Fiche-conseils sur la cybersécurité destinée aux consommateurs

Navigation sécuritaire

Visiter des sites Web est l'activité la plus élémentaire sur Internet. Ce faisant, selon qu'on soit prudent et bien préparé ou non, on accède à un monde de possibilités et de divertissements où on se trouve devant une foule de problèmes.

En règle générale, la navigation se fait au moyen de **navigateurs**, par exemple *Internet Explorer*, *Firefox*, *Chrome* ou *Safari*. Bien que ces navigateurs soient actualisés régulièrement, l'usage que nous faisons du Web a évolué à un point tel que nous y pratiquons plusieurs de nos activités, par exemple nous y faisons nos achats et nos transactions bancaires. Voilà pourquoi l'utilisation du Web s'accompagne désormais d'un cortège de risques potentiels.

Types de risques

La navigation sur le Web comporte deux principaux types de risques : les risques **technologiques**, issus de logiciels dangereux et de bogues dans les programmes utilisés, et les risques **comportementaux**, découlant des décisions que nous prenons en ligne.

Heureusement, il existe plusieurs façons de se prémunir contre ces risques, de même que d'en protéger son réseau et son ordinateur. Et tous les deux peuvent être réduits au minimum en évitant les sites Web dont on doute de la légitimité et en se gardant de pratiquer des activités au cours desquelles on expose son ordinateur à des fichiers inconnus, par exemple le partage de fichiers et le téléchargement illégal de musique ou de vidéos. Si plusieurs personnes utilisent le même ordinateur, il convient de veiller à ce que chacune prenne aussi ces précautions.

Risques technologiques

Les mauvaises nouvelles :

- Les problèmes de sécurité peuvent découler d'un défaut du produit utilisé.
- Pour les régler, il suffit de consacrer un peu de temps à en apprendre davantage sur le logiciel et le matériel en question. Heureusement, cela se résume à prendre quelques précautions élémentaires.

Les bonnes nouvelles :

- Tout devient beaucoup plus facile une fois que l'on sait comment tirer parti des fonctions de sécurité intégrées et des outils de confidentialité.
- Nul besoin de chercher longtemps pour trouver ces solutions de sécurité, car bien souvent, elles sont d'ores et déjà intégrées au navigateur et à l'ordinateur.
- Les défauts technologiques sont généralement repérés rapidement par les développeurs et éliminés au moyen de correctifs de logiciels et de mises à jour.
- Une fois mises en place, les pratiques de cybersécurité technologiques n'exigent habituellement qu'une mise à jour mineure.

Les façons de se protéger :

Maintenir à jour son logiciel : Les fabricants de logiciels publient fréquemment des correctifs logiciels, des modifications et des mises à jour afin de corriger des bogues et d'éliminer des menaces à la sécurité fraîchement découverts. En mettant à jour son logiciel régulièrement, on évite de s'exposer aux risques connus qu'il comporte. **Il est particulièrement important de mettre à jour son navigateur régulièrement puisqu'il s'agit de la voie de communication principale entre l'ordinateur et Internet.** La fréquence des mises à jour du logiciel à partir des paramètres de l'ordinateur est réglable.

Sécuriser son routeur et son réseau sans fil : Le **mot de passe** ou la **phrase passe** permettant d'accéder au routeur sans fil doivent être **robustes**, de sorte que personne de l'extérieur du foyer n'y accède. Cela procure une double protection : 1) en faisant obstacle à l'accès au stockage et aux dispositifs de votre réseau et 2) en empêchant d'autres personnes d'épuiser sa limite mensuelle de bande passante.

Apprendre à gérer son pare-feu : Les pare-feu permettent de contrôler les chaînes de connexion au réseau provenant d'autres ordinateurs. Pour ce faire, il suffit de désactiver certains ports du système d'exploitation. Tant les systèmes d'exploitation Mac que Windows sont dotés de pare-feu intégrés.

