4e à 6e année

La sécurité en ligne : comprendre les risques

Adaptation française : Centre franco-ontarien de ressources pédagogiques

ROGERS cybersecure catalyst

Internet est un endroit où les enfants peuvent apprendre; communiquer avec leurs amies et amis et leur famille par messagerie, par courriel ou sur les médias sociaux; jouer à des jeux; ou écouter leur musique et leurs émissions préférées en continu. Il est possible d'y accéder de n'importe où, n'importe quand et à partir de n'importe quel appareil (téléphone, tablette, ordinateur). Cependant, l'utilisation d'appareils connectés à Internet n'est pas sans risques, et s'ils n'y sont pas correctement sensibilisés, les enfants peuvent s'exposer aux divers dangers du Web, comme la fraude ou le vol d'identité, ou voir leurs appareils infectés par des virus ou d'autres maliciels.

Cette ressource fournit des renseignements et des conseils aux parents, aux tutrices et aux tuteurs pour les aider à expliquer aux enfants comment repérer les risques liés à l'utilisation d'appareils connectés à Internet et comment socialiser, naviguer et télécharger du contenu en toute sécurité.

A DÉFINITIONS

Pour protéger leurs renseignements privés, les enfants doivent aussi protéger leurs appareils. Consultez les définitions ci-dessous pour comprendre ces risques et savoir les reconnaître :

Fraude

- Les fraudeuses et fraudeurs, des personnes qui s'adonnent à des manœuvres ou à des ruses malhonnêtes, incitent les enfants à faire des téléchargements ou des achats, leur demandent de répondre à des questionnaires et leur offrent des biens comme de l'argent, des prix, des consoles de jeu ou des tablettes gratuites.

Virus

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

Vol d'identité

- Les cybercriminelles et cybercriminels en apprennent le plus possible sur les renseignements privés ou personnels des enfants, puis les utilisent pour se faire passer pour eux et ouvrir des comptes bancaires à leur nom. Les fraudeuses et fraudeurs peuvent aussi prendre le contrôle de leurs comptes de jeux en ligne et de leurs comptes de médias sociaux.

Maliciel

- Type de virus installé secrètement dans le but de voler les renseignements privés d'une ou d'un enfant, d'espionner son 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

- Il importe que les enfants soient conscients des messages qu'ils reçoivent sur leurs appareils, de la véritable identité de l'expéditrice ou de l'expéditeur et des gestes qu'on leur demande de poser.

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

- Les pourriels sont souvent envoyés par des fraudeuses et fraudeurs qui utilisent les courriels, les messages privés sur les médias sociaux ou les messages textes (si les enfants ont déjà un téléphone cellulaire) pour inciter leurs victimes à cliquer sur des liens dangereux. Ces personnes peuvent aussi joindre des virus à leurs messages afin d'infecter des appareils et des comptes, ce qui empêche les enfants de les utiliser.

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.

- Ces messages ont l'air réels et peuvent amener les enfants à divulguer des renseignements personnels et privés, ce qui permet aux fraudeuses et fraudeurs de prendre le contrôle de leurs comptes. On appelle ce type de fraude de l'« hameçonnage ».

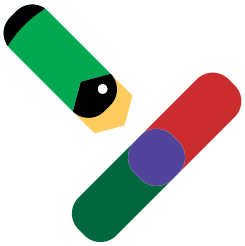
Hameçonnage : Tentative frauduleuse ou fraude effectuée par une utilisatrice ou un utilisateur d'Internet dans le but d'obtenir des renseignements privés ou personnels à des fins illégales.

À ne pas oublier!

Demandez aux enfants d'imaginer qu'ils sont au terrain de jeux et qu'une personne inconnue leur offre une tablette gratuite. Tout ce qu'ils doivent faire pour l'avoir, c'est lui donner leur nom, leur adresse et leur numéro de téléphone. Pensez-vous qu'ils le feraient? Il est très probable que non! Ce devrait être pareil en ligne lorsqu'ils se retrouvent devant des concours, des publicités ou des courriels qui paraissent trop beaux pour être vrais.

PERTINENCE

Prévenir les risques en ligne

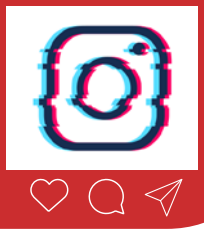


Lisez cette liste de conseils avec vos enfants pour les aider à éviter les risques pour eux-mêmes et leurs appareils. Ces conseils concernent les courriels en particulier, mais beaucoup s'appliquent aussi à d'autres formes de communications!

