Liste de vérification sur la cybersécurité: sécurité en ligne des enfants et des adolescents

Grandir devant les écrans comporte des avantages et des risques. Vos enfants vont passer du temps en ligne – c'est prévisible et même essentiel en cette époque de haute technologie. Tout comme vous prenez des mesures pour les protéger dans le monde physique, vous devez faire preuve de vigilance et d'attention pour assurer leur sécurité dans le monde virtuel. **La protection en ligne de vos enfants commence par une conversation. Cette liste de vérification aidera vos enfants à se familiariser avec la sécurité en ligne et les rôles que nous remplissons pour assurer en la sécurité de nos familles.**

1. Communiquez moins d'information

Encouragez votre enfant à se demander s'il partagerait l'information ou la photo qu'il désire publier avec une personne qu'il ne connaît pas. S'il répond non, il ne doit pas la publier.

Ce que vous pouvez faire :

- ❑ Renseignements personnels : expliquez à vos enfants quels renseignements sont considérés comme confidentiels. Ils ne doivent communiquer à personne des renseignements permettant de les identifier comme leur nom complet, leur adresse ou leur numéro de téléphone.
- ❑ Photos : qu'il s'agisse de photos de votre domicile, de membres de votre famille, de l'école ou de vos vacances, il vaut toujours mieux en publier le moins possible.
- ❑ Localisation : désactivez les géobalises ou les services de localisation dans les applications.
- ❑ Adresse courriel : une adresse courriel est un renseignement personnel – il faut éviter de la publier dans les forums publics ou de l'entrer sur des sites non dignes de confiance.

2. Soyez futé avec les mots de passe

Mémoriser un nouveau mot de passe différent pour chaque compte en ligne est pénible. Nous le savons. Le piratage l'est aussi.

Comment créer un mot de passe robuste :

- ❑ Utilisez un mot de passe différent pour chaque compte important.
- ❑ Utilisez un mot de passe comprenant au moins huit caractères. Plus il sera long, mieux cela vaudra.
- ❑ Il doit comprendre des lettres (majuscules et minuscules), des chiffres et des symboles.
- ❑ Évitez d'utiliser des mots courants tels que « mot de passe » et « utilisateur ». Créez des mots de passe faciles à mémoriser pour ne pas avoir à les conserver sous forme écrite, ce qui constituerait un risque.
- ❑ Si vous croyez qu'une personne (autre qu'un parent ou un tuteur) connaît votre mot de passe, remplacez-le immédiatement.
- ❑ Réinitialisez régulièrement vos mots de passe.

3. Rien n'est gratuit

Ce que vous pouvez faire :

- ❑ Limitez votre activité sur le réseau Wi-Fi à la maison. Le réseau public Wi-Fi est moins sûr que votre réseau privé.
- ❑ Supprimez toute application que vous n'utilisez pas.
- ❑ Évitez les jeux-questionnaires et les applications gratuites. Souvent, l'utilisateur « paie » quand même en dévoilant des renseignements personnels, ses activités en ligne, le lieu où il se trouve, en rendant accessible une liste de contacts, en publiant des messages texte, etc.

4. Protégez votre vie privée

Ce que vous pouvez faire :

- ❑ Paramètres dans le téléphone : vérifiez les paramètres de confidentialité dans le téléphone de vos enfants.
- ❑ Applications et comptes : lors de l'ouverture d'un nouveau compte, vos enfants ne doivent pas accepter automatiquement les paramètres par défaut. Aidez-les à créer le compte et à en configurer les paramètres de confidentialité.
- ❑ Médias sociaux : encouragez vos proches à opter pour la confidentialité et à publier moins d'information dans leurs comptes sur les médias sociaux. Les inconnus auront ainsi plus de mal à se connecter avec eux en ligne et à vérifier leur activité sur le Web.

5. Faux comptes et escroqueries

Nombre d'escroqueries ciblent les enfants sur le Web, des escroqueries liées au magasinage aux jeux-questionnaires en passant par les faux concours et les fausses bourses d'études. En promettant des offres, des prix et des récompenses, ces escroqueries incitent les enfants à cliquer sur des liens et à dévoiler leurs renseignements personnels.

