7e à 12e année

La sécurité en ligne : comprendre les risques

Adaptation française : Centre franco-ontarien de ressources pédagogiques

ROGERS cybersecure catalyst

Internet est un endroit où l'on peut apprendre, communiquer avec ses amies et amis et sa famille, jouer à des jeux, ou écouter sa musique ou ses émissions préférées en continu. On peut y accéder de n'importe où, n'importe quand et à partir de n'importe quel appareil (téléphone, tablette, ordinateur). Toutefois, Internet et les appareils que l'on utilise pour y accéder ne sont pas sans risque; sans la sensibilisation appropriée, on peut s'exposer aux divers dangers du Web.

Les adolescentes et adolescents, tout particulièrement, sont souvent la cible des cybercriminelles et des cybercriminels, car elles et ils n'ont pas encore d'antécédents de crédit; le vol d'identité et l'ouverture de comptes de cartes de crédit à leur nom sont donc un jeu d'enfant. Il faut prendre conscience du danger et prendre soin de sa sécurité en ligne.

Cette ressource présente des renseignements sur la sensibilisation à la sécurité, afin de te donner les connaissances nécessaires pour comprendre les risques d'Internet, pour toi et tes appareils. Tu éviteras ainsi d'être victime de fraude ou de vol d'identité, ou de voir tes appareils infectés par des virus ou d'autres maliciels.

A DÉFINITIONS

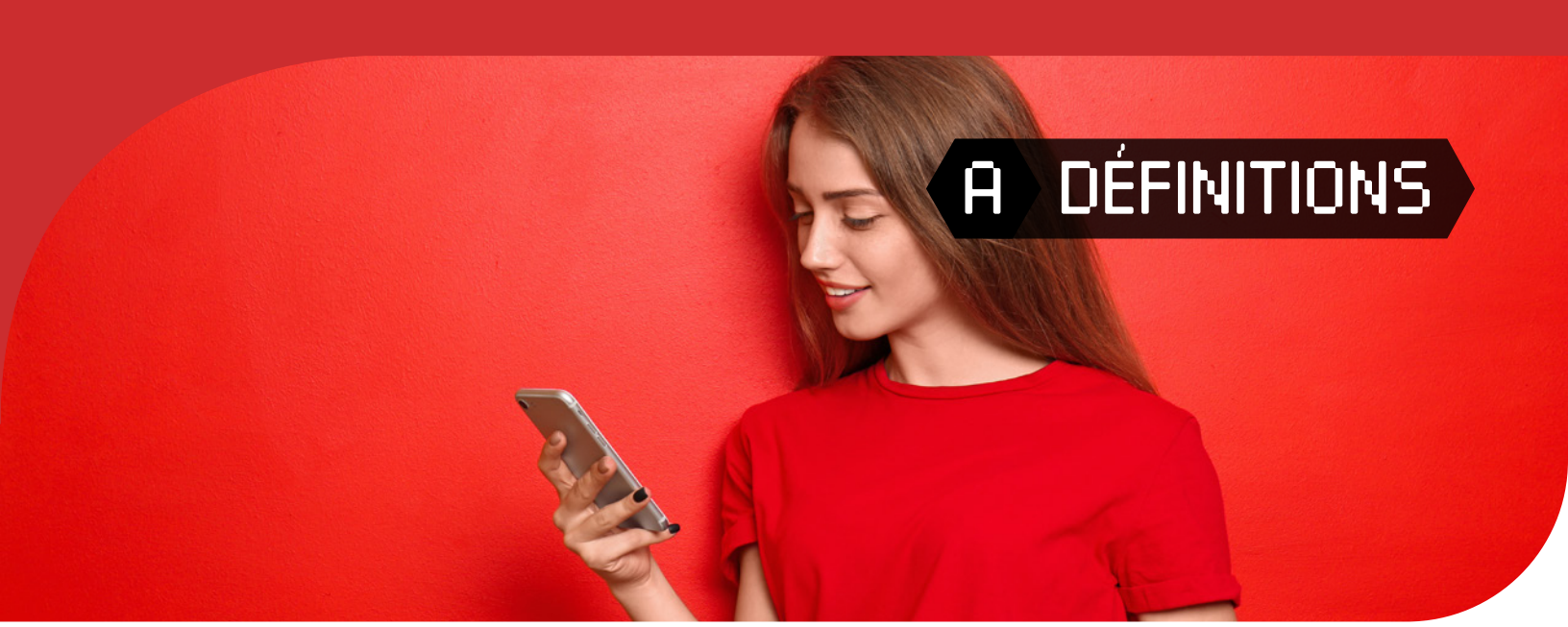
Les dangers d'Internet ont de multiples visages (fraude, vol d'identité, maliciels ou virus), et se manifestent lorsque l'on utilise des appareils connectés. Afin de protéger tes renseignements et tes comptes privés, tu dois aussi protéger tes appareils. Consulte les définitions pour connaître les termes et problèmes courants auxquels faire attention.

