Se protéger en ligne au Canada : un guide pour les nouveaux arrivants et arrivantes

Conseils de cybersécurité pour les particuliers, les familles et la population étudiante

Version française

Toronto Metropolitan University

ROGERS cybersecure catalyst

ROGERS

Etablissement.Org
Bienvenue en Ontario

Introduction

S'installer dans un nouveau pays s'accompagne de nombreux changements, et Internet peut être un excellent outil pour vous aider à vous adapter à la vie au Canada. Toutefois, sans précaution, naviguer sur Internet peut vous exposer à des risques en ligne.

Ce guide a pour but de vous aider à mieux comprendre les risques en ligne. Vous y trouverez des conseils pratiques pour rester en sécurité sur Internet, apprendre à reconnaître les signaux d'alerte, protéger vos renseignements personnels et savoir quoi faire si vous pensez être victime d'une fraude ou d'une arnaque.

The Catalyst a élaboré ce guide en collaboration avec OCASI - Ontario Council of Agencies Serving Immigrants et Rogers pour aider les nouveaux arrivants et arrivantes à se protéger en ligne.

Quels sont les risques à connaître en ligne?

Internet fait partie intégrante de la vie moderne, et il est important de comprendre ce qui pourrait compromettre votre sécurité et celle de vos renseignements personnels. Quelques risques possibles :

- La divulgation de vos renseignements personnels ou médicaux
- La fuite ou l'utilisation inappropriée de vos informations financières
- L'utilisation inappropriée ou la manipulation d'images que vous partagez
- Le harcèlement

Des cybercriminels peuvent aussi tenter de vous arnaquer, de vous exploiter ou de vous intimider en ligne.

Vos renseignements personnels sont sensibles : il est crucial de les protéger.

Comment savoir ce qui est fiable en ligne

La meilleure façon de vous protéger contre les arnaques ou les fraudes est de reconnaître les activités suspectes, comme les appels ou les messages de sources inconnues. Avant de cliquer sur un lien ou de transmettre des informations, posez-vous ces questions :

- Est-ce quelque chose que j'attendais?
- Est-ce que je connais l'expéditeur et semble-t-il légitime?
- Est-ce qu'on me demande des renseignements personnels ou sensibles?
- Est-ce qu'on utilise la peur, les menaces, l'urgence ou la coercition pour me pousser à agir ou à fournir des informations?

Ces signaux doivent vous inciter à la prudence. Prenez un moment pour faire les vérifications nécessaires.

Dans le doute, ne répondez pas.

Quelques pistes de vérification

- Cherchez la page officielle ou le numéro de téléphone par une autre source pour confirmer la légitimité de l'expéditeur.
  - Certaines agences gouvernementales, comme l'Agence du revenu du Canada, disposent de pages pour vérifier si elles vous ont réellement contacté.
- Si on vous envoie un lien ou une pièce jointe, placez le curseur de votre souris dessus.
  - Remarque : Cela fonctionne uniquement sur ordinateur, pas sur un téléphone mobile. L'URL ou le nom semble-t-il cohérent? En cas de doute, ne cliquez pas et vérifiez auprès d'une source officielle.
- Attention aux usurpateurs qui prétendent être des membres de votre famille pour obtenir des renseignements.
  - Vous pouvez convenir avec vos proches d'un mot de sécurité secret pour confirmer leur identité.
- La règle clé : faire une pause et mener des vérifications avant de faire quoi que ce soit.

Comment rester en sécurité en ligne

Au-delà des bonnes habitudes, utiliser les bons outils et réglages est essentiel pour votre sécurité. Voici quelques mesures à prendre :

1. Sécurisez vos comptes

- Utilisez des phrases ou des mots de passe complexes.
- Activez l'authentification multifactorielle (par un deuxième appareil, un code ou par biométrie).
- Vérifiez les paramètres de confidentialité de vos médias sociaux.
- Inscrivez-vous aux alertes de fraude de votre institution bancaire.

2. Sécurisez vos connexions

- Protégez votre WiFi en remplaçant le mot de passe par défaut par un mot de passe robuste.
- Désactivez le Bluetooth quand vous ne l'utilisez pas.
- Si vous devez utiliser un WiFi public, recourez à un réseau privé virtuel (*VPN* en anglais).