Recourir à un logiciel antivirus/antimaliciel : Il s'agit d'investir dans cette puissante ligne de défense, d'apprendre à la configurer et enfin, de la laisser faire son œuvre. *Norton*, *Symantec* et *Avast* sont des marques bien connues de logiciels antivirus.

Savoir reconnaître un site sécurisé : Un site sécurisé chiffre les données transmises entre celui-ci et l'ordinateur. Cela signifie que pendant sa transmission, l'information est sécurisée. Les sites sécurisés sont reconnaissables à leur adresse qui commence par *https,* plutôt que par *http* et à l'icône du cadenas figurant dans le coin droit supérieur ou inférieur de la fenêtre du navigateur et **non** du site Web en soi.

Toutefois, le fait qu'un site soit sécurisé ne garantit pas que les renseignements demeureront protégés *après* leur transmission. Les sites Web stockant les numéros de carte de crédit en vue d'achats futurs illustrent bien ce propos. Par conséquent, il est préférable de refuser le stockage permanent de ces renseignements comme élément du profil du client.

Bloquer ce dont on ne veut pas : Les navigateurs et les applications de messagerie électronique permettent de bloquer tout contact avec des personnes ou des sites particuliers. La plupart des navigateurs sont dotés d'une fonctionnalité de filtrage, laquelle permet de bloquer les sites selon le type de contenu.

Liquider ses témoins : Les témoins (*cookies)* sont de petits fichiers stockés dans l'ordinateur. Ils assurent le suivi de l'utilisation que l'on fait de sites Web particuliers, par exemple les préférences de l'utilisateur, l'information nécessaire à l'ouverture d'une session, les renseignements sur la carte de crédit, etc. Il est judicieux de supprimer ces fichiers régulièrement.

Recourir aux outils de confidentialité : Les sites de médias sociaux et les navigateurs proposent des outils permettant de personnaliser les renseignements personnels partagés avec les autres internautes. On doit prendre le temps de lire et de comprendre ces paramètres et les utiliser. Les navigateurs offrent un autre outil de confidentialité, la navigation privée, laquelle permet de naviguer sur le Web sans laisser, dans la mémoire cache de l'ordinateur, de renseignements révélant les sites visités. (Cependant, il faut garder à l'esprit que la navigation privée ne s'applique qu'à l'ordinateur utilisé. Il est possible que le fournisseur de service Internet ou d'autres applications conservent ces indications.)

Risques comportementaux

Les mauvaises nouvelles :

- Ces risques peuvent être difficiles à détecter, car on peut y être exposé accidentellement par des amis ou des membres de la famille.
- Il n'existe pas de solution simple pour s'en prémunir. L'unique façon de s'en protéger consiste à faire preuve de prudence et de scepticisme et à apprendre à repérer les escroqueries les plus courantes.

Les bonnes nouvelles :

- S'arrêter un moment et réfléchir avant d'agir constitue la solution à plusieurs problèmes provoqués par le comportement.
- Ces solutions sont faciles à mettre en œuvre et contribuent à rendre l'expérience sur le Web plus agréable, et ce, tant pour soi que pour son entourage.
- Apprendre à lutter contre ce type de problèmes de sécurité permet d'aider sa famille, ses amis et ses collègues à devenir plus prudents également.
- Plus on cultive le réflexe de penser à ce type de problèmes, plus on repère aisément les nouveaux pièges dans lesquels peuvent nous précipiter nos comportements irréfléchis.

Les façons de se protéger :

Réfléchir avant d'agir : Avant de cliquer sur quoi que ce soit ou de remplir un formulaire, il convient de s'arrêter et de se demander si ce devant quoi on se trouve est réaliste. Comment cette entreprise totalement inconnue peut-elle se permettre de donner tous ces appareils

électroniques en ne réclamant pas plus que le temps requis pour une brève partie d'un jeu en ligne? Si c'est trop beau pour être vrai, c'est que ça ne l'est pas.