Fraude

Les fraudeuses et fraudeurs, des personnes qui s'adonnent à des manœuvres ou à des ruses malhonnêtes, t'incitent à faire des téléchargements ou des achats, te demandent de répondre à des questionnaires et t'offrent des biens comme de l'argent, des prix, des consoles de jeu ou des tablettes gratuites.

Vol d'identité

Les cybercriminelles et cybercriminels en apprennent le plus possible sur tes renseignements privés ou personnels, puis les utilisent pour se faire passer pour toi et ouvrir des comptes bancaires à ton nom. Les fraudeuses et fraudeurs peuvent aussi prendre le contrôle de tes comptes de jeu en ligne et de tes comptes de médias sociaux.



A DÉFINITIONS

Virus

Codes conçus pour se copier discrètement dans les dossiers ou programmes d'ordinateur dans le but de détruire des données et de perturber le fonctionnement des appareils et des réseaux.

Maliciel

Type de virus installé secrètement dans le but de voler tes renseignements privés, d'espionner ton appareil ou d'en crypter le contenu jusqu'à ce que de l'argent soit versé à la malfaitrice ou au malfaiteur.

B PERTINENCE

Éviter les risques en ligne

Les risques se cachent pratiquement partout : extensions et modules du navigateur, courriels, messages textes ou privés, liens infectés, publications sur les médias sociaux, salles de clavardage, publicités, applications, plateformes de jeu en ligne, etc.

Les stratagèmes deviennent de plus en plus sophistiqués, et tu peux divulguer sans le savoir des renseignements confidentiels qui permettent aux cybercriminelles et cybercriminels d'accéder à tes comptes ou d'en créer de nouveaux à ton nom.

Pour t'inscrire à un nouveau jeu ou te créer un nouveau compte, tu as besoin d'une adresse courriel. Malheureusement, les fraudeuses et les fraudeurs utilisent le plus souvent les courriels et les messages textes pour envoyer des communications dans l'intention de tromper les gens. Ce type de communication est appelé « pourriel ».

Fraudeuses et fraudeurs

Personnes qui envoient des pourriels ou qui participent à des mensonges en incitant les gens à leur donner quelque chose, comme des renseignements ou de l'argent.

Pourriel

Communication indésirable ou non sollicitée, généralement sous forme de courriels ou de messages textes.

Hameçonnage

Tentative frauduleuse ou fraude visant une utilisatrice ou un utilisateur d'Internet dont le but est d'obtenir des renseignements privés ou personnels à des fins illégales.

Mystification

Communication qui semble provenir d'une source connue, par exemple une connaissance, alors qu'en réalité, elle émane d'une source inconnue, comme une fraudeuse ou un fraudeur.

