LA LIBERTÉ
Depuis 1913

Clinique de Cyber-Criminologie

GÉNÉRATION CYBER-SMART

COMPORTEMENTS PUBLICS ***

Qu'entendons-nous par «comportements publics» ? Bien que la plupart des enfants soient d'abord exposés à l'internet à la maison sous la surveillance de leurs parents ou tuteurs légaux, ils devront tôt ou tard accéder à l'internet en dehors de ce contexte, comme à l'école, où ils devront toujours pratiquer une cyberhygiène appropriée afin de se protéger. Cette section traite de l'étiquette entourant l'utilisation publique de l'internet, de l'utilisation des réseaux publics à la navigation sur son propre appareil en dehors de l'intimité de chez soi.

generationcybersmart.ca

Un projet rendu possible financièrement grâce à :

Secrétariat aux relations canadiennes Québec

Société de la francophonie manitobaine

QUELS SONT LES TYPES DE COMPORTEMENTS PUBLICS?

Séparons ce sujet en deux aspects différents : les appareils publics et les réseaux publics. Dans le but d'enseigner les meilleures pratiques de cyberhygiène dans le plus grand nombre de situations possible, les appareils publics désignent **tout appareil auquel vous ou votre enfant avez accès et qui n'est ni le vôtre ni le sien** - c'est-à-dire l'ordinateur sur lequel il se connecte à l'école ou à la bibliothèque publique, mais aussi le téléphone de son ami, l'iPad de sa grand-mère lorsque vous lui rendez visite, etc. Nous qualifierons même ces appareils personnels comme étant publics, car ils permettent à d'autres personnes que vous et votre enfant d'accéder à des éléments tels que l'historique de navigation, les comptes qui n'ont pas été déconnectés, etc.

De la même manière, nous ferons référence aux réseaux publics comme étant tout réseau qui n'est pas celui que vous utilisez à la maison, y compris le réseau Wi-Fi chez les amis de votre enfant ou dans un restaurant où vous allez, la connexion Bluetooth qu'ils utilisent pour se connecter aux écouteurs de leurs amis, et ainsi de suite. La raison en est que vous ne pouvez pas garantir la sécurité totale d'un réseau ou d'une connexion en dehors de votre domicile : **plus il y a de personnes capables de se connecter, plus les risques de compromission sont élevés.**

QUELS SONT LES RISQUES LIÉS À LA NAVIGATION EN LIGNE EN PUBLIC?

Différents risques peuvent découler de la navigation sur un appareil public. Qu'il s'agisse d'un appareil appartenant à une personne que vous connaissez ou simplement d'un appareil qu'un espace public vous permet d'utiliser, **l'appareil que vous utilisez peut manquer de contrôles de sécurité appropriés et permettre à des personnes non autorisées d'obtenir un accès physique au système et de compromettre potentiellement des informations sensibles stockées sur l'appareil ou dans vos comptes**. Ils peuvent également avoir été infectés par des logiciels malveillants ou compromis d'une autre manière, ce qui signifie que tout compte auquel vous vous connectez peut être détourné, ou que les données que vous avez saisies peuvent être interceptées plus facilement. Par exemple, les pirates utilisent parfois ce que l'on appelle un enregistreur de frappe, c'est-à-dire un système capable d'enregistrer les touches sur lesquelles vous tapez et ce sur quoi vous cliquez, dans l'espoir de voler votre mot de passe au moment où vous le saisissez dans le nouvel appareil. Le risque de compromission est toujours plus élevé avec les appareils partagés, comme ceux que l'on trouve à la bibliothèque ou à l'école, car davantage de personnes peuvent y accéder, et un virus téléchargé peut donc avoir été placé là intentionnellement par un pirate qui utilisait précédemment le même appareil.

L'utilisation de **réseaux publics peut également présenter divers risques de sécurité** en raison de leur nature ouverte et partagée. Si elles ne sont pas correctement sécurisées, les connexions sans fil peuvent être vulnérables à de nombreux types d'attaques au cours desquelles des personnes non autorisées ont accès à tout ce qui est envoyé ou fait à travers le réseau, ce qui peut inclure vos informations de connexion, vos données personnelles ou vos données financières. Et comme vous ne pouvez pas contrôler les protocoles de sécurité utilisés sur ces réseaux publics, vous n'avez aucune idée des faiblesses existantes ou des méthodes de chiffrement utilisées. Vous n'avez donc aucun moyen de savoir si le réseau ou la connexion a déjà été attaqué et pourrait mettre vos informations et votre appareil en danger. C'est le cas même si une connexion est protégée par un mot de passe, car n'importe qui peut demander le mot de passe et accéder au même réseau que vous.

En d'autres mots, tout ce à quoi vous avez accès publiquement, mais surtout les connexions et les appareils dont vous ne connaissez pas le propriétaire, peut être compromis et présenter des risques potentiels. Toutes les connexions sans fil peuvent être piratées, y compris les connexions Bluetooth et AirDrop. Même les codes QR, de plus en plus populaires depuis la pandémie, peuvent mener à un site à risque ou lancer le téléchargement d'un maliciel.

COMMENT POUVONS-NOUS ASSURER NOTRE SÉCURITÉ?

De nos jours, nous pouvons facilement nous connecter aux réseaux publics ou utiliser l'appareil de quelqu'un d'autre sans penser consciemment aux risques potentiels. Il se peut même que votre enfant doive se connecter à un appareil de l'école pour effectuer un travail en classe. Il y a cependant des mesures que vous pouvez prendre et garder à l'esprit pour assurer la sécurité de vos comportements publics et pour sécuriser votre connexion et vos appareils à la maison.

