Aider nos jeunes

à utiliser leur téléphone intelligent de façon sécuritaire

Créé en partenariat avec :

Habilo Médias

PENSEZCYBERSECURITE.CA
Protégez-vous en ligne.

TELUS[MD]

Aider nos jeunes
à utiliser leur téléphone intelligent de façon responsable

Mot de bienvenue d'Andrea Goertz

Si vous avez un enfant d'âge scolaire, il vous a probablement déjà posé cette question brûlante : « Je peux avoir un téléphone intelligent? » Déterminer si un enfant est prêt est une lourde tâche, mais assurer sa sécurité en ligne peut sembler un défi sans fin.

Je suis mère de deux adolescents et tous les jours, je vois mes enfants et leurs amis profiter de la technologie, que ce soit sur un téléphone intelligent, une tablette ou un ordinateur portatif. La technologie peut être très avantageuse sur le plan des relations sociales, de l'éducation et de la communication avec la famille. Toutefois, en tant que parents, nous devons connaître la puissance des appareils intelligents et les possibilités qu'ils offrent, afin de pouvoir conseiller nos enfants lorsqu'ils seront prêts à avoir leur premier appareil.

Ce guide a été créé pour aider les parents à prendre une décision éclairée.

Nous croyons que l'action à l'échelle communautaire permet d'accomplir de grandes choses. C'est pourquoi TELUS AVERTI, un programme éducatif unique qui met l'accent sur la sécurité dans l'utilisation d'Internet et des téléphones intelligents, s'est associé à Pensez cybersécurité et à HabiloMédias. Ensemble, nous avons créé un guide convivial pour les parents et les gardiens d'enfants, afin qu'ils puissent donner aux enfants des moyens d'assurer leur sécurité en ligne lorsqu'ils commencent à utiliser la technologie.

Depuis le lancement de TELUS AVERTI en 2013, plus de 750 000 Canadiens ont fait appel gratuitement à nos séminaires et nos ressources en ligne afin d'accroître la sécurité de leurs familles sur Internet. J'espère que vous trouverez ce nouveau guide pour les parents précieux et utile. Si vous avez des questions, veuillez nous écrire à l'adresse averti@telus.com

Cordialement,

Andrea Goertz – Cadre déléguée de TELUS AVERTI
Chef de Communications et durabilité, TELUS

1. Que font les jeunes en ligne?

Habilo Médias

JEUNES CANADIENS DANS UN MONDE BRANCHÉ

La vie en ligne

Les élèves canadiens sont plus branchés, plus mobiles et plus sociaux que jamais.

www.habilomedias.ca/JCMB

ACCÈS À INTERNET

45 % des élèves se connectent à Internet à partir d'un cellulaire ou d'un téléphone intelligent

60 % des garçons se connectent à Internet par le biais d'une console de jeux vidéo

Année	Ordinateur partagé	Propre ordinateur	Portable	Bibliothèque/ Centre communautaire	Lecteur MP3	Cellulaire/ Tél. intelligent	Console de jeux
4	64 %	17 %	56 %	6 %	47 %	12 %	46 %
5	59 %	19 %	62 %	9 %	49 %	21 %	47 %
6	59 %	20 %	63 %	6 %	55 %	25 %	48 %
7	54 %	21 %	69 %	7 %	55 %	37 %	45 %
8	50 %	23 %	73 %	4 %	53 %	56 %	41 %
9	41 %	23 %	75 %	6 %	44 %	68 %	43 %
10	39 %	25 %	78 %	6 %	38 %	69 %	34 %
11	37 %	27 %	73 %	6 %	36 %	75 %	38 %

59% des enfants de la 4e année du primaire à la 5e année du secondaire ont un téléphone mobile (téléphone intelligent ou téléphone mobile sans transmission de données).

69% des enfants ont accès à un téléphone mobile (le leur ou celui de quelqu'un d'autre).