PERTINENCE

Prévention des risques en ligne

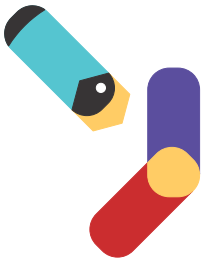
Suis les étapes recommandées ci-dessous pour éviter les risques pour toi et tes appareils. Ces astuces portent expressément sur les courriels; toutefois, beaucoup de ces règles peuvent aussi s'appliquer à d'autres formes de communications!

- **Ne réponds pas aux pourriels.** Ainsi, la fraudeuse ou le fraudeur ne saura pas que le compte est actif!

- **Ne clique sur aucun lien;** passe plutôt ton curseur sur le lien pour voir le vrai site Web. Si le message indique que ton compte a été verrouillé, ouvre ton navigateur et connecte-toi directement à partir du site de l'organisation pour voir s'il y a réellement un problème.

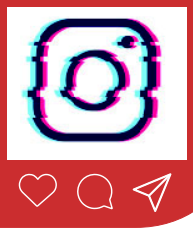
- **Ne clique pas sur les pièces jointes et ne les télécharge pas!** Contacte l'expéditrice ou l'expéditeur directement pour en savoir plus sur une pièce jointe inattendue avant de l'ouvrir.

- **Vérifie l'adresse courriel de l'expéditrice ou de l'expéditeur.** Passe ton curseur sur l'adresse courriel ou le nom de l'expéditrice ou de l'expéditeur; si le courriel provient d'une amie ou d'un ami, vérifie que l'adresse est la bonne. En cas de doute, vérifie! Communique directement avec l'expéditrice ou l'expéditeur pour savoir si le courriel provient réellement d'elle ou de lui.



À ne pas oublier!

Si le courriel ressemble à ceci : serviceclientele@instagram.cz, il est probable qu'il s'agisse d'une mystification, puisqu'un courriel provenant d'Instagram se terminerait par « instagram.com ».



B PERTINENCE

Prévention des risques en ligne

Suis les étapes recommandées ci-dessous pour éviter les risques pour toi et tes appareils. Ces astuces portent expressément sur les courriels; toutefois, beaucoup de ces règles peuvent aussi s'appliquer à d'autres formes de communications!

- **Vérifie l'objet :** Si tu reçois un courriel d'une amie ou d'un ami ou d'un membre de ta famille dont l'objet semble urgent (par exemple, « J'ai besoin de ton aide »), appelle la personne directement. Si tu reçois un courriel d'une entreprise avec l'objet « Votre compte a été suspendu », dis-le à un parent ou à une tutrice ou à un tuteur, qui pourra vérifier le tout.

- **Cherche les erreurs d'orthographe et de grammaire :** Normalement, les vraies entreprises envoient des courriels ne contenant aucune erreur d'orthographe ou de grammaire.

- **Méfie-toi des demandes de renseignements personnels :** Il ne faut jamais communiquer de renseignements personnels (noms d'utilisateur, mots de passe, numéros de compte, etc.)

- **Dossier de courrier indésirable :** Entraîne ta boîte de réception à envoyer automatiquement les pourriels dans ton dossier de courrier indésirable en les y transférant chaque fois que tu en reçois un.

- **Bloque l'expéditrice ou l'expéditeur :** De cette façon, tu ne recevras plus de courriels de sa part.

- **Supprime le faux courriel :** Ne le garde pas dans ta boîte de réception; toi-même ou quelqu'un d'autre pourriez l'ouvrir.

Le savais-tu?

Tu peux contribuer à la lutte contre la fraude, les pourriels et les menaces électroniques en les signalant à l'adresse pourriel@combattrelepourriel.gc.ca.

Socialisation sécuritaire sur Internet

Socialiser avec des amies ou des amis sur les sites de jeu ou les médias sociaux est une façon amusante d'échanger avec d'autres. Malheureusement, les cybercriminelles et les cybercriminels peuvent prendre le contrôle de ton profil ou en créer un nouveau à ton nom. Leur but est d'envoyer de faux messages à tes amies et amis et à tes abonnées et abonnés, les invitant à envoyer de l'argent ou à installer des logiciels malveillants sur leurs appareils – tout ça, en se faisant passer pour toi.

