Maternelle
à
3e année

La sécurité en ligne : comprendre les risques

Adaptation française : Centre franco-ontarien de ressources pédagogiques

ROGERS
cybersecure
catalyst

Aux yeux des jeunes enfants, Internet peut représenter la porte d'entrée d'un énorme terrain de jeu virtuel! Il faut donc les surveiller de près lorsqu'ils utilisent des appareils connectés à Internet comme des ordinateurs portables ou de bureau, des tablettes, des téléphones cellulaires, des consoles de jeux vidéo ou des télévisions intelligentes.

Les parents et les tutrices et tuteurs qui laissent leurs enfants explorer ce « terrain de jeu virtuel » doivent absolument discuter avec eux des nombreux risques, tant pour les enfants eux-mêmes que pour leurs appareils.

Cette ressource fournit des renseignements et des conseils aux parents, aux tutrices et aux tuteurs pour les aider à discuter avec leurs enfants des risques liés à l'utilisation d'appareils électroniques et à leur expliquer comment repérer et déjouer ces risques lorsqu'ils socialisent, naviguent et téléchargent du contenu en ligne.

A DÉFINITIONS

Les parents, les tutrices et tuteurs trouveront probablement les mots suivants étranges et difficiles à expliquer à de jeunes enfants. Voici donc des définitions simplifiées pour les aider :

Escroqueries - Définition du risque

- Les escrocs ou les personnes qui participent à des activités malhonnêtes et stratagèmes de tromperies, incitent les enfants à télécharger ou à acheter quelque chose, leur demandent de faire des quiz et offrent des récompenses comme de l'argent, des prix, des systèmes de jeu ou des tablettes gratuites.

Escroqueries - Explication des risques pour les jeunes

- Parfois, il y a de mauvaises personnes qui utilisent l'Internet pour envoyer des messages sur des appareils pour inciter les enfants à donner des informations comme leur nom, âge ou adresse. Les enfants doivent toujours demander à un adulte avant de cliquer sur des images ou des liens, ou d'ouvrir des messages de personnes inconnues.

Virus – Définition du risque

- 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.

Virus – Explication du risque pour les jeunes

- Imaginez un vrai virus, comme le rhume ou la grippe, mais qui infecte un appareil. Si l'appareil d'un enfant, comme sa tablette ou son téléphone, tombe malade, il cesse de fonctionner correctement.

Vol d'identité – Définition du risque

- 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 jeu en ligne et de leurs comptes de médias sociaux.

Vol d'identité – Explication du risque pour les jeunes

- Parfois, de mauvaises personnes tentent d'utiliser des renseignements sur des enfants, comme leurs photos, leur nom ou leurs intérêts, pour se faire passer pour eux. Leur but est d'amener d'autres personnes à les aider. C'est pourquoi les enfants ne doivent jamais divulguer de renseignements privés en ligne sans en parler d'abord à une ou un adulte!

Maliciel – Définition du risque

- Type de virus installé secrètement dans le but de voler les renseignements privés 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.

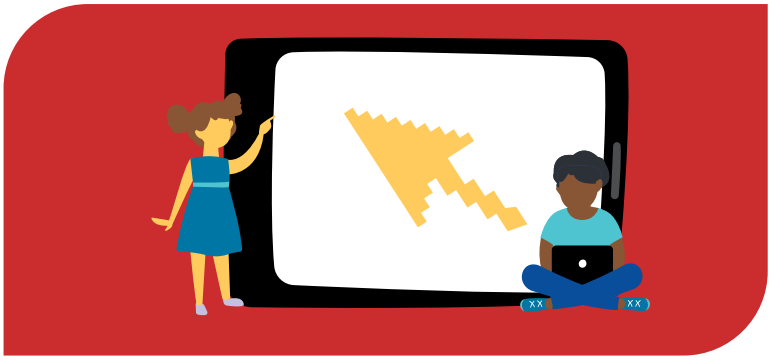
Maliciel – Explication du risque pour les jeunes

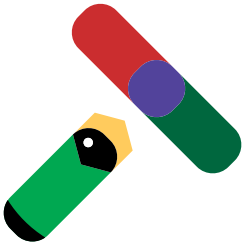
- Type de virus pouvant se trouver sur un ordinateur ou un autre appareil à l'insu de tous. Il y vole discrètement des renseignements, comme des mots de passe et des photos, et peut aussi supprimer des dossiers pouvant être nécessaires plus tard !