AVEC CELLULAIRE/ TÉL. INTELLIGENT

Année	Possèdent	Le leur/ partagé
4	24 %	na %
5	31 %	na %
6	38 %	na %
7	55 %	60 %
8	68 %	75 %
9	84 %	88 %
10	88 %	88 %
11	86 %	86 %

COMPORTEMENT CRUEL OU MÉCHANT

55 % des élèves ayant un comportement méchant ou cruel en ligne disent qu'ils ne « faisaient que plaisanter ».

Vouloir faire des représailles était une autre raison commune :

48 % ont dit que c'était parce que quelqu'un leur avait déjà dit quelque chose de méchant ou de cruel

32 % ont dit que c'était parce que quelqu'un avait dit quelque chose de méchant ou de cruel à propos d'un de leurs amis.

RÉPONSES PAR RAPPORT AU COMPORTEMENT MÉCHANT OU CRUEL ET AUX MENACES

Demander de l'aide de ses parent	50 %
L'ignorer en espérant que ça arrête	42 %
Demander de l'aide de ses amis	38 %
Demander de l'aide de son professeur (9e option d'une liste de 11)	17 %

Les élèves sont plus prêts à confronter la personne directement pour régler un conflit.

SPECTATEURS ET INTERVENANTS

65 % des élèves ont fait quelque chose pour aider quelqu'un qui faisait face à un comportement cruel ou méchant en ligne. Les élèves qui ont fait de le cyberintimidation et ceux qui ont été intimidés en ligne sont également susceptibles d'intervenir et d'aider.

LA CULTURE À L'ÉCOLE, LES RÈGLES ET LES INTERVENTIONS

Il y a une très faible corrélation entre la présence de règles à l'école et si un élève **s'engage** ou non dans un comportement de cyberintimidation ou fait **l'expérience** de la cyberintimidation mais il y a une forte corrélation entre le fait d'avoir une règle à la maison exigeant de traiter les gens avec respect en ligne et des niveaux moins élevés de comportements méchants ou menaçants.

APPRENDRE À PROPOS DE LA CYBERINTIMIDATION

62 % des élèves ont appris des choses à propos de la cyberintimidation de leurs enseignants et...	**43 %** de leurs parents

ACTIVITÉS EN LIGNE

LES ACTIVITÉS LES PLUS FRÉQUENTES EN LIGNE, TEL QUE INDIQUÉ PAR LES ÉLÈVES, SONT:

52 % des enfants de la 4e année du primaire à la 5e année du secondaire lisent ou publient des messages sur les réseaux sociaux une fois par semaine ou plus.

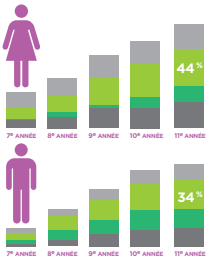
Parmi les élèves de la 4e à la 6e année du primaire,
32 % ont un compte Facebook

Parmi les élèves de la 1re à la 5e année du secondaire,
82 % ont un compte Facebook

7 DES 10 SITES PRÉFÉRÉS PAR LES ÉLÈVES OFFRENT COMME ACTIVITÉS PRINCIPALES D'AFFICHER ET DE PARTAGER DE L'INFORMATION ET DU CONTENU

CHERCHER DE L'INFORMATION EN LIGNE

DIFFICULTÉS RELATIONNELLES
QUESTIONS DE SANTÉ PHYSIQUE
SEXUALITÉ
QUESTIONS DE SANTÉ MENTALE



MÉTHODOLOGIE

L'enquête a été menée de février à juin 2013.

5 436 élèves canadiens,
de la 4e à la 11e année, dans les 10 provinces et les 3 territoires