Pour te protéger et protéger tes renseignements et tes appareils, consulte cette liste de contrôle :

- **En ligne, les adolescentes et les adolescents devraient seulement jouer à des jeux, clavarder et suivre ou ajouter des amies et amis qu'elles et ils connaissent dans la vraie vie!** C'est facile d'être flatté ou curieux à propos d'une personne populaire et ayant beaucoup d'influence, mais il est important de supprimer les demandes d'amitié de personnes que l'on ne connaît pas personnellement.

- **Ne te laisse pas tenter par les sites Web ou les publicités qui incitent à se connecter ou à cliquer sur des liens externes, des questionnaires ou des concours**, en indiquant par exemple « découvre qui parle de toi » ou « qui a le béguin pour toi », ou les messages te disant de cliquer sur des liens, car « tu dois absolument voir ça! »

APPEL À L'ACTION

Détournement de clic

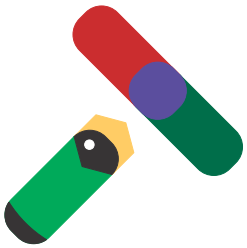
Méthode malveillante, aussi appelée « *clickjacking* », qui consiste à inciter quelqu'un à cliquer sur quelque chose qui n'est pas ce qu'elle ou il perçoit, et qui peut révéler des renseignements confidentiels ou permettre à d'autres de prendre contrôle de son ordinateur.

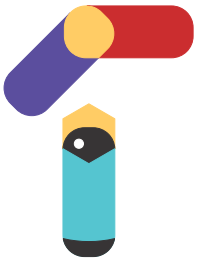
Socialisation sécuritaire sur Internet

- **Fais particulièrement attention aux liens et aux pièces jointes** provenant de plateformes de clavardage de jeux en ligne et des médias sociaux, même s'ils sont envoyés par une amie ou un ami. Si tu n'es pas certain à 100 %, appelle d'abord l'expéditrice ou l'expéditeur ou envoie-lui un message texte!

- **Ne clique que sur les publications de gens que tu connais dans la vraie vie ou de comptes fiables.** Le simple fait d'aimer et de partager une publication piratée sur les médias sociaux, ou de cliquer par inadvertance dessus, peut entraîner la publication automatique de pourriels, de maliciels ou de publications malveillantes sur ton profil. C'est ce qu'on appelle le détournement de clic.

- **Prends garde à ce que tu partages!** Ne divulgue jamais de renseignements personnels ou privés sur les réseaux sociaux, même sur un compte privé, car tu ne sais jamais si le compte d'une amie ou d'un ami a été piraté, et si la ou le pirate informatique a accès à tes renseignements.





Navigation sécuritaire sur Internet

Les sites Web offrent un monde de plaisirs et d'exploration, mais ils exposent aussi à bien des risques inattendus. Pour te protéger, suis ces étapes simples :

- **Bloque les fenêtres et les bannières publicitaires :** Ces distractions irritantes apparaissent entre autres sur les sites Web, dans les jeux et dans les vidéos; tu peux les bloquer en mettant à jour les réglages de ton navigateur (par exemple : Internet Explorer, Google Chrome, Firefox). Cela t'évitera de cliquer par inadvertance sur l'une d'elles. Tu peux aussi installer des bloqueurs de publicité, mais n'oublie pas de te renseigner avant de les installer!

- **Navigue sur les sites Web qui commencent par « https » ou qui sont précédés d'un symbole de cadenas :** Ce sont les sites Web les plus sûrs, bien que la protection ne soit pas garantie!

- **Ajoute à tes favoris** les sites Web que tu consultes souvent.

- **Active la recherche sécurisée** sur ton navigateur.

- **Supprime régulièrement les témoins** enregistrés sur ton navigateur.