A DÉFINITIONS

Éviter les risques en ligne

- Tous ces risques peuvent provenir de diverses formes de communication et d'interaction avec des appareils, par exemple des courriels, des messages textes, des fonctions de clavardage dans des mondes virtuels ou des jeux en ligne, des liens infectés vers des sites Web, des bannières publicitaires téléchargeables, des fenêtres contextuelles sur des sites Web, ou des publications sur les médias sociaux et des applications.





B PERTINENCE

- 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.

- Les fraudeuses et fraudeurs, ou « mauvaises personnes », tentent de profiter de l'innocence des enfants et de leur manque d'expérience avec les appareils connectés à Internet afin de les amener à divulguer des renseignements personnels et privés. C'est ce qu'on appelle de l'« hameçonnage ».

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.

B PERTINENCE

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.**

- **Ils ne doivent cliquer sur aucun lien, photo, vidéo, fenêtre contextuelle ou publicité** qui leur semble douteux, et ne doivent visiter aucun nouveau site Web ni télécharger un jeu sans d'abord demander la permission à un parent ou à une tutrice ou un tuteur!

- **Les enfants doivent aviser une ou un adulte de confiance** s'ils reçoivent un message sur l'appareil qu'ils utilisent. Ils doivent s'assurer de ne pas partager ni transférer de messages dont ils ne sont pas certains : si ces derniers contiennent des virus, ils pourraient mettre d'autres personnes à risque!

- **Les enfants ne doivent pas répondre à des messages ou à des demandes d'amitié provenant de personnes inconnues.** Il en va de même pour les appels ou les messages textes de personnes ou de numéros qu'ils ne connaissent pas.

- **Il faut réfléchir avant de cliquer!** Si quelque chose semble bizarre ou trop beau pour être vrai, par exemple une personne qui offre un jouet gratuit ou un prix à condition de répondre à un questionnaire ou de remplir un formulaire, il ne faut pas se laisser avoir. Les enfants ne doivent jamais divulguer de renseignements, de photos ou de vidéos d'eux-mêmes ou d'autres personnes sans permission.

APPEL À L'ACTION

Prévention des risques en ligne

- **La prévention des risques pour les appareils ou les enfants sur Internet passe par les parents et les tutrices et tuteurs, et les mesures préventives mises en place à la maison. Vous trouverez ci-dessous une liste de vérification des mesures à prendre pour assurer la sécurité des enfants et de leurs appareils. Rassemblez votre famille pour effectuer quelques-unes des tâches ci-dessous et engager la conversation :**

- **Paramétrez le contrôle parental sur tous les appareils et les sites afin de restreindre le temps d'accès et de recevoir des notifications et des alertes lors de tentatives d'accès à des sites bloqués.**

Astuce : Ajoutez à vos favoris les sites que vos enfants utilisent souvent, que ce soit un site de jeux éducatifs ou leur vidéo YouTube préférée, pour en faciliter l'accès.

- **Installez un bloqueur de fenêtres contextuelles et de publicités pour que les enfants ne cliquent pas sur quelque chose d'inapproprié par mégarde!**

Fenêtres contextuelles et bannières publicitaires : Publicités qui figurent sur des sites Web ou dans des vidéos. Il peut s'agir d'images ou d'animations qui bougent ou qui clignotent. Attention, elles contiennent parfois des virus dangereux!

- **Utilisez un mode de recherche sûr dans votre navigateur,** et encouragez l'utilisation de moteurs de recherche adaptés aux enfants, comme Qwant Junior, ou Kiddle et Safe Search Kids, ces deux derniers pris en charge par Google.

Moteur de recherche : Type de site Web qui aide les gens à trouver sur Internet des renseignements sur un sujet en particulier.

- **Les parents et les tutrices et tuteurs doivent s'informer sur les dernières fraudes et les nouvelles à propos de la sécurité des appareils.** En se tenant à jour et en restant alertes, elles et ils seront en mesure de relayer l'information à leurs enfants. Les enfants doivent parler à un parent ou à une tutrice ou un tuteur, ou à une ou un adulte de confiance, de tout ce qui leur paraît suspect lorsqu'ils utilisent un appareil.

APPEL À L'ACTION

Navigation sécuritaire sur Internet

- Les enfants vont sur Internet pour consulter des sites contenant des pages et des pages d'information, d'images et de vidéos. Ils peuvent y apprendre une foule de choses ou se divertir pendant des heures; il est toutefois important qu'ils naviguent en toute sécurité ou sous la supervision d'un parent, d'une tutrice ou d'un tuteur ou d'une ou un adulte de confiance, comme une sœur ou un frère plus âgé ou une éducatrice ou un éducateur.
- Afin de protéger les enfants lorsqu'ils naviguent, assurez-vous qu'ils demandent toujours la permission à un parent, à une tutrice ou un tuteur ou à une ou un adulte de confiance avant d'utiliser un appareil.

- **Ne cliquez pas sur les fenêtres ou les bannières publicitaires** qui apparaissent sur les sites Web : elles peuvent contenir des virus et demander des renseignements personnels et privés.

- **Évitez les offres spéciales et les promesses de cadeaux, d'argent et de prix.** Rien n'est réellement gratuit! Les questionnaires et concours amusants peuvent être très tentants, mais ils sont souvent fouineurs et demandent aux enfants de fournir des renseignements tels que leur adresse courriel ou de se connecter à un compte de médias sociaux pour obtenir les résultats.

- **Empêchez les appareils des enfants et ceux des autres de stocker des renseignements** pour les entrer automatiquement plus tard. Les appareils demandent souvent d'enregistrer ces renseignements pour le côté pratique de la chose, mais cette information risque de tomber entre de mauvaises mains!
- **Méfiez-vous des faux sites Web.** Les fraudeuses et fraudeurs, ou les « mauvaises personnes », peuvent créer de faux sites très semblables aux originaux! Ils peuvent avoir des adresses et des logos ressemblants, mais leur but est d'obtenir les renseignements des enfants ou d'installer un virus sur leur appareil.

APPEL À L'ACTION

Téléchargements sécuritaires

- **Il y a tant de choses à télécharger sur Internet. Il est possible que les jeunes enfants ne sachent même pas que ce qu'ils sont en train de faire est considéré comme un téléchargement.**
- **Généralement, lorsque les enfants veulent enregistrer quelque chose sur leur ordinateur, leur tablette ou leur téléphone, ils doivent d'abord le télécharger. Le plus souvent, ce sont des versions nouvelles ou mises à jour d'applications mobiles, des photos et des vidéos qu'ils souhaitent conserver pour plus tard ou des documents électroniques comme des livres numériques.**
- **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. Certains fichiers peuvent contenir des virus ou des maliciels.**

Pour protéger les enfants et leurs appareils, il est recommandé que les enfants **demandent l'avis d'un parent ou d'une tutrice ou d'un tuteur** avant de télécharger quoi que ce soit, afin de s'assurer que le contenu est approprié et qu'il provient d'un site de confiance ou d'une boutique de jeux certifiée.

Astuce

Vous ne savez pas comment déterminer si un site est sûr 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.

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.

À la pêche aux renseignements!

- Comme nous l'avons appris, les fraudeuses et fraudeurs, ou « mauvaises personnes », s'adonnent souvent à l'hameçonnage pour mettre la main sur les renseignements personnels et privés d'autrui afin de voler leur identité, de leur soutirer de l'argent ou d'installer des virus sur leurs appareils.

- Cette ressource t'aidera à éviter les situations où cela pourrait t'arriver. En te servant de tes nouvelles connaissances, colorie les images sous l'hameçon qui représentent des moyens qu'emploient les fraudeuses et fraudeurs pour infecter tes appareils et obtenir tes renseignements. Ensuite, associe chaque moyen à son image!

1. TÉLÉCHARGEMENTS 2. COURRIELS 3. JEUX VIDÉO 4. MESSAGES TEXTES

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