Canadians Connected
Canadiens branchés

Fiche-conseils sur la cybersécurité destinée aux consommateurs

Socialiser et interagir en ligne

Internet est devenu un volet essentiel de la vie sociale de la plupart d'entre nous : nous l'utilisons pour obtenir des nouvelles d'amis de longue date, garder le contact avec les membres de notre famille et pour faire de nouvelles rencontres. Malheureusement, les interactions en ligne ne sont pas toutes aussi constructives que celles-ci. Cette fiche-conseils explique certaines des situations problématiques que nous rencontrons lorsque nous socialisons en ligne et procure des conseils sur la façon de les gérer.

Risques en matière de vie privée et d'identité

Usurpation d'identité

Chaque fois que vous ajoutez des détails personnels à votre profil en ligne, le risque qu'un arnaqueur les dérobe plane. Bien que plusieurs de ces détails puissent sembler anodins, votre date de naissance et votre nom complets, par exemple, ils peuvent suffire à ouvrir toute grande la porte à vos comptes en ligne. Également, si les mises à jour de vos renseignements sont divulguées, les arnaqueurs peuvent demeurer à l'affût pour accumuler des détails qui leur permettront de deviner votre mot de passe ou votre question de sécurité. Sur les réseaux sociaux tels que Facebook, vous risquez de donner accès à votre compte aux arnaqueurs tout simplement en « aimant » ou en « partageant » une page frauduleuse ou en permettant l'infiltration d'une application hostile dans votre profil.

Hameçonnage

La plupart des messages visant l'hameçonnage constituent des arnaques passablement évidentes : un courriel ou un message vous demandant de transmettre votre mot de passe et votre nom d'utilisateur à l'un de vos comptes en ligne. Cependant, le partage de renseignements personnels en ligne – ne serait-ce qu'en discutant d'activités telles que votre travail ou vos passe-temps – peut déclencher la réception de messages de harponnage personnalisés. Puisqu'ils vous sont destinés de manière ciblée pour capter votre attention, ceux-ci se révèlent possiblement beaucoup plus

Mystification

En franchissant un pas au-delà de l'usurpation d'identité, la mystification consiste à prétendre être quelqu'un d'autre en ligne. Prendre les commandes d'un profil en ligne ou en créer un nouveau en votre nom peut faire partie de cette activité. Bien souvent, la mystification n'est que la première étape d'une fraude de plus grande envergure : par exemple, les arnaqueurs recourent à des comptes Facebook ou à des courriels piratés pour transmettre de faux messages aux amis de la personne, prétendant avoir besoin d'argent urgemment pour se tirer d'un mauvais pas, évoquant parfois l'impossibilité de quitter un pays étranger.

Tips for Safe and Secure Surfing

Pêche à la traîne

Il s'agit désormais d'un terme générique désignant toutes les activités en ligne visant à compliquer la vie d'autrui. Certaines ne visent qu'à irriter, mais les campagnes de diffamation, le harcèlement et même les menaces de violence peuvent en faire partie. Certains joueurs en ligne se plaisent à mécontenter leurs adversaires. Par exemple, ils formulent des commentaires racistes ou misogynes ou encore anéantissent leurs personnages de jeu. La pêche à la traîne sévit aussi fréquemment dans les environnements interactifs tels que les réseaux sociaux ou les forums de sites Web populaires.

Environnements hostiles

Alors que des personnes particulières peuvent être la cible de pêche à la traîne, plusieurs environnements en ligne peuvent faire preuve d'hostilité envers les femmes, les minorités visibles et d'autres groupes en raison de la langue ou des attitudes qu'ils adoptent généralement.

Arnaques

Internet a facilité la vie à bien des gens, y compris aux maîtres de l'arnaque. Bien que la plupart des arnaques en ligne soient assez évidentes, certaines peuvent être alléchantes ou suffisamment intimidantes pour vous faire mordre à l'hameçon, telles qu'un message vous annonçant que vous avez gagné un prix ou qu'un avertissement vous indiquant que votre ordinateur est infecté par un maliciel.

Canulars

Puisque les gens les propagent sans savoir qu'il s'agit de canulars, ceux-ci peuvent survivre longtemps sur Internet. Bien qu'ils soient rarement préjudiciables, ils peuvent vous inciter à prendre de mauvaises décisions pour votre santé ou influencer injustement votre opinion sur une personne, une entreprise ou un produit particuliers (les vedettes et les politiciens en sont des victimes de choix).