Témoins

Les témoins, aussi appelés « *cookies* », sont conçus spécialement pour permettre aux navigateurs Web de suivre, de personnaliser et d'enregistrer les renseignements à propos de la session de chaque utilisatrice et utilisateur. Une session, c'est simplement le temps passé sur un site Web.

Les fraudeuses et les fraudeurs ont perfectionné leurs techniques de mystification ou d'usurpation de vrais sites Web. Ces sites factices imitent les vrais de façon si convaincante qu'il peut être difficile de distinguer le vrai du faux. Tu as un doute? N'oublie pas ce qui suit :

- **Vérifie l'adresse du site Web deux fois plutôt qu'une :** Les fraudeuses et les fraudeurs peuvent faire passer un site Web pour le vrai simplement en changeant une lettre (par exemple : remplacer un « o » par un « zéro ») ou en changeant la fin de l'adresse du site Web (par exemple : changer « .com » par « .net »).

- **Vérifie le certificat du site Web :** Assure-toi que le site Web que tu consultes est le bon en cliquant sur le symbole de cadenas dans la barre d'adresse de ton navigateur et en t'assurant que le certificat est valide.

Téléchargements sécuritaires

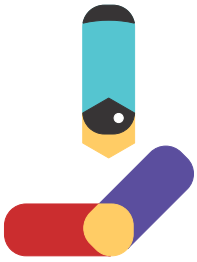
Il y a tant à télécharger, et tant de choses gratuites! Cela peut sembler excitant, mais il ne faut pas oublier que gratuit ne veut pas forcément dire sécuritaire. Mis à part les problèmes relatifs aux droits d'auteur (et la possibilité que le contenu soit acquis illégalement), les jeux, les fonds d'écran, les sonneries, les films et la musique que tu télécharges gratuitement pourraient être secrètement combinés à des maliciels et des virus. Lorsque tu télécharges, protège-toi et protège tes appareils :

- **Ne télécharge qu'à partir de sites Web fiables et réputés.** Vérifie toujours l'adresse du site Web avant tout! Si tu as un doute, cherche le contenu sur un site Web plus sûr. S'il n'est pas accessible ailleurs, méfie-toi.

- Prends le temps de **vérifier soigneusement le lien de téléchargement** en plaçant ton curseur sur le lien de façon à révéler l'adresse Web.

- **On pourrait t'inciter à télécharger des programmes d'installation ou des plugiciels** en plus du programme que tu souhaites obtenir. Habituellement, rien n'est requis pour télécharger quoi que ce soit; fais bien tes recherches avant de procéder.

- **Avant de télécharger, sauvegarde le contenu de ton appareil.** Analyse le fichier à l'aide de ton programme de détection de virus ou de maliciel avant de le télécharger, et aussi après, pour plus de certitude.



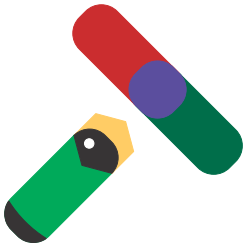
Le savais-tu?

Placé au début d'une adresse Web, « HTTPS » est l'abréviation de « Hypertext Transfer Protocol Secure »; c'est une façon assez technique de dire qu'il y a une communication sécurisée dans un réseau informatique.

ROGERS cybersecure catalyst

C APPEL À L'ACTION

Même si tu t'es bien renseigné et que tu as le logiciel de sécurité le plus récent, tu ne dois pas baisser ta garde! Tout comme dans la vraie vie, tu pourrais avoir les meilleurs dispositifs de sécurité à la maison pour te protéger – les meilleurs verrous, projecteurs, caméras, chiens de garde, agents de sécurité armés et portails – mais si tu laisses entrer la première personne venue, tu peux t'exposer à un risque. Le fait de savoir repérer et éviter ces risques t'aidera, toi et les autres, à être en sécurité en ligne.



Qu'as-tu appris?
Quelles sont les fraudes dont tu as entendu parler? Quelles sont les meilleures façons de t'en protéger?

