

Fiche-conseils sur la cybersécurité destinée aux consommateurs

La plupart de nos activités en ligne s'intègrent à l'une de ces trois catégories : échanger, faire des achats et s'amuser. Chacune comporte son lot de risques, et les consommateurs doivent en être conscients de sorte qu'ils puissent prendre les mesures requises pour s'en prémunir et protéger leurs ordinateurs.

L'Autorité canadienne pour les enregistrements Internet (ACEI) et son partenaire HabiloMédias tiennent à veiller à ce que lorsque vous êtes en ligne, vous demeuriez en sécurité. Vous trouverez donc ci-dessous une liste des risques potentiels auxquels vous pourriez vous heurter au cours de vos activités en ligne ainsi que des outils proposés pour les atténuer.

Cyberfraudes

En ligne, c'est facile de se faire flouer par des personnes qui multiplient les promesses fallacieuses. Vous pouvez consulter une liste exhaustive des cyberfraudes au <http://www.rcmp-grc.gc.ca/scams-fraudes/index-fra.htm>.

Outils utiles : [Signets](#), [Communications avec les sites et les FAI](#), [Crédit prépayé](#), [Signalement de la cybercriminalité](#), [Sites sécurisés](#), [Systèmes de cotation par les utilisateurs/fournisseurs](#).

Cybersquattage

Des escrocs peuvent enregistrer une adresse Web qui semble appartenir à une entreprise établie en bonne et due forme ou encore qui est susceptible d'être saisie accidentellement en tentant de naviguer vers un site Web légitime.

Outils utiles : [Signets](#), [Filtres de contenu](#).

Dépenses excessives

Il est facile de perdre le fil de ses dépenses lorsqu'on a la possibilité de faire des achats tangibles ou virtuels instantanément.

Outils utiles : [Crédit prépayé](#), [Filtres de contenu](#).

Hameçonnage

Il s'agit de courriels semblant provenir d'une institution bancaire ou d'une autre entreprise qui vous sont transmis dans l'espoir d'obtenir des renseignements à votre sujet.

Outils utiles : [Cryptage des courriels](#), [Signalement de la cybercriminalité](#).

Harcèlement (*Griefing*)

Certaines personnes se plaisent à embêter les gens sciemment en gâchant les expériences qui devraient être agréables.

Outils utiles : [Blocage d'autres utilisateurs](#), [Communications avec les sites et les FAI](#), [Filtres de contenu](#), [Paramètres de confidentialité](#), [Systèmes de cotation par les utilisateurs/fournisseurs](#).

Imposture

En ligne, c'est facile de se faire passer pour quelqu'un d'autre. Il existe une profusion de faux profils créés par des imposteurs sur Facebook et Twitter.

Outils utiles : [Blocage d'autres utilisateurs](#), [Mises à jour du navigateur et de l'antivirus](#), [Cryptage des courriels](#), [Pare-feu](#), [Gestion de la réputation](#), [Politiques de confidentialité](#), [Paramètres de confidentialité](#).

Logiciels espions

Ce sont des logiciels malveillants qui recueillent des données dans votre ordinateur. Certains enregistrent tout ce que vous saisissez au clavier.

Outils utiles : [Signets](#), [Mises à jour du navigateur et de l'antivirus](#), [Pare-feu](#), [Sites sécurisés](#).

Programmes malveillants

Ces programmes, qui prétendent être utiles ou s'installent en vous incitant à cocher une case, peuvent endommager votre ordinateur ou même en prendre les commandes.

Outils utiles : [Signets](#), [Mises à jour du navigateur et de l'antivirus](#), [Pare-feu](#), [Sites sécurisés](#).

Témoins

Il s'agit de petits fichiers que votre navigateur sauvegarde dans votre ordinateur. Le plus souvent, ils contiennent des données telles que votre nom d'utilisateur et votre mot de passe.

Outils utiles : [Mises à jour du navigateur et de l'antivirus](#), [Effacement de la mémoire cache du navigateur](#), [Politiques de confidentialité](#), [Navigation privée](#), [Sites sécurisés](#).

Usurpation d'identité

Les escrocs peuvent usurper votre identité en ligne en accédant aux renseignements sur votre carte de crédit, à votre information bancaire ou à d'autres données auxquelles vous recourez pour vérifier votre identité.

Outils utiles : [Signets](#), [Mises à jour du navigateur et de l'antivirus](#), [Effacement de la mémoire cache](#), [Pare-feu](#), [Politiques de confidentialité](#), [Navigation privée](#), [Signalement de la cybercriminalité](#), [Sites sécurisés](#).

Vol de données

Entre de mauvaises mains, vos données personnelles et financières peuvent prendre une valeur insoupçonnée.

Outils utiles : [Signets](#), [Mises à jour du navigateur et de l'antivirus](#), [Effacement de la mémoire cache](#), [Détermination de mots de passe robustes](#), [Cryptage des courriels](#), [Pare-feu](#), [Politiques de confidentialité](#), [Paramètres de confidentialité](#), [Navigation privée](#), [Signalement de la cybercriminalité](#), [Sites sécurisés](#).

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



Définition des outils utiles

Blocage d'autres utilisateurs : Presque tous les types d'outils de communication en ligne vous permettent de bloquer les échanges entre vous et certains utilisateurs.

Communications avec les sites et les FAI : Les comportements importuns, sans être criminels, peuvent être signalés au site où ils ont cours ou au FAI qui l'héberge.

