Canadians Connected
Canadiens branchés

Fiche-conseils sur la cybersécurité destinée aux consommateurs

Appareils mobiles

Non seulement les appareils mobiles sont des outils indispensables nous permettant de garder contact avec nos amis, les membres de notre famille et le travail, mais nous les utilisons de plus en plus pour nous connecter à Internet. Bien que certains téléphones intelligents soient aussi puissants que les ordinateurs, il nous arrive malheureusement trop souvent de ne pas les utiliser avec la prudence dont nous faisons preuve en nous servant de ces derniers; et la plupart du temps, ces appareils ne sont pas dotés des mesures de protection de la vie privée et visant à assurer la sécurité qui sont intégrées à nos ordinateurs. De plus, puisque nous gardons ces appareils à portée de main, nous disposons d'une foule d'occasions de nous laisser distraire et de prendre de mauvaises décisions.

Risques liés à l'utilisation des appareils mobiles

Vol de données

En raison de leur commodité, nous nous servons des appareils mobiles à la fois pour accomplir notre travail et faire nos achats en ligne. Malheureusement, cela signifie que l'appareil contient probablement une profusion de renseignements personnels sur son propriétaire. Inutile d'être un pirate informatique pour extraire de l'information d'un appareil mobile; des gens oublient tous les jours leurs téléphones et leurs tablettes électroniques dans les taxis, les avions et les restaurants, et selon le Commissariat à la protection de la vie privée, moins de la moitié des Canadiens utilisent un mot de passe pour verrouiller leur appareil ou y définissent des paramètres rigoureux de confidentialité. Dès qu'elle met la main sur vos données, une personne peut les utiliser pour avoir accès à vos comptes, faire des achats avec vos cartes de crédit ou même usurper votre identité en ligne.

Programme malveillant

Bien qu'il soit possible à un programme malveillant d'avoir accès à un téléphone cellulaire, dans la plupart des cas, ce sont les utilisateurs qui mettent en péril la sécurité de leur appareil en téléchargeant des applications contenant ce type de programme. Malgré que la plupart d'entre nous fassent maintenant preuve de prudence en téléchargeant des applications sur nos ordinateurs, il nous arrive fréquemment d'être distrait en utilisant nos appareils numériques et, en un clic, il devient de plus en plus facile de ne pas réfléchir suffisamment au moment du téléchargement d'une application. Contrairement aux programmes malveillants conçus pour les ordinateurs et issus habituellement du marché gris ou de sites illégaux tels que les sites de partage de fichiers, les logiciels malveillants conçus pour les appareils mobiles se cachent souvent parmi les nombreuses applications légitimes gratuites ou offertes à peu de frais qui se font passer pour des jeux ou même pour des logiciels de sécurité. Il existe deux principaux types de programmes malveillants connus : ceux qui volent vos données quand vous utilisez votre téléphone et ceux qui utilisent vos comptes à votre insu pour payer des achats.

Cyberintimidation

Que ce soit par appareil mobile ou par l'entremise de réseaux sociaux, la cyberintimidation et le harcèlement sont des problèmes de grande importance. Des études ont démontré que les adolescents qui sont d'avides utilisateurs de téléphones cellulaires sont plus susceptibles d'être à la fois les cibles et les instigateurs de la cyberintimidation, et les appareils photo sur la plupart des téléphones permettent de capter et de télécharger les images de n'importe quelle situation embarrassante.

Sextage

Puisque nous utilisons principalement les téléphones pour parler ou texter avec une seule personne à la fois, nous oublions fréquemment que tout ce que nous faisons au moyen d'un appareil mobile peut être sauvegardé, copié et acheminé à un nombre insoupçonné de personnes. Le sextage (et le partage de sextos que vous recevez) peut entraîner différentes répercussions allant de l'embarras jusqu'à la poursuite criminelle, et les adolescents ne sont pas les seuls en cause. De fait, une étude réalisée en 2012 a révélé que les adultes sont deux fois plus susceptibles de se livrer à ce type d'activité que le sont les adolescents.

Dépenses excessives

La facilité avec laquelle nous pouvons acheter des biens au moyen d'un téléphone ou d'une tablette – qu'il s'agisse d'applications pour l'appareil ou de marchandise dans une boutique virtuelle – peut nous inciter à faire des achats irréfléchis. De même, plusieurs applications de jeux, particulièrement celles conçues pour les enfants, encouragent les utilisateurs à dépenser de l'argent pour accéder à d'autres étapes du jeu. Ainsi, les enfants peuvent utiliser les renseignements relatifs aux cartes de crédit de leurs parents si ces derniers ne sont pas vigilants. Enfin, l'utilisation du téléphone à elle seule peut entraîner des coûts imprévisibles alors qu'augmente le nombre d'appels, de textos et de recherches en ligne.

Distraction

Il existe dans plusieurs endroits des lois interdisant l'utilisation d'appareils mobiles au volant, mais les cyclistes et les piétons qui s'en servent peuvent également être victimes d'accidents. De même, avoir un appareil à portée de main pendant que vous faites autre chose vous incite à effectuer plusieurs tâches simultanément, vous rendant ainsi moins efficaces dans la réalisation de chacune de chacune d'elles. Les appareils mobiles peuvent également être source de troubles du sommeil, tout particulièrement pour les adolescents qui ressentent le besoin de répondre immédiatement aux textos qu'ils reçoivent et qui redoutent de ne pas être au courant de ce que font leurs amis.