41 % garçons | 46 % filles | 13 % sans indication

126 anglophones | 14 francophones

140 écoles et 51 commissions scolaires

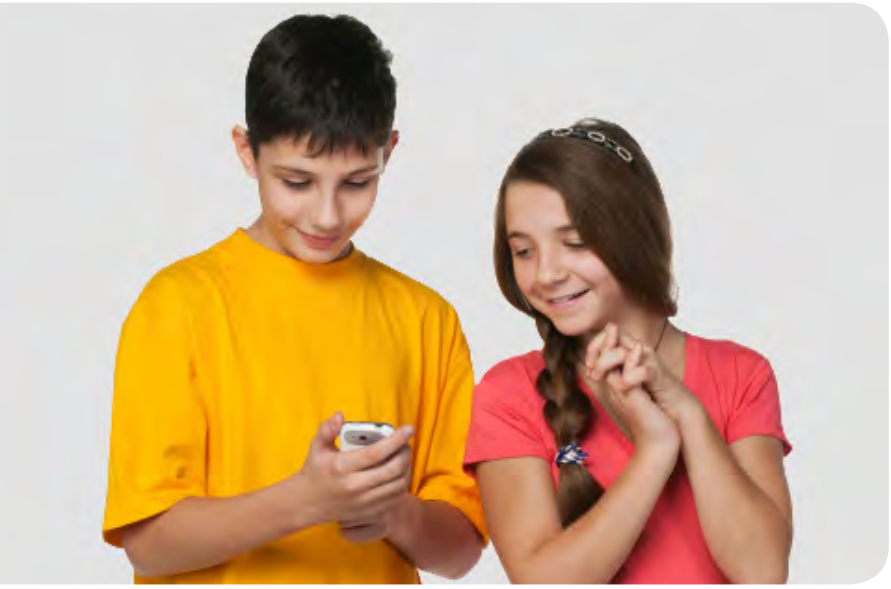
Source: **HabiloMédias**

2. Votre enfant est-il prêt à avoir un téléphone intelligent?

Une question revient souvent : « À quel âge mon enfant devrait-il avoir son premier téléphone intelligent? » La réponse dépend davantage de sa maturité et de sa capacité à utiliser un téléphone intelligent de façon responsable que de son âge. Ainsi, posez-vous les questions suivantes :

- Avez-vous fixé des limites pour l'utilisation des iPods, des tablettes, des ordinateurs et des consoles de jeu? Si oui, votre enfant comprend-il et respecte-t-il ces limites?
- Votre enfant a-t-il besoin d'un téléphone pour communiquer avec vous en cas d'urgence?
- Êtes-vous certain que votre enfant n'utilisera pas le téléphone à des moments inappropriés (p. ex. en classe)?
- Avez-vous expliqué à votre enfant comment utiliser son téléphone intelligent de façon responsable et lui avez-vous parlé du partage de photos et de publications inappropriées?

Si vous avez répondu « oui » à toutes ces questions, il se peut que votre enfant soit prêt à avoir son premier téléphone. Mais votre tâche ne s'arrête pas ici. Vous devez maintenir le dialogue avec votre enfant sur les comportements appropriés à adopter en ligne, que ce soit sur un téléphone intelligent, une tablette, un ordinateur, une console de jeu en réseau ou un iPod.



3. Une fois que vous avez décidé de donner un téléphone intelligent à votre enfant

Vous avez pris la décision de donner un téléphone intelligent à votre enfant et il est impatient de l'avoir. Voici quelques facteurs à prendre en compte avant d'acheter le téléphone.

Avant d'acheter un téléphone intelligent à votre enfant

Prenez en compte les facteurs suivants :

Contrôle parental : Les appareils ne sont pas tous égaux en matière de contrôle parental. Avant d'acheter un téléphone intelligent, faites des recherches sur les options de contrôle parental des téléphones intelligents offerts pour choisir celui qui répond le mieux à vos besoins.

Données ou voix seulement : Déterminez si vous voulez que votre enfant puisse faire des appels seulement ou si vous voulez qu'il puisse aussi utiliser des données pour envoyer des textos, des courriels et naviguer sur Internet. Discutez avec le fournisseur de services des forfaits de données et de la façon de gérer l'utilisation des données de votre enfant.

Style et fonctionnalité : De très beaux téléphones intelligents avec beaucoup de fonctions sont offerts sur le marché, mais avant de choisir un modèle pour votre enfant, pensez à la fonctionnalité et à la durabilité qu'aura l'appareil lorsqu'il sera entre les mains de votre enfant.