- Ne pas répondre aux pourriels : Ainsi, la fraudeuse ou le fraudeur ne saura pas que le compte de l'enfant est actif!
- Ne cliquer sur aucun lien : Dites à vos enfants de passer le curseur sur le lien pour voir l'adresse. Si le message porte sur un problème avec un compte, par exemple Fortnite ou TikTok, les enfants doivent ouvrir leur navigateur ou l'application en question et se connecter directement à leur compte pour vérifier s'il y a vraiment quelque chose qui cloche.
- Ne pas cliquer sur les pièces jointes et ne pas les télécharger : Les enfants doivent communiquer directement avec l'expéditrice ou l'expéditeur et lui demander si le message provient vraiment d'elle ou de lui. Mieux vaut prévenir que guérir!
- Vérifier l'adresse courriel de l'expéditrice ou de l'expéditeur : Si le courriel provient d'une amie ou d'un ami ou d'un membre de la famille, ou s'il concerne l'école, les enfants doivent vérifier que l'adresse correspond à celle utilisée habituellement par cette personne.
- Vérifier l'objet : Si les enfants reçoivent un courriel d'une personne connue et que l'objet semble urgent (p. ex. : « J'ai besoin de ton aide »), il vaut mieux l'appeler ou lui envoyer un message texte directement!
- Chercher les erreurs d'orthographe et de grammaire : Si les enfants reçoivent un courriel provenant d'une réelle entreprise, le texte ne contiendra normalement pas de fautes d'orthographe ou de grammaire.
- Faire attention aux demandes de renseignements personnels : Les enfants ne doivent jamais divulguer de renseignements personnels, que ce soit leurs noms d'utilisatrice ou d'utilisateur, leurs mots de passe ou leurs numéros de compte.
- Envoyer les courriels dans la boîte de pourriels : Les enfants peuvent faire en sorte que leur boîte de réception envoie automatiquement les pourriels dans le dossier de courrier indésirable en les y plaçant chaque fois qu'ils en reçoivent.

À ne pas oublier!

Si l'adresse courriel ressemble à « serviceclientele@instagram.cz », il est probable qu'elle soit frauduleuse, car les courriels d'Instagram proviennent habituellement d'une adresse se terminant par « instagram.com »



C APPEL À L'ACTION

Le saviez-vous?

Si des enfants tombent sur ce genre de courriels, leurs parents ou tutrices et tuteurs peuvent se joindre 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

- Les enfants peuvent utiliser des appareils de nombreuses façons pour socialiser en ligne : jouer à des jeux virtuels avec leurs amies et amis, ou publier des photos de leurs animaux de compagnie sur les médias sociaux. Les fraudeuses et fraudeurs utilisent souvent les astuces mentionnées plus haut : elles et ils se font passer pour quelqu'un d'autre et envoient des demandes d'amitié, d'abonnement ou de messages.

Pour protéger les enfants sur ces plateformes, demandez-leur de se référer à la liste suivante lorsqu'ils socialisent en ligne :

- **En ligne, les enfants devraient seulement interagir avec des personnes qu'ils connaissent dans la vraie vie, que ce soit pour jouer à des jeux, clavarder, s'abonner à des comptes ou faire des demandes d'amitié!** Il est facile d'être flatté ou curieux à propos d'une personne populaire ou très influente, mais il est important de supprimer les demandes d'amitié de gens que les enfants ne connaissent pas personnellement.
- **Il ne faut pas se laisser tenter par les sites Web ou les publicités qui demandent de lier un compte ou de cliquer sur des liens externes, des questionnaires ou des concours,** par exemple ceux qui disent « découvrez qui parle de vous » ou « découvrez qui a un faible pour vous », ou les messages qui demandent aux enfants de cliquer sur un lien pour voir quelque chose de génial.
- **Il faut faire particulièrement attention aux liens et aux pièces jointes** provenant des plateformes de clavardage de jeux et des médias sociaux, même s'ils proviennent d'amies ou d'amis. Si les enfants ne sont pas sûrs à 100 %, il vaut mieux appeler l'amie ou l'ami en question ou lui envoyer un message texte d'abord!
- **Les enfants doivent vérifier l'adresse courriel de l'expéditrice ou de l'expéditeur :** Si le courriel provient d'une amie ou d'un ami ou d'un membre de la famille, ou s'il concerne l'école, les enfants devraient vérifier que l'adresse correspond à celle que la personne utilise habituellement.
- **Les enfants ne doivent cliquer que sur les publications de gens qu'ils connaissent 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 dessus par inadvertance, peut rediriger les enfants vers des pourriels ou des maliciels, ou faire en sorte que des publications malveillantes apparaissent sur leur profil.
- **Les enfants doivent être conscients de ce qu'ils publient!** Ils ne doivent jamais divulguer de renseignements personnels ou privés lorsqu'ils socialisent, même quand ils utilisent un compte privé : peut-être que le compte d'une amie ou d'un ami a été piraté sans que les enfants le sachent, et qu'une ou un pirate a accès à leurs renseignements.