Obtenir un deuxième avis : Bien que les sites voués à l'escroquerie prolifèrent, la meilleure arme contre ceux-ci se trouve juste au bout de nos doigts. Les sites Web anticanulars consacrés aux escroqueries contribuent à les mettre au jour et permettent de vérifier si l'histoire relatée dans un courriel donné est véridique. *Snopes* (www.snopes.com) est probablement le plus célèbre de ceux-ci, mais il en existe d'autres, par exemple www.hoaxbuster.com/ (en français), www.hoaxbusters.org, www.truthorfiction.com et www.nonprofit.net/hoax.

S'abstenir de participer : C'est parce qu'elles circulent d'un ami et d'un collègue à l'autre que plusieurs menaces à la sécurité prennent de l'ampleur. Pour agir contre ce type d'attaques, il suffit d'interrompre la chaîne.

Propager la nouvelle : Quelqu'un vous a-t-il transmis un canular? Parfois, avec les meilleures intentions du monde, les gens de notre entourage font circuler des faussetés. Certains ne prennent pas le temps de vérifier la véracité de l'information avant de la relayer. Il est bien avisé d'en parler, mais en faisant preuve de courtoisie et en appuyant ses dires en tout temps. Dans le même ordre d'idées, avertir les autres des escroqueries et des fraudes que l'on découvre est toujours indiqué. Les nouvelles sur les fourberies qui circulent doivent être propagées. Plus les gens seront nombreux à les signaler, plus le nombre de victimes piégées diminuera.

Choisir des mots de passe et des phrases passe robustes : Un mot de passe robuste consiste en un mot de huit lettres ou plus, dont on remplace certaines lettres par des chiffres et des caractères (tels que @ et !). Par exemple, le mot chandelier peut être modifié comme ceci : c4@nd3l!er. Il est aussi préférable de ne pas utiliser le même mot de passe pour tous les types de comptes. Un truc simple consiste à ajouter la première et la dernière lettre du nom du site dans lequel on ouvre une session. Si le mot de passe habituel est c4@nd3l!er, le mot de passe dans *Facebook* devient Fc4@nd3l!erk.

Vider la mémoire cache, effacer l'historique et fermer les sessions : Supprimer les renseignements qui, autrement, restent derrière soi, particulièrement des ordinateurs partagés, est une bonne habitude à acquérir. Il est aussi important de fermer en bonne et due forme la session (par un lien *Fermer la session* ou *Quitter*) des services Web utilisés. Ainsi, le prochain internaute n'accédera pas à vos comptes.

Ne pas mordre à l'hameçon : Les banques sont des établissements de bonne réputation qui ne sollicitent **jamais** la transmission de renseignements sur les comptes bancaires par courriel. Les courriels d'*hameçonnage* tentant d'obtenir des mots de passe ou des renseignements personnels devraient toujours demeurer sans réponse. La transmission de courriels au nom d'un agent de la banque de l'utilisateur ou de liens dirigeant vers de faux sites Web sont les méthodes généralement employées. On doute? Alors, on téléphone à l'entreprise ou à sa banque pour vérifier.

Suivre la foule : Pourquoi ne pas profiter des listes créées par les internautes ou des discussions qui ont cours au sujet des sites Web, des personnes et des entreprises problématiques? Par exemple, les vendeurs en ligne sur des sites comme *Amazon* et *eBay* sont cotés par les gens qui ont fait des affaires avec eux.

Établir une limite : Il est judicieux de recourir à des solutions de paiement en ligne limitées à une somme déterminée, par exemple aux cartes de crédit prépayées, aux cartes-cadeaux ou aux cartes de temps prépayées. Si la carte était dérobée ou les données usurpées ou utilisées à mauvais escient, la perte se limiterait à la valeur de la carte.

Pour obtenir plus de renseignements :

Veuillez consulter la *Fiche-conseils sur la sécurité destinée aux consommateurs* de l'Autorité canadienne pour les enregistrements Internet (ACEI) et HabiloMédias est disponible au www.acei.ca et sur le site Web au www.habilomedias.ca, même que d'autres ressources favorisant la littératie numérique.

L'ACEI est fière de commanditer HabiloMédias et le travail essentiel dont il s'acquitte au nom de la population canadienne.