Si vous lui donnez le téléphone usagé d'un membre de la famille : Vous pouvez aussi donner votre téléphone cellulaire usagé à votre enfant et vous en procurer un nouveau. Si vous optez pour cette solution, assurez-vous d'effacer toutes les données de votre téléphone avant de le lui donner.

Avant de donner le téléphone intelligent à votre enfant

Avant de remettre le téléphone à votre enfant, voici quelques mesures à prendre avec lui pour garantir qu'il utilise le téléphone de façon optimale, sécuritaire et responsable. Nous avons réparti ces mesures en quatre catégories :

a) La sécurité avant tout

b) L'utilisation des données

c) Les médias sociaux et les applications

d) Les autres facteurs importants

a) La sécurité avant tout

Configurez la fonction de verrouillage. La mesure la plus importante est probablement de verrouiller l'appareil et de modifier les paramètres de façon à ce que l'écran se verrouille automatiquement après un délai d'une à cinq minutes. Le verrouillage de l'écran est une mesure particulièrement importante pour les jeunes qui utilisent un téléphone intelligent. En effet, leurs « amis » peuvent s'emparer de leur appareil et publier « à la blague » des commentaires sur leur compte Facebook (les enfants laissent habituellement leur session ouverte) ou envoyer des textos ou des courriels en assumant leur identité.

Choisissez des mots de passe difficiles à trouver. Choisissez un mot de passe difficile à trouver pour le téléphone intelligent, les applications et les comptes de réseaux sociaux (comme Instagram) auxquels votre enfant est abonné. Un bon mot de passe peut contrecarrer les plans d'une personne qui voudrait s'immiscer dans son téléphone intelligent ou ses comptes de réseaux sociaux ou modifier le mot de passe de ses applications. Votre mot de passe doit contenir au moins six caractères (des chiffres, des lettres et d'autres caractères). Vous pouvez augmenter l'efficacité de votre mot de passe en utilisant les premières lettres des mots d'une phrase, plutôt qu'un terme (p. ex. JOJMMDP pour « Je n'oublie jamais mon mot de passe »), en remplaçant certaines lettres par des chiffres ou d'autres caractères et en utilisant une combinaison de lettres majuscules et minuscules (p. ex. 1c@RLp). Assurez-vous que votre enfant utilise des mots de passe difficiles à deviner et qu'il ne se sert pas du même mot de passe pour tous ses comptes. Notez ses mots de passe sur un bout de papier et rangez le bout de papier dans un lieu sûr à la maison (ne notez jamais les mots de passe dans un livre d'école ou dans l'appareil). Aussi, faites bien comprendre à votre enfant qu'il ne doit jamais divulguer son mot de passe à quiconque, sauf à vous.

Installez ou activez un logiciel de localisation/verrouillage/nettoyage à distance et installez un logiciel de sécurité. Vous pouvez télécharger des logiciels gratuits dans le téléphone pour le localiser, en faire le suivi ou effacer son contenu à distance en cas de perte ou de vol. L'application conçue pour les iPhone est Localiser mon iPhone. Pour les BlackBerry, il s'agit de BlackBerry Protect et pour les appareils Android, le nom varie d'un fabricant à l'autre. Par exemple, l'application de Samsung s'appelle Localiser mon appareil.

Assurez-vous que la fonction de géomarquage est désactivée. Les photos ou les vidéos prises avec la plupart des téléphones intelligents contiennent une balise géographique relavant l'endroit exact où la photo a été prise. Pensez-y, si vous prenez une photo de votre enfant lors de sa première journée à l'école et que vous publiez cette photo sur votre réseau social favori, n'importe qui peut trouver l'endroit exact où cette photo a été prise. La fonction de géomarquage se trouve habituellement dans les paramètres de l'appareil photo ou dans les paramètres généraux du téléphone.

Ajoutez à la liste de contacts les numéros des membres de la famille et de personnes à joindre en cas d'urgence. Add parents, grandparents, sitters and I.C.E. (In Case of Emergency) contacts. Having a few contacts labeled ICE lets anyone know who to call in case of an emergency.

Que faire en cas d'urgence. Rappelez à votre enfant qu'il doit vous appeler ou composer le 911 dans une situation d'urgence.