Navigation sécuritaire sur Internet

- **Comment les enfants peuvent-ils se protéger lorsqu'ils naviguent sur des sites Web, regardent des vidéos ou jouent à un jeu qu'ils viennent tout juste de télécharger? Les fraudeuses et fraudeurs ont plus d'un tour dans leur sac pour amener les gens à cliquer sur quelque chose qui pourrait contenir un virus, un maliciel ou un logiciel espion.**
- **Assurez-vous que les enfants sont à l'affût de ce qui suit :**

- **Offres :** On trouve beaucoup d'offres de cadeaux, d'argent ou de prix en ligne. Rien n'est réellement gratuit. Il pourrait y avoir un coût caché indésirable, par exemple un virus qui s'installe sur l'appareil.

- **Enregistrement automatique :** Ne permettez pas aux navigateurs, comme Firefox ou Safari, d'entrer (ou de conserver) automatiquement les données des enfants, par exemple leur prénom, leur nom de famille, leur date de naissance ou leur adresse, car ces renseignements risquent d'être transmis à leur insu à d'autres personnes ou à des entreprises.

- **Fenêtres contextuelles et bannières publicitaires :** En plus d'être dérangeantes, elles peuvent contenir des virus, des maliciels ou des logiciel espions. Elles apparaissent sur les sites Web, dans les jeux, et même pendant les vidéos! Les enfants doivent surveiller leurs clics pour éviter les mauvais tours.

- **Questionnaires et concours en ligne :** Bien qu'il puisse être bien tentant pour les enfants de savoir quelle saveur de crème glacée leur correspond le mieux ou quel personnage de Pokémon leur ressemble le plus, ces questionnaires fouineurs n'ont qu'un but : recueillir leurs renseignements personnels et privés, en leur demandant de donner cette information avant de commencer ou de lier l'un de leurs comptes en ligne.

- **Faux sites Web :** Les fraudeuses et fraudeurs peuvent créer de faux sites Web, qui sont souvent très semblables aux originaux : elles et ils espèrent que les gens ne le remarqueront pas, et ainsi entreront leurs renseignements personnels et privés ou installeront accidentellement un virus sur leur appareil. Tenez-vous-en aux sites de confiance. Si les enfants trouvent un site fiable qu'ils prévoient utiliser souvent, demandez-leur de l'ajouter à leurs favoris pour en faciliter l'accès plus tard.

APPEL À L'ACTION

Téléchargements sécuritaires

- **Il y a tant de choses à télécharger sur Internet. Il est possible que les enfants ne sachent même pas que ce qu'ils sont en train de faire est considéré comme un téléchargement. Généralement, lorsqu'ils veulent enregistrer quelque chose sur leur ordinateur, leur tablette ou leur téléphone, ils doivent d'abord le télécharger. Il peut s'agir de versions nouvelles ou mises à jour d'applications mobiles, de photos et de vidéos qu'ils souhaitent conserver pour plus tard ou de documents électroniques.**

- **La plupart de ces téléchargements sont gratuits, ce qui peut paraître excitant, mais rappelez-vous que ce qui est gratuit n'est pas nécessairement sûr. Les jeux, les fonds d'écran, les sonneries, les chansons ou les films gratuits pourraient être infestés de maliciels et d'autres virus sans qu'on s'en rende compte.**

Amorce de conversation : As-tu déjà reçu des pourriels? Comment as-tu réagi? Qu'est-ce que les fraudeuses et fraudeurs souhaitent obtenir en envoyant ce type de messages?

Astuce

Vous ne savez pas comment déterminer si un site est sécuritaire pour les téléchargements? Vérifiez que l'adresse commence par « HTTPS » et qu'il y a un symbole de cadenas dans la barre d'adresse! Lorsque l'adresse d'un site commence par « HTTPS:// », cela signifie que la communication est sécurisée dans un réseau d'ordinateurs.

APPEL À L'ACTION

Prévenir les risques en ligne

Pour protéger vos enfants et leurs appareils, assurez-vous qu'ils prennent les précautions suivantes lorsqu'ils effectuent des téléchargements :

- **Téléchargez uniquement à partir de sites fiables ou de bonne réputation.** Les enfants doivent toujours vérifier l'adresse du site avant tout! N'oubliez pas de vérifier qu'elle commence par « HTTPS » et qu'il y a un symbole de cadenas dans la barre d'adresse.