Notre principal conseil en matière de navigation publique est d'**éviter de vous connecter à des comptes importants** : ne vous connectez à votre compte bancaire, à votre adresse courriel ou à vos réseaux sociaux que sur vos propres appareils, et si vous devez vous connecter lorsque vous n'êtes pas chez vous, utilisez vos données personnelles plutôt que le réseau Wi-Fi. Dans les paramètres Wi-Fi de votre appareil, vous trouverez également l'option permettant de rejoindre automatiquement un réseau Wi-Fi, une fonction que vous pouvez désactiver si vous voulez vous assurer que vous n'accéderez pas à un compte important en vous connectant accidentellement à un réseau public, ou si vous voulez vous assurer que votre enfant ne commettra pas cette erreur.

Nous avons également inclus dans les ressources pour enfants de **ne pas utiliser des fonctions comme AirDrop** (ou Quick Share sur Android), et ce principalement pour les protéger contre la réception de fichiers provenant de sources inconnues. Par le passé, des personnes ont reçu du contenu inapproprié ou des maliciels à travers ces fonctions ; il est donc recommandé de ne pas laisser les enfants accepter des fichiers via cette fonction.

Dans les paramètres de votre appareil (sur iPhone : Réglages > Général > AirDrop; sur Android : Paramètres > Appareils connectés > Préférences de connexion), il est possible de configurer cette fonction pour ne pas recevoir de fichiers ou de liens de qui que ce soit. Vous avez également la possibilité de ne recevoir que des fichiers provenant de vos contacts, mais cela peut tout de même présenter des risques si l'appareil de l'autre personne a été compromis.

Sur un appareil public, pour tout compte auquel vous vous connectez, veillez toujours à vous déconnecter après utilisation, même s'il s'agit d'un compte auquel vous ne tenez pas beaucoup. Chaque compte auquel vous vous connectez contient des informations personnelles qui peuvent être utilisées contre vous dans le cadre d'attaques d'hameçonnage ou pour essayer de deviner vos mots de passe importants, par exemple, et il est donc préférable de les garder en sécurité. Cela signifie aussi qu'il faut veiller à **ne pas laisser le navigateur public enregistrer vos mots de passe** ou vous garder connecté, comme les navigateurs vous le demandent souvent. Bien qu'il soit plus facile de cliquer sur «enregistrer» pour faire disparaître la bulle, une fois que vous avez enregistré vos informations dans un navigateur, n'importe qui peut revenir sur votre compte sans que vous le sachiez.

Ces conseils permettent de s'assurer que, quoi qu'il arrive à l'appareil ou au réseau que vous utilisez, vos données les plus importantes restent en sécurité. Bien entendu, ils doivent être associés à d'autres conseils de cyberhygiène, comme l'utilisation de mots de passe uniques afin que vos autres comptes importants ne soient pas touchés en cas de fuite de données. C'est également une bonne idée de mettre en place l'authentification multifactorielle sur tous vos comptes principaux. De cette manière, si un pirate a installé un enregistreur de frappe sur un appareil public que vous utilisez, il ne pourra toujours pas accéder à vos comptes, puisqu'il n'aura pas accès à l'appareil ou au numéro de téléphone qui émet un code à usage unique, par exemple.

GLOSSAIRE

- **Wi-Fi** : Le Wi-Fi est une technologie qui permet aux appareils électroniques de se connecter à un réseau local sans fil, généralement à l'aide d'ondes radio.
- **Connexion sans fil** : Une connexion sans fil est un lien de communication établi entre des appareils électroniques sans l'utilisation de câbles ou de fils physiques. Les connexions sans fil s'appuient sur des signaux radio ou des ondes infrarouges pour transmettre des données entre des appareils.
- **Réseau sécurisé ou non sécurisé** : Un réseau sécurisé est un réseau informatique qui a mis en place des mesures pour protéger la confidentialité, l'intégrité et la disponibilité des données qu'il transmet.
- **Authentification multifactorielle** : L'authentification multifactorielle est un mécanisme de sécurité qui exige des utilisateurs qu'ils fournissent plusieurs formes d'identification avant d'accorder l'accès à un système, un compte ou une application. L'objectif de l'authentification multifactorielle est de renforcer la sécurité du processus d'authentification en ajoutant une couche supplémentaire de vérification au-delà du nom d'utilisateur et du mot de passe.
- **Ver informatique** : Un ver informatique est un type de maliciel capable de s'auto-reproduire et de se propager de manière indépendante dans les réseaux et systèmes informatiques sans requérir d'interaction de la part de l'utilisateur. Contrairement aux virus, qui nécessitent généralement un programme hôte pour être infectés et se propager, les vers sont des programmes autonomes qui peuvent se propager automatiquement en exploitant les vulnérabilités des protocoles de réseau, des systèmes d'exploitation ou des applications logicielles.
- **Enregistreur de frappe** : Un enregistreur de frappe est un type de logiciel ou de matériel de surveillance qui enregistre chaque touche tapée sur un clavier et les mouvements de souris, souvent de manière secrète et à l'insu de l'utilisateur.
- **Logiciel malveillant ou maliciel** : Les maliciels, mot-valise pour logiciels malveillants, désignent tout type de logiciel spécifiquement conçu pour perturber, endommager ou obtenir un accès non autorisé à des systèmes, réseaux ou appareils informatiques, souvent à l'insu ou sans le consentement de l'utilisateur.

Balayez ce QR code à l'aide de votre caméra pour visionner nos vidéos