Les ados au volant. À titre d'exemple, plus du tiers des adolescents ontariens ont admis avoir déjà texté au volant, même si la plupart d'entre eux savent que c'est dangereux! Si votre enfant a l'âge de conduire, vous devez insister sur les conséquences de texter au volant ou d'être à bord d'un véhicule conduit par un ado qui utilise un téléphone intelligent au volant, car ces conséquences peuvent parfois être fatales.

b) L'utilisation des données

Gestion des données. Familiarisez-vous avec le logiciel de gestion des données du téléphone intelligent de votre enfant. Certains appareils comportent une application intégrée qui bloque automatiquement la transmission de données lorsqu'une certaine limite est atteinte, tandis que pour d'autres appareils, la transmission de données doit être activée ou désactivée manuellement. Votre enfant et vous devez savoir quand il est nécessaire de désactiver la transmission de données et quand il est opportun de la réactiver.

L'application Mon compte TELUS permet aux parents de suivre l'utilisation de données pour les comptes à leur nom.

c) Les médias sociaux et les applications

Votre enfant pourra accéder à toutes sortes d'applications de médias sociaux (comme YouTube, Twitter et Instagram), ainsi qu'à des jeux et à d'autres applications sur son téléphone intelligent. Il est très important de comprendre les paramètres d'autorisation et de confidentialité des comptes de réseaux sociaux auxquels ils sont abonnés et des applications qu'ils téléchargent, et de les régler selon vos besoins. Il est primordial de lire attentivement les modalités concernant ces paramètres et ne pas les accepter aveuglément.

Les paramètres d'autorisation déterminent le contenu à votre sujet auquel il est possible ou non d'accéder ou pouvant être partagé ou non (p. ex. vos listes de contacts, vos photos et autres fichiers et votre profil) sur un réseau social ou dans une application mobile à laquelle vous êtes abonné.

Les paramètres de confidentialité déterminent qui peut ou non voir votre profil et vos publications privées.

Gardez l'œil sur vos paramètres d'autorisation. Chaque fois que votre enfant télécharge une application sur son téléphone intelligent ou qu'il s'abonne à un réseau social, il permet peut-être à ses concepteurs de voir ses renseignements personnels, comme son carnet d'adresses, les renseignements de son compte Facebook ou Twitter, l'endroit où il se trouve et même ses photos.

Gardez l'œil sur les paramètres de confidentialité avec votre enfant. Vérifiez bien quels sont les renseignements partagés publiquement, et ceux auxquels les applications ont accès. Votre enfant communique peut-être plus d'information que vous ne le pensez.

Gardez l'œil sur vos paramètres de confidentialité. Vérifiez bien quels sont les renseignements partagés publiquement, et ceux auxquels les applications téléchargées sur le téléphone intelligent de votre enfant ont accès. Il communique peut-être plus d'information que vous ne le pensez.

Utilisation des applications en toute sécurité. Tous les téléphones intelligents ont une boutique d'applications intégrées à partir de laquelle on peut généralement télécharger des applications en toute sécurité. Habituellement, ces applications ne contiennent pas de virus ou de logiciels malveillants, mais vérifiez tout de même les médias sociaux utilisés par votre enfant ainsi que les paramètres de confidentialité des applications en question. Même si de nombreux téléphones intelligents permettent à l'utilisateur de télécharger des applications à l'extérieur de la boutique d'applications intégrée, cela n'est pas recommandé.

Beaucoup d'applications gratuites utilisent une petite quantité de données pour diffuser des publicités sur l'appareil. Ces applications créent parfois de fausses alertes de virus et proposent ensuite d'installer un autre logiciel pour enrayer la menace. Le problème est que le logiciel en question est parfois une application payante ou malveillante.

d) Les autres facteurs importants

Filtres de recherche Google. Si le téléphone de votre enfant utilise une application Google, il serait judicieux de l'ouvrir afin de vérifier les paramètres Google. Sous Recherche et Google Now, cliquez sur Comptes et confidentialité, puis sur Filtre SafeSearch. En sélectionnant ce paramètre, vous bloquerez l'affichage de contenu explicite dans les résultats de recherche Google. Assurez-vous de le sélectionner pour réduire les risques que votre enfant soit malencontreusement exposé à du contenu que vous ne voulez pas qu'il voie.