3. Sécurisez vos appareils

- Créez des mots de passe, des codes, des phrases secrètes ou des numéros d'identification personnels (NIP) robustes.
- Installez un logiciel de sécurité fiable sur tous vos appareils.
- Maintenez vos applications et vos logiciels à jour, et supprimez ceux que vous n'utilisez pas.
- Ne laissez jamais vos appareils sans surveillance et évitez de les prêter à des inconnus.
- Sauvegardez vos données et logiciels importants.

Rendez-vous sur le site pensezcybersecurite.ca pour en savoir plus sur les mesures de sécurité recommandées par le Gouvernement du Canada.

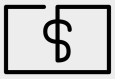
Mesures à prendre si vous croyez être victime d'une fraude en ligne

Si vous croyez avoir été victime d'une arnaque, d'une fraude en ligne ou de tout autre cybercrime, voici ce que vous devez faire :

1. Prenez des précautions supplémentaires selon la situation (changez vos mots de passe, analysez vos appareils, vérifiez vos relevés bancaires pour repérer des transactions inhabituelles).
2. Contactez votre banque ou votre compagnie de carte de crédit si vos comptes sont compromis.
3. Pour les incidents graves, appelez le numéro réservé aux situations non urgentes de votre service de police local.
4. Signalez toute fraude ou arnaque au Centre antifraude du Canada : https://antifraudcentre-centreantifraude.ca/index-fra.htm.

Voici des exemples d'incidents à signaler au service de police local, à vos institutions financières et au Centre antifraude du Canada :

Vol d'identité :
Quelqu'un a utilisé vos renseignements personnels pour ouvrir des comptes ou emprunter en votre nom. Contactez le service de police local et vos institutions financières.



Fraude financière :
Vous savez ou suspectez que de l'argent a été volé dans votre compte bancaire. Contactez le service de police local, vos institutions financières et le Centre antifraude du Canada.

Hameçonnage et piratage psychologique :
Quelqu'un vous a manipulé pour avoir accès à vos comptes.

Harcèlement en ligne et cyberintimidation :
Vous avez reçu des messages menaçants ou vos renseignements personnels ont été divulgués en ligne.

Comment la population étudiante peut rester en sécurité en ligne

La population étudiante est une cible de choix pour les cybercriminels et les arnaqueurs. Certains cherchent à les appâter avec des promesses alléchantes : amélioration des notes, prêts étudiants à bas coût, corrigés gratuits pour réussir des examens. Si une offre semble trop belle pour être vraie, c'est probablement une arnaque.

Votre numéro étudiant, vos dossiers et vos renseignements financiers valent de l'or pour les fraudeurs. Ne transmettez ces informations qu'à votre établissement scolaire. Si vous croyez qu'elles ont été communiquées sans votre autorisation, signalez-le au service de sécurité de votre école ou à toute administration responsable – vous n'êtes probablement pas la seule victime.

Aidez votre famille à rester en sécurité en ligne

Les enfants peuvent être exposés à des risques importants sur Internet, comme être manipulés par des inconnus, subir du harcèlement, de la cyberintimidation ou se faire demander d'envoyer des photos personnelles.

Ces situations peuvent être très perturbantes. Il est donc essentiel d'en parler ouvertement avec votre enfant et de lui expliquer comment rester prudent en ligne. Rappelez-lui de ne jamais transmettre de renseignements personnels, de photos ou de vidéos à des personnes qu'il ne connaît pas et de vous prévenir immédiatement si quelque chose en ligne le met mal à l'aise.

Ressources additionnelles

En plus de vérifier les paramètres de sécurité des comptes de votre enfant et de signaler toute menace aux autorités, pensez aussi à signaler tout cas d'exploitation d'enfants en ligne sur cybertip.ca/fr.

Si votre enfant a besoin de parler à quelqu'un de ce qui lui arrive en ligne, suggérez-lui de se tourner vers des ressources qui peuvent l'aider.