Conseils pour naviguer en toute sécurité

Fermez votre session. Fermez toujours votre session après avoir utilisé vos comptes en ligne. Ce faisant, les autres utilisateurs auront plus de mal à y accéder (par exemple, si vous fermez votre navigateur sans fermer votre session sur Facebook, une personne utilisant le même ordinateur que vous n'aura pas à ouvrir une session pour accéder à votre compte).

Utilisez les paramètres de confidentialité. Presque tous les réseaux sociaux proposent des outils vous permettant de déterminer les personnes pouvant consulter les renseignements sur votre profil et les éléments que vous publiez en ligne. À tout le moins, veillez à ce que votre compte ne soit pas réglé à « public ».

Sachez choisir de bons mots de passe. Choisissez un mot de passe robuste, soit d'au moins huit caractères en minuscules et en majuscules comportant des chiffres ou des signes typographiques. À chaque compte son mot de passe (ajoutez à votre mot de passe un premier et un dernier caractère exclusifs à chaque compte) et ne partagez jamais vos mots de passe avec quiconque.

Gardez votre sang-froid. Si vous pensez faire l'objet de pêche à la traîne par une personne que vous connaissez, ne répondez pas : faites une capture d'écran et collez-la dans un programme graphique, puis attendez jusqu'à ce que vous puissiez en discuter hors ligne avec la personne concernée. S'il s'agit d'un inconnu et que la pêche à la traîne perdure, bloquez la personne et signalez l'incident.

Opposez-vous. Si vous êtes témoin de harcèlement ou si le langage ou les attitudes que vous observez dans un forum en ligne vous déplaisent, exprimez votre désapprobation. Signalez toute forme de harcèlement ou d'abus. Des modérateurs sont affectés à presque tous les jeux en ligne, et la plupart des réseaux sociaux permettent de désigner ou de faire état d'un billet abusif. Même les sites privés peuvent faire l'objet d'une plainte en s'adressant au fournisseur de service Internet, lequel refusera la plupart du temps d'héberger du matériel haineux ou harcelant.

Protégez votre vie privée. En ligne, ne communiquez aucun renseignement vous identifiant personnellement, par exemple votre date de naissance ou votre nom complets, votre numéro d'assurance sociale ou votre numéro de téléphone. Songez que des arnaqueurs ont pu avoir piraté le compte d'une personne de votre entourage et surveiller tout ce que vous publiez. Faites preuve d'une prudence toute particulière quant aux renseignements que vous diffusez sous le paramètre par défaut « public » dans les réseaux tels que Twitter. Souvenez-vous d'appliquer la même règle lorsque vous pratiquez le réseautage professionnel ou que vous consultez des sites d'offres d'emploi.

Protégez-vous. Recourez aux logiciels de sécurité et aux extensions des navigateurs qui vous avertissent lorsque vous faites l'objet d'une filature en ligne. Certains logiciels de sécurité vous indiqueront, avant que vous le visitiez, si un site est malicieux.

Soyez avare de vos données. Ne communiquez pas vos renseignements personnels à moins d'y être obligé : même si vous les transmettez à une personne digne de confiance, rien ne garantit qu'ils ne seront pas piratés. Ne répondez pas aux sondages en ligne et apprenez aux enfants à ne pas partager de renseignements à leur sujet ni à propos de votre famille, et ce, même si la source semble digne de foi (des arnaqueurs ont déjà eu recours à des sites Web de lettres au père Noël pour recueillir des renseignements sur les enfants).

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

Ouvrez l'œil. Vérifiez vos comptes bancaires et de carte de crédit régulièrement pour vous assurer qu'ils ne sont pas utilisés à mauvais escient. De plus, effectuez une recherche sur votre nom de temps à autre (vous pouvez régler une alerte Google pour automatiser cette activité) pour vous assurer que personne n'usurpe votre identité en ligne.

Soyez prudent. Presque toutes les arnaques en ligne peuvent être évitées en gardant à l'esprit l'adage « si ça semble trop beau pour être vrai, c'est probablement le cas ».

Pensez-y à deux fois plutôt qu'une. Avant de croire, de répéter ou de transférer quoi que ce soit, vérifiez-en la véracité : effectuez une recherche sur le sujet en question ou consultez les sites dénonçant les canulars tels que Snopes (www.snopes.com) et About Urban Legends (www.urbanlegends.about.com).

Vérifiez la source. Avant de répondre à un message, assurez-vous qu'il provient d'un expéditeur répertorié. Ne répondez à aucun message et ne cliquez sur aucun lien avant d'y avoir veillé. Même si un message provient de l'une de vos connaissances, si quoi que ce soit semble louche, fiez-vous à votre intuition.

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