Crédit prépayé : Certaines institutions bancaires et cartes de crédit vous offrent des cartes de crédit prépayé qui limitent vos dépenses à une somme fixe.

Cryptage des courriels : Les courriels peuvent être interceptés et lus. Les logiciels de cryptage et certains services de messagerie électronique vous permettent de crypter vos courriels de sorte qu'ils demeurent confidentiels.

Détermination de mots de passe robustes : Choisissez un mot de passe comportant au moins sept caractères et inspiré d'un mot sans aucun rapport avec vous. Remplacez certaines lettres par des chiffres, des caractères spéciaux ou des signes de ponctuation et écrivez-le en utilisant des majuscules et des minuscules. Puis personnalisez le mot de passe pour chaque site en y ajoutant la première et la dernière lettre de son nom. (bananes devient b@nAn2s et une fois dans Facebook, il se transforme en fb@nAn2sk.) En plus de vos comptes en ligne, assurez-vous que tous les appareils en réseau que votre famille possède – les ordinateurs, les téléphones, les tablettes, et les appareils branchés à Internet, par exemple les appareils intelligents mesurant votre activité physique – soient protégés par un mot de passe unique.

Effacement de la mémoire cache : Comme c'est dans la mémoire cache que votre navigateur sauvegarde les témoins, il convient de l'effacer fréquemment.

Filtres de contenu : Les navigateurs, les FAI, les sites Web et des logiciels spéciaux proposent tous des façons de filtrer le contenu indésirable.

Gestion de la réputation : Lancez une recherche de votre nom, puis visualisez les photos de vous qui se trouvent en ligne. Si certaines vous déplaisent, tentez de les faire retirer. Et libre à vous d'en publier certaines qui reflètent l'image que vous souhaitez projeter. Envisagez d'enregistrer votre nom à titre d'adresse Web (www.votrenom.ca).

Mises à jour du navigateur et de l'antivirus : Votre navigateur constitue votre défense de première ligne contre les logiciels malveillants, mais à défaut de le mettre à jour, il risque de prêter le flanc aux attaques. Et c'est tout aussi vrai pour les antivirus gratuits ou commerciaux que vous pouvez vous procurer. Les appareils branchés à Internet peuvent également être vulnérables : prenez l'habitude de consulter le site du fabricant au moins deux fois par année pour voir s'il y a des mises à jour pour le micrologiciel.

Navigation privée : La plupart des navigateurs proposent un mode de navigation grâce auquel aucun historique de vos activités n'est conservé dans votre mémoire cache.

Paramètres de confidentialité : Les sites de réseautage social tels que Facebook sont munis de paramètres de confidentialité vous donnant la latitude de sélectionner les personnes autorisées à prendre connaissance de votre profil. Comme, la plupart du temps, ces paramètres par défaut ne sont pas optimaux, veillez à régler les vôtres de façon à ce que seuls vos amis puissent le consulter.

Pare-feu : Ils bloquent l'accès non autorisé à votre ordinateur. Veillez à ce que le vôtre soit activé en vérifiant l'état de ce paramètre dans votre panneau de configuration.

Politique de confidentialité : Tous les sites qui recueillent des données devraient être dotés d'une politique de confidentialité. Elle doit être aisément intelligible et expliquer le sort réservé à l'information que vous

communiquiez au site, de même que la façon dont vous pouvez la supprimer si vous le souhaitez. Assurez-vous également de bien lire les politiques de confidentialité de tout appareils branché à Internet que vous considérez acheter : plusieurs de ces appareils recueillent beaucoup de données, directement et en ayant accès à vos autres comptes.

Signalement de la cybercriminalité : On ne peut faire échec à la cybercriminalité sans la signaler. Si vous êtes au courant de tentatives cybercriminelles, qu'elles aient réussi ou échoué, signalez-les au <http://www.recol.ca/>.

Signets : Il est possible d'enregistrer des signets ou des favoris dans la plupart des navigateurs, ce qui vous permet de vous rendre directement à vos sites Web de prédilection.

Sites sécurisés : Les sites Web sécurisés ont recours à des méthodes pour assurer la sécurité de vos données, par exemple au cryptage. Pour les repérer, il suffit de vérifier si leur adresse commence par *https* et si, quand vous vous y trouvez, un cadenas figure dans le coin droit inférieur de la fenêtre de votre navigateur (plutôt que dans le site Web lui-même).

Systèmes de cotation par les utilisateurs/fournisseurs : Certains sites commerciaux permettent aux utilisateurs d'accorder une cote aux fournisseurs afin d'évaluer la qualité de leurs produits et services. Aussi, recherchez les cotes élevées et les commentaires élogieux. Également, certains jeux en ligne et univers virtuels évaluent les utilisateurs en fonction de la rétroaction de leurs pairs. Vous pouvez recourir à ces outils pour contribuer à la lutte contre le harcèlement (*griefing*).

À propos de nous

L'Autorité canadienne pour les enregistrements Internet (ACEI) est l'organisme qui gère le registre des noms de domaine .CA du Canada, élabore et applique les politiques qui soutiennent la communauté Internet du Canada et représente le domaine .CA sur le plan international.

HabiloMédias est un centre canadien sans but lucratif qui œuvre pour l'éducation aux médias et la littératie numérique. Il a pour objectif de veiller à ce que les jeunes développent une pensée critique qui leur permet d'utiliser les médias à titre de citoyens numériques actifs et éclairés. HabiloMédias offre des centaines de ressources en éducation aux médias et littératie numérique aux bibliothécaires, aux parents et aux éducateurs sur son site Web. HabiloMedias.ca