- Jeunesse, J'écoute, le seul service de santé mentale en ligne accessible en tout temps au Canada offrant un soutien gratuit, multilingue et confidentiel. Il suffit de texter PARLER au 686868 ou d'aller sur le site jeunessejecoute.ca.

- Allo J'écoute, qui offre en plus de 100 langues des services de soutien confidentiels pour la population étudiante de niveau postsecondaire de l'Ontario et de la Nouvelle-Écosse. Il suffit d'aller sur le site allojecoute.ca.

Conclusion

Internet offre de nombreux avantages, mais les cybercriminels cherchent toujours des occasions d'exploiter les personnes en ligne. Vous avez le pouvoir de vous protéger, ainsi que vos proches, en posant des questions et en adoptant des habitudes sécuritaires en ligne.

Ce guide présente des exemples et des conseils pour vous aider à rester en sécurité en ligne. Pour obtenir d'autres ressources, consultez nos guides électroniques pour les nouveaux arrivants et arrivantes, la population étudiante et les familles.

Accédez à d'autres ressources (anglais seulement)
cybersecurecatalyst.ca/cyber-resources-for-educators-schools

Termes à connaître

Voici un glossaire des expressions et des mots courants utilisés dans ce guide. Vous y trouverez des définitions claires qui vous aideront à rester en sécurité en ligne.

Arnaque :
Fausse offre ou message frauduleux qui a pour but de vous inciter à donner quelque chose de précieux, comme de l'argent ou des renseignements personnels.

Menace :
Quand quelqu'un dit ou fait quelque chose qui vous fait sentir en danger, souvent pour vous intimider ou vous forcer à agir.

Coercition :
Quand quelqu'un vous pousse ou vous oblige à faire quelque chose que vous ne voulez pas faire.

URL :
Adresse que vous saisissez dans un navigateur pour aller sur un site web, par exemple pensezcybersecurite.ca.

Usurpateurs :
Personnes qui se font passer pour quelqu'un d'autre (proche ou entreprise) afin de gagner votre confiance.

Mot de sécurité :
Mot secret que vous convenez d'utiliser avec une personne de confiance pour confirmer qu'il s'agit bien d'elle.

Authentification multifactorielle :
Mesure de sécurité qui demande plus qu'un mot de passe, comme un code envoyé sur votre téléphone ou une empreinte digitale.

Bluetooth :
Technologie sans fil qui permet à des appareils (comme des écouteurs ou des haut-parleurs) de se connecter sans câble.

Phrase secrètes / Phrase de passe :
Mot de passe composé de plusieurs mots, chiffres ou symboles, ce qui le rend plus difficile à deviner, par exemple Guide!$écuritéNouveauxArrivants2025.

NIP (Numéro d'identification personnel) :
Code numérique court, souvent de 4 à 6 chiffres, utilisé pour accéder à des comptes ou à des appareils (comme un téléphone).

Logiciel de sécurité :
Applications ou programmes installés sur vos appareils pour vous protéger contre les virus et logiciels malveillants.

Hameçonnage et piratage psychologique :
Techniques utilisées par des criminels pour vous tromper et obtenir vos renseignements personnels, souvent par appel téléphonique, courriel, SMS ou sites web frauduleux.

Cyberintimidation :
Quand quelqu'un utilise Internet pour harceler, menacer ou humilier une autre personne.

Mot de passe robuste :
Mot de passe long et unique composé de lettres, de chiffres et de symboles, sans détails personnels, pour qu'il soit difficile à deviner ou à pirater.

Renseignements personnels :
Toute information qui permet de vous identifier, comme votre nom, votre adresse, votre numéro de téléphone ou votre établissement scolaire. Les cybercriminels peuvent s'en servir pour voler votre identité ou commettre des fraudes.

Renseignements médicaux :
Informations contenant vos antécédents médicaux, visites chez le médecin ou détails d'assurance. Ces données sont privées et précieuses pour les cybercriminels, qui peuvent les utiliser pour frauder.

La cybersécurité pour tout le monde

Visitez notre site (anglais seulement)

cybersecurecatalyst.ca

Toronto Metropolitan University

cybersecure catalyst

ROGERS

Etablissement.Org
Bienvenue en Ontario