellement, un pare-feu protège votre ordinateur du piratage par le biais de connexions compromises.

Sur la plupart des systèmes d'exploitation Windows, les protections du pare-feu sont activées par défaut. Les pare-feu des systèmes d'exploitation Mac et Linux sont désactivés par défaut et leur activation peut faire une grande différence. Pour savoir si le pare-feu est activé, vérifiez les paramètres dans le Panneau de configuration (pour le système d'exploitation Windows) ou dans Préférences système / Sécurité et confidentialité (pour les Mac).

Exécutez un antivirus générique ou spécialisé dans les logiciels espions

Pour protéger votre appareil contre les virus et les logiciels espions, vous devez installer et exécuter un antivirus. Les antivirus analysent votre ordinateur et les fichiers que vous téléchargez. S'ils détectent des virus, ils en bloquent l'installation. Certains logiciels peuvent mettre le virus en quarantaine pour l'empêcher d'infecter votre ordinateur, tandis que d'autres sont capables de le supprimer.

Les antivirus s'appuient sur les caractéristiques particulières des virus pour les détecter; toutefois, les cybercriminels les modifient constamment pour pouvoir infecter des appareils. Pour cette raison, assurez-vous d'avoir la dernière version de votre antivirus. La plupart des antivirus se mettent à jour automatiquement. Si tel n'est pas le cas, configurez votre antivirus pour qu'il le fasse.

Il existe aussi des antivirus spécialisés dans les logiciels espions (antispyware). Si vous craignez que l'auteur puisse utiliser un logiciel espion, l'exécution d'un antispyware peut être de mise.

Les antivirus et les antispyware n'empêchent pas forcément toute installation de logiciels malveillants. Cependant, ils renforcent la protection de votre ordinateur. Il en existe de nombreux qui sont gratuits pour les particuliers. Consultez les moteurs de recherche sur le «meilleur antivirus ou antispyware gratuit» pour vous assurer que ces programmes répondent à vos besoins spécifiques.

Désactiver l'accès à distance

Si vous craignez que quelqu'un accède à votre ordinateur à distance, avec ou sans votre permission, vous pouvez désactiver l'autorisation d'accès à distance. Vous pourrez toujours la réactiver au besoin.

La manière de désactiver l'accès à distance sur votre ordinateur dépend du système d'exploitation. Sur un ordinateur Windows, vous voulez activer le paramètre: «Ne pas autoriser les connexions à distance à cet ordinateur» (se trouve généralement dans le Panneau de configuration). Si vous avez un Mac, allez dans Préférences Système / Partage, et décochez «Connexion à distance» et «Gestion à distance». Le meilleur moyen de trouver des directives spécifiques à votre ordinateur est de rechercher sur Google «comment désactiver l'accès à distance à [votre système d'exploitation (par exemple, Windows 11)]».

Désactiver le partage de fichiers

Si votre ordinateur est relié à un réseau (même s'il n'est pas connecté à Internet), d'autres appareils reliés au même réseau peuvent accéder aux fichiers de votre ordinateur. Cela peut être problématique si vous êtes connectée à un réseau Wi-Fi public et que vos paramètres sont configurés pour le partage. Si vous n'avez pas besoin que quelqu'un d'autre ait accès à vos fichiers, désactivez le partage de fichiers.

La manière de désactiver le partage de fichiers dépend du système d'exploitation que vous utilisez. Le meilleur moyen est de rechercher sur Google «comment désactiver le partage de fichiers sur [votre système d'exploitation (par exemple Windows 11)]». Pour la plupart des versions de Windows, le paramètre se trouve dans le Panneau de configuration et vous devez sélectionner «désactiver le partage de fichiers et d'imprimantes». Pour un Mac, allez dans Préférences Système / Partage, et décochez «partage de fichiers» et «partage d'imprimante».

Utiliser un compte non-administrateur pour l'usage quotidien

Certains logiciels malveillants et «*hacks*» nécessitent un accès administratif à votre ordinateur. Par conséquent, si vous êtes connectée en tant qu'administrateur et que vous cliquez accidentellement sur un lien contenant un logiciel malveillant, celui-ci sera téléchargé et installé. Toutefois, si vous êtes connectée en tant que non-administrateur et que la configuration n'autorise pas un non-administrateur à installer de logiciels, celui-ci ne s'installera pas, même si vous cliquez accidentellement sur un lien contenant un logiciel malveillant.

Il est donc utile de créer un compte non-administrateur pour votre utilisation quotidienne. Vous pouvez toujours vous connecter sur le compte administrateur lorsque vous devez installer un logiciel ou apporter des modifications à votre ordinateur. Windows et Mac vous permettent tous deux de créer plusieurs utilisateurs.

Pratiques visant à renforcer la sécurité informatique

Outre les paramètres que vous pouvez activer ou désactiver et l'exécution de logiciels pour améliorer la protection, il existe d'autres bonnes pratiques qui peuvent renforcer la sécurité et la confidentialité.

Utiliser un mot de passe sur votre ordinateur

Pour empêcher quiconque d'accéder à votre contenu, commencez par verrouiller votre ordinateur avec un mot de passe. Alors que la plupart des gens craignent le piratage, le moyen le plus simple d'accéder à votre ordinateur est simplement de l'avoir à portée de main, soit à partir de chez vous ou parce qu'on vous l'a dérobé. N'oubliez pas qu'il est plus facile pour un ex-partenaire de deviner votre mot de passe et d'accéder à votre appareil.

Ne cliquez pas sur des liens provenant de personnes inconnues ou suspectes

Une autre bonne pratique consiste à ne pas cliquer sur les liens ou les pièces jointes d'origine suspecte. Ces liens ou pièces jointes peuvent parfois contenir des logiciels malveillants qui s'installent automatiquement, dès que vous cliquez. Si vous devez recevoir des fichiers ou ouvrir des liens d'une personne en qui vous n'avez pas confiance, envisagez de le faire à partir d'un service infonuagique ou trouvez une autre manière de communiquer.

Se déconnecter des comptes et quitter les programmes

Lorsque vous avez fini d'utiliser un compte, un programme ou l'ordinateur lui-même, quittez et déconnectez-vous. Si vous laissez votre ordinateur connecté, il sera plus facile pour quelqu'un d'autre d'accéder à vos comptes. Il est toujours préférable de se déconnecter lorsque vous avez terminé.

Éteindre les points d'accès lorsqu'ils ne sont pas utilisés

Désactivez l'accès Wi-Fi, Bluetooth, Airdrop ou tout autre accès de connectivité que vous n'utilisez pas. Si le point d'accès est éteint, il sera plus difficile pour quelqu'un de se connecter à distance. Vous pouvez toujours l'allumer quand vous voulez vous connecter.

La violence fondée sur le genre facilitée par la technologie (VFGFT) fait partie d'un continuum de violence qui peut se produire à la fois en ligne et en personne. Si vous ou l'une de vos connaissances faites face à la VFGFT, vous n'êtes pas seule. Vous pouvez consulter hebergementfemmes.ca pour trouver une maison d'hébergement près de chez vous afin de discuter de vos options et de créer un plan de sécurité. Vous n'avez pas besoin de résider dans une maison d'hébergement pour accéder à un soutien et à des services gratuits et confidentiels.

Ce projet est rendu possible grâce au financement du ministère Femmes et Égalité des genres Canada (FEGC).

Femmes et Égalité des genres Canada | Women and Gender Equality Canada

Canada