Astuce!

Si tu télécharges un virus ou un maliciel par inadvertance, déconnecte ton appareil d'Internet et ferme-le immédiatement. Consulte une technicienne professionnelle ou un technicien professionnel pour régler le problème.

ACTIVITÉ 1

Les activités sont une bonne façon de t'exercer et de mettre en pratique tes connaissances sur le sujet abordé dans la ressource.

Trouve la fraude!

Jette un coup d'œil à l'exemple de courriel ci-dessous.
Peux-tu repérer tous les signes indiquant que ce courriel est une fraude?

NETFLIX

Votre compte a été suspendu.

Veuillez mettre à jour vos informations de facturation.

Bonjour,

Désolé pour l'interruption, mais nous rencontrons des problèmes avec vos informations de facturation actuelles. Nous réessaierons, mais en attendant, vous devrez peut-être mettre à jour vos informations de paiement afin d'éviter la suspension de votre compte.

METTRE À JOUR LE COMPTE

Nous sommes là si vous avez besoin d'aide. Visitez le centre d'aide pour de plus amples renseignements ou communiquez avec nous.

- L'équipe Netflix

SIGNES DE FRAUDE :

1) _____

2) _____

3) _____

4) _____

RÉPONSES

1) « Bonjour » : C'est une salutation très informelle et générique; une entreprise de bonne réputation comme Netflix s'adresse généralement à une cliente ou un client en utilisant son nom!

2) <METTRE À JOUR LE COMPTE> : Les entreprises t'invitent habituellement à te connecter à ton compte dans un nouvel onglet ou dans un navigateur, pas directement à partir d'un lien dans un courriel.

3) « Visitez le centre d'aide pour de plus amples renseignements ou communiquez avec nous » : Les entreprises te suggéreraient d'aller directement sur leur page Web ou te donneraient l'adresse courriel ou le numéro de téléphone de leur service à la clientèle.

4) « L'équipe Netflix » : Ce n'est pas une signature habituelle; c'est presque trop informel!

ACTIVITÉ 2

Situations problématiques

Réfléchis aux situations qui suivent en utilisant tes nouvelles connaissances sur la sécurité des appareils. Que ferais-tu ensuite?

1. Tu reçois un courriel te prévenant que ton compte a été suspendu. Que fais-tu?

a. L'ignorer
b. Cliquer sur le lien dans le courriel
c. Se connecter au compte à partir d'un navigateur pour voir directement si c'est vrai
d. Aucune de ces réponses

2. Tu télécharges une nouvelle application sur ta tablette, et télécharges un virus par erreur. Que fais-tu?

a. Déconnecter l'appareil d'Internet immédiatement
b. Fermer l'appareil et le confier à une technicienne professionnelle ou à un technicien professionnel
c. Ignorer le problème jusqu'à ce qu'il disparaisse
d. Les réponses a) et b)

3. Tu reçois un message privé d'une admiratrice secrète ou d'un admirateur secret avec un lien vers son vidéoclip préféré. Que fais-tu?

a. Faire suivre le message à tes amies et amis
b. Supprimer le message
c. Ouvrir le message et cliquer sur le lien
d. Toutes ces réponses

[réponses] 1. C, 2. D, 3. B

POUR EN SAVOIR PLUS

Pour en savoir plus sur la cybersécurité ou pour poursuivre la conversation et l'apprentissage, consulte le site du Centre canadien pour la cybersécurité :

https://www.cyber.gc.ca/fr/

Jeunesse, J'écoute

Pour de l'aide, envoyez un message texte au 686868 ou téléphonez au 1-800-668-6868 partout au Canada, 24 heures sur 24, 7 jours sur 7, ou accédez aux ressources en ligne sur jeunessejecoute.ca.

Toronto Metropolitan University

ROGERS cybersecure catalyst

Adaptation française : Centre franco-ontarien de ressources pédagogiques