Services infonuagiques. Les nouveaux téléphones intelligents sont compatibles avec de nombreux services d'infonuagique. Ces services permettent de stocker divers types de données, comme les contacts, les calendriers, les photos et les vidéos. Décidez avec votre enfant quels services utiliser, le cas échéant. Vérifiez aussi s'il n'y a pas d'autres services d'infonuagique qui seraient automatiquement activés sur l'appareil. Il est essentiel de choisir des mots de passe sécuritaires pour l'utilisation de services d'infonuagique, car ces derniers contiennent des renseignements personnels auxquels on ne souhaite pas que des camarades de classe ni des étrangers aient accès.

Entente familiale. Rédigez une entente avec votre enfant concernant l'utilisation de son téléphone intelligent et l'utilisation d'Internet dans la famille en général. Une fois l'entente rédigée, demandez à tous les membres de la famille de la signer et de la lire au moins tous les six mois. La section suivante, Entente familiale sur l'utilisation d'Internet, donne de bons exemples de règles et d'ententes familiales.

4. Entente familiale sur l'utilisation d'Internet

Les recherches de HabiloMédias ont démontré que les enfants encadrés par des règles à la maison relativement à l'utilisation d'Internet (incluant les téléphones intelligents) sont moins susceptibles de commettre des gestes comme communiquer leurs coordonnées, visiter des sites de jeu, chercher de la pornographie en ligne et parler à des étrangers en ligne. C'est une bonne idée de s'entendre en famille sur un certain nombre de règles à respecter dans le cyberespace. C'est le meilleur moyen pour parents et enfants de mettre au point ensemble une façon d'utiliser Internet de manière prudente et responsable.

- Chez les jeunes enfants, il est logique d'établir des règles et de les leur expliquer. Au fur et à mesure qu'ils vieillissent et explorent davantage le monde virtuel, vous pouvez discuter de nouvelles règles avec eux.
- La règle la plus importante : si quelque chose se produit en ligne qui effraie vos enfants, les préoccupe ou les rend mal à l'aise, ils doivent vous en parler ou en parler à un autre adulte en qui ils ont confiance. Assurez-vous qu'ils savent que vous êtes dans leur équipe. Plusieurs enfants hésitent à parler à leurs parents lorsque les choses virent mal parce qu'ils craignent de perdre leur accès à Internet ou à leurs appareils numériques.
- Pour des règles plus précises, voici quelques idées de départ :
  - Je demanderai toujours la permission de mes parents avant de donner tout renseignement personnel en ligne, y compris mon nom, mon sexe, mon numéro de téléphone, mon adresse postale ou de courriel, l'emplacement de mon école, les adresses, les numéros de téléphone ou les adresses de courriel de mes parents au travail, les données sur leurs cartes de crédit ou des photos de moi et de ma famille.
  - Je ne visiterai aucun site web que mes parents n'approuveraient pas.
  - Je ne révélerai mes mots de passe à personne (sauf à mes parents ou à un adulte en qui j'ai confiance), pas même à mon meilleur ami.
  - Je n'irai JAMAIS rencontrer en personne quelqu'un que je ne connais que par Internet sans être accompagné d'un parent ou d'un adulte en qui j'ai confiance.
  - Je consulterai d'abord un adulte avant de télécharger du contenu, d'ouvrir des pièces jointes ou de suivre des liens qui pourraient ne pas être sécuritaires.
  - Je me rappellerai toujours qu'il y a des gens de l'autre côté de l'écran que je peux blesser par ce que je dis et fais.
  - Je ne serai pas méchant ou cruel envers quiconque en ligne, même si quelqu'un est méchant avec moi en premier lieu.
  - Si quelqu'un est méchant avec moi en ligne, je me rappellerai que ce n'est pas de ma faute.
  - Si je vois quelqu'un d'autre être méchant ou cruel en ligne envers une autre personne, je ferai mon possible pour aider la victime.
  - Si je me fâche pendant que je suis en ligne, je me calmerai avant de dire ou de faire quoi que ce soit.
  - Je ne partagerai en ligne aucun contenu qui appartient à quelqu'un d'autre sans sa permission.
  - Je penserai toujours à comment quelqu'un pourrait se sentir avant de partager quelque chose en ligne. Je ne partagerai jamais quoi que ce soit qui pourrait embarrasser quelqu'un ou le faire sentir mal.
  - Dans le cadre de mes travaux scolaires ou de mes projets personnels, je citerai toujours les gens dont j'ai utilisé les idées ou copié une partie des textes directement sur Internet.
  - Je ne désactiverai aucun logiciel de filtrage installé par mes parents sur l'ordinateur ou le téléphone intelligent.
  - Je n'achèterai rien en ligne à moins d'avoir la permission de mes parents.
  - Je n'utiliserai jamais mon téléphone pendant que je conduis.