- **Pour prévenir les problèmes, les enfants devraient idéalement sauvegarder les données de leur appareil avant d'effectuer un téléchargement,** par exemple en enregistrant les dossiers importants sur un disque dur externe ou en copiant les données d'un téléphone sur un ordinateur.

- **Prenez le temps d'observer soigneusement le lien de téléchargement.** Les enfants doivent passer le curseur sur le lien pour voir l'adresse avant de cliquer. Est-ce que l'adresse correspond? Est-elle étrange ou extrêmement longue?

- **Les parents, les tutrices et tuteurs doivent s'informer sur les dernières fraudes et les nouvelles à propos de la sécurité des appareils.** Si un enfant télécharge un virus ou un maliciel par accident, assurez-vous qu'elle ou il déconnecte son appareil d'Internet et l'éteint immédiatement. Consultez une technicienne professionnelle ou un technicien professionnel pour régler le problème.

Cette ressource contient des renseignements importants à transmettre aux enfants pour les sensibiliser aux risques en ligne et leur expliquer comment éviter de se faire soutirer des renseignements personnels ou privés. Si les enfants se retrouvent dans une mauvaise situation, ils doivent en parler à une ou un adulte de confiance immédiatement. Plus ils attendent, plus la situation risque d'empirer.

ACTIVITÉ 1

Les enfants peuvent s'exercer et mettre en évidence leurs connaissances sur les sujets abordés dans cette ressource par l'entremise d'activités pratiques. Laissez-les essayer par eux-mêmes, en leur offrant de l'aide au besoin.

La sécurité en ligne : mot caché sur les risques en ligne

Peux-tu trouver les mots clés suivants sur la compréhension et l'évitement des risques en ligne? À mesure que tu les trouves, réfléchis à ce qu'ils signifient, à ce que tu as appris et à la manière dont tu peux transmettre cette information à d'autres!

L	B	Y	M	R	G	C	J	A	P	H	Z	X	P	T
O	T	P	I	E	C	E	S	J	O	I	N	T	E	S
A	V	T	O	T	S	R	Q	O	U	V	V	C	I	S
T	C	R	I	N	H	S	B	S	R	J	V	O	O	Z
T	P	H	I	M	E	B	A	C	R	M	I	U	J	S
E	E	S	G	L	K	P	L	G	I	Z	B	R	O	U
N	R	E	X	P	E	D	I	T	E	U	R	R	A	P
T	S	H	E	A	G	P	L	K	L	N	U	I	N	P
I	O	N	C	O	M	M	U	N	I	Q	U	E	R	R
O	N	P	I	E	G	E	F	U	A	V	H	L	A	I
N	N	A	Q	J	Z	F	A	B	S	P	Y	H	U	M
Q	E	E	M	S	E	C	U	R	I	T	A	I	R	E
Q	L	I	H	D	J	A	X	V	U	G	X	Z	U	R
H	E	C	O	D	Q	W	P	Y	A	E	K	I	C	F
X	U	E	N	V	A	W	K	N	Q	C	H	F	G	R

Communiquer

Pièces jointes

Message

Expéditeur

Piège

Faux

~~Sécuritaire~~

Pourriel

Attention

Personnel

Supprimer

Courriel

À ne pas oublier!

Fiez-vous à votre instinct.

Si quelque chose semble suspect, évitez-le!

ACTIVITÉ 2

Repérage des faux sites Web

Voici deux versions d'adresses de sites populaires : l'une est la bonne, et l'autre est fausse.
Peux-tu trouver la vraie adresse? Comment as-tu deviné?

Khan Academy
Une organisation éducative à but non lucratif ayant pour but d'offrir aux élèves une panoplie d'outils d'apprentissage en ligne.

1

a. https://fr.khancademy.org/

b. https://fr.khanacademy.org/

Kahoot!
Une plateforme d'apprentissage ludique utilisée comme technologie éducative dans les écoles.

2

a. https://kahoot.com/fr

b. https://kah0ot.com/fr

Qwant Junior
Le seul moteur de recherche français conçu exprès pour les enfants.

3

a. https://www.qwantjunior.com/

b. https://www.qwantjunior.cz/

[Réponses] 1.B – Dans la réponse a), il manque le « a » dans « academy »; 2.A – Dans la réponse b), un « o » est remplacé par un « 0 »; 3.A – La réponse b) se termine par « .cz » au lieu de « .com » ou « .ca ».

0 POUR EN SAVOIR PLUS

Pour en savoir plus sur la cybersécurité ou pour poursuivre la conversation et l'apprentissage, consultez 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