Contenu inapproprié

Plusieurs des préoccupations qu'ont les parents qui souhaitent contrôler l'expérience Internet de leurs enfants sont les mêmes en ce qui concerne les appareils mobiles. De nombreuses applications sont conçues pour les jeunes enfants et les adolescents. Toutefois, puisque les nouvelles applications sont souvent catapultées sur le marché et que ce sont les concepteurs qui les évaluent, il est parfois difficile de connaître la nature véritable du produit offert.

Atteintes à la vie privée

Même si vous ne stockez pas vos renseignements personnels dans votre téléphone, il s'y accumule des données sur votre identité et l'endroit où vous vous trouvez. Plusieurs applications légitimes communiqueront ces données aux concepteurs de l'application ou à des tiers. La plupart du temps, cette collecte de données est énoncée dans les modalités que vous acceptez quand vous téléchargez l'application, mais des atteintes à la vie privée sont commises secrètement et de façon malicieuse, notamment au moyen de logiciels espions qui permettent à une personne d'utiliser à distance l'appareil photo ou le microphone de votre appareil, même lorsqu'il est éteint.

Comment vous protéger

Renseignez-vous. Assurez-vous de comprendre les fonctionnalités d'un téléphone mobile avant de l'acheter, que ce soit pour vous ou votre enfant. Comprenez les paramètres de sécurité et de protection de la vie privée de l'appareil et appliquez-les, ou mieux encore, demandez quel appareil possède les meilleurs outils de sécurité avant de faire votre achat. Avant de télécharger une application, prenez connaissance des modalités pour connaître lesquels parmi vos renseignements personnels seront recueillis.

Faites preuve de politesse. Traiter les gens à qui vous parlez ou à qui vous envoyez des textos avec la même courtoisie que celle dont vous faites preuve avec les gens avec qui vous communiquez face à face. Souvenez-vous qu'un grand nombre des indices qui nous servent à comprendre ce qu'une personne veut exprimer, notamment son expression faciale, son langage corporel et son ton, sont absents de l'échange de textos. Alors, assurez-vous de formuler clairement vos énoncés et ne tirez pas de conclusions hâtives quant à la signification des propos de votre interlocuteur.

Voyez plus loin. Essayez d'imaginer qui pourrait voir les textes ou les photos que vous envoyez ou que vous faites suivre à l'aide de votre appareil. Avant d'envoyer un texte ou une photo, réfléchissez à ce que pourrait ressentir la personne qui les reçoit ou qui vous les a envoyés.

Procurez-vous un effaceur. Il existe un logiciel, conçu pour presque tous les appareils mobiles, qui vous permet de les suivre, de les désactiver ou d'en effacer la mémoire à distance. Vous devez immédiatement utiliser ce logiciel si vous perdez votre appareil ou si on vous le dérobe. Si vous vous procurez un nouvel appareil, assurez-vous d'avoir effacé complètement la mémoire de l'ancien avant de le vendre, de le donner ou de le jeter. (Vous devriez pouvoir obtenir ces renseignements sur le site Web du fabricant de votre appareil).

Privilégiez la sécurité. Établissez vos comptes en ligne de façon à utiliser des connexions sûres au moyen des versions « https » de l'adresse du site.

Faites preuve de prudence. Faites des recherches sur l'application avant de la télécharger pour vous assurer de sa fiabilité et veiller à ce qu'elle ne cache pas de contenu indésirable. Ne cliquez pas sur les liens que vous recevez par courriel ou textos.

Éteignez les appareils dont vous ne vous servez pas. Les technologies Bluetooth et WiFi, ainsi que d'autres méthodes de connexion, peuvent être la cible de pirates informatiques. Il est préférable de les éteindre lorsque vous ne les utilisez pas. De plus, activez l'option « non-découverte » sur tous vos appareils Bluetooth afin qu'il soit impossible aux utilisateurs de périphériques Bluetooth près de vous de les détecter.

N'exposez pas vos données. Ne transmettez jamais d'information sensible, ne faites jamais d'achat ou de transactions bancaires en ligne lorsque vous utilisez un point d'accès sans fil public. Ceux-ci sont très vulnérables au piratage.

Fixez des limites de dépenses. Quand vous faites des achats en ligne, utilisez des cartes de crédit prépayées ou à faible limite de crédit pour éviter de trop dépenser. Si vous partagez un appareil avec une autre personne, faites en sorte d'effacer l'information sur votre carte de crédit de la mémoire de l'appareil après chaque achat effectué en ligne. Expliquez aux jeunes enfants que les achats relatifs aux jeux coûtent de l'« argent réel » et qu'ils doivent demander la permission avant de se procurer quoi que ce soit. Demandez, pour les enfants et les adolescents, un forfait avec limites strictes (de façon à ce qu'ils ne puissent plus envoyer de textos une fois la limite atteinte au lieu de devoir payer un montant plus élevé) ou un forfait illimité de messagerie texte.

Abstenez-vous d'effectuer plusieurs tâches simultanément. N'utilisez jamais un appareil mobile au volant, à bicyclette ou en marchant. Lorsque vous travaillez, laissez votre appareil hors de portée pour vous éviter de succomber à la tentation de vérifier si vous avez reçu quelque chose. Déclarez des endroits « sans téléphone » dans votre maison; dans les chambres à coucher ou autour de la table, par exemple.

Discutez. Avant que votre enfant ou votre adolescent commence à se servir d'un appareil mobile, discutez de ces enjeux avec lui. Rassurez-le en lui disant qu'il peut se confier à vous s'il arrive quoi que ce soit. Dites-lui que, dans un tel cas, vous ne vous affolerez pas et ne lui confisquerez pas son appareil.

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 disponible au www.acei.ca et sur le site Web 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.

Habilo Médias