Visitez http://mediatechparenting.net/contracts-and-agreements (en anglais seulement) pour obtenir d'autres excellents modèles d'entente à rédiger avec votre famille.

5. L'éthique en ligne

Il est tout aussi important de protéger les jeunes des dangers d'Internet que de protéger Internet des jeunes qui pourraient en faire une utilisation abusive. Les parents, gardiens d'enfants, enseignants et adultes doivent montrer aux jeunes à être prudents en ligne en protégeant leurs renseignements personnels et en évitant les prédateurs. Cependant, ils doivent aussi leur parler de l'éthique en ligne et des répercussions que peuvent avoir leurs gestes sur d'autres personnes.

- **Faites attention à ce que vous publiez.** Les jeunes doivent savoir qu'une fois qu'ils publient quelque chose en ligne, ils n'en ont plus le contrôle, même s'ils le font de façon anonyme. Tout ce qui est publié peut être transféré, copié et enregistré, peut-être pour toujours. Ce qui paraît amusant ou « cool » aujourd'hui, comme les photos prises lors d'une fête, pourrait apporter beaucoup de problèmes à votre enfant ou le mettre dans l'embarras demain. Vous devez dire à votre enfant qu'il est important de contrôler l'image qu'il projette dans le monde virtuel. En effet, les employeurs vérifient souvent la présence en ligne de leurs candidats, et les découvertes qu'ils font pourraient avoir une influence sur de futures possibilités de travail pour votre enfant.
- **Protégez les sentiments et les réputations.** Votre enfant est responsable de préserver sa réputation en ligne, mais celle des autres également. On parle de cybertintimidation lorsqu'un enfant ou un adolescent se sent mal à l'aise, humilié, tourmenté ou harcelé sur Internet. Comme ces gestes se déroulent derrière des écrans, les jeunes oublient souvent que la cyberintimidation a des répercussions graves et bien réelles sur toutes les personnes impliquées. Votre enfant doit savoir que lorsqu'il « aime » ou partage une publication offensante – un geste souvent perçu comme étant inoffensif – il contribue à la propagation de l'humiliation et devient une partie du problème. Ces gestes pourraient même constituer une infraction criminelle.
- **Connaissez la loi.** Les adolescents partagent souvent du contenu explicite entre eux en utilisant des services de messagerie (communément appelé le sextage). Toutefois, ils ne connaissent peut-être pas les risques et les conséquences liés au partage de ce type de contenu. Au Canada, la loi en matière de cyberintimidation interdit la distribution non consensuelle d'images intimes. Le site web Pensez cybersécurité présente plus d'information sur les lois que votre adolescent devrait connaître.
- **Téléchargez avec prudence et respect.** Pour être un cybercitoyen courtois et réfléchi, il est important de respecter les droits d'auteur. Les jeunes téléchargent beaucoup de films, d'émissions de télé, de musique et de logiciels protégés par des droits d'auteur sur leurs appareils, risquant ainsi de contracter des virus ou de faire l'objet de poursuites judiciaires. Discutez de