Ce que vous pouvez faire :

- ❑ Faux comptes : aidez vos enfants à prendre conscience que les gens qui communiquent avec eux peuvent ne pas être ceux qu'ils disent être. Les escrocs se créent une fausse identité et un faux compte en ligne pour tromper les gens en les amenant à se prendre d'amitié pour eux ou à communiquer leurs renseignements personnels.
- ❑ Faux sites Web : les escrocs montent de faux sites Web de détaillants qui ressemblent à de véritables magasins en ligne. Le hic, c'est que vous ne recevrez pas la marchandise que vous y avez achetée. Montrez à vos enfants comment accéder directement à un site de confiance.
- ❑ Fausses offres : lorsque cela semble trop beau pour être vrai, c'est sûrement le cas.
- ❑ Escroquerie par téléphone ou messagerie texte : si le numéro affiché est inconnu, il faut ignorer l'appel ou le message. Il ne faut pas répondre à l'appel ou cliquer sur des liens envoyés par message texte. Il ne faut pas communiquer de renseignements personnels à une personne qu'on ne connaît pas.
- ❑ Escroquerie par courriel : il faut éviter d'ouvrir les pièces jointes à un message ou de cliquer sur les liens qu'il contient si on n'en connaît pas la source. En cas de réception d'un courriel accompagné d'une pièce jointe suspecte, il faut l'ignorer et le supprimer tout simplement.

6. Paramètres de sécurité

Ce que vous pouvez faire :

- ❑ Configurez les contrôles parentaux, par exemple les filtres SafeSearch de Google, qui aident au blocage de sites au contenu explicite.
- ❑ Créez des mots de passe robustes et encouragez tous les membres de votre famille à les changer régulièrement.
- ❑ Activez l'authentification à deux facteurs, qui est un peu comme un système de verrouillage de porte comprenant plus d'une serrure.
- ❑ Assurez-vous que les applications intrusives ne sont pas installées et que celles qui ne servent plus sont désinstallées.
- ❑ Activez l'outil « Find my Mobile » afin de pouvoir repérer les appareils manquants et protéger les données.

7. Conversation ouverte

La protection en ligne de vos enfants commence par une conversation. La meilleure façon de protéger vos enfants est de parler ouvertement et régulièrement avec eux de la cybersécurité. En montrant à vos enfants que vous leur faites confiance et en leur donnant des conseils pour utiliser Internet intelligemment et de façon sécuritaire, vous les aidez à devenir des utilisateurs avertis et prudents.

8. « Je suis là pour t'aider »

Personne n'aime surmonter seul des difficultés, et se protéger en ligne peut s'avérer difficile. Faites bien comprendre à votre enfant que vous êtes là pour le soutenir si quelque chose sur le Web le met mal à l'aise ou le perturbe. S'il se trouve dans une situation pénible (par exemple, s'il est victime de cyberintimidation ou d'extorsion), rassurez-le en lui disant qu'il n'est pas seul et que vous vous en sortirez ensemble.

La présente liste de vérification est un outil important que vous pouvez consulter en tout temps alors que poursuivez la conversation avec vos enfants. Même si leurs comportements en ligne évolueront à mesure qu'ils vieilliront, cette liste peut vous aider, vos enfants et vous, à vous souvenir des risques existants sur les diverses plateformes et les différents appareils utilisés. L'imprimer est une bonne idée, car vous pourrez ainsi la consulter régulièrement et conserver la maîtrise de la sécurité en ligne de vos enfants.

Signaler une fraude

Si vous croyez que vos renseignements personnels ont été volés ou obtenus par des moyens frauduleux en ligne, par téléphone ou par tout autre moyen, téléphonez-nous immédiatement.

N'hésitez pas à nous appeler si vous avez des questions ou des commentaires d'ordre général concernant la protection des renseignements personnels et la sécurité.
1 800 769-2511 (services bancaires par téléphone)
1 800 769-2555 (services bancaires mobiles et en ligne)
1 800 769-2512 (cartes de crédit)
1 800 769-2535 (Centre de soutien clientèle, Services bancaires en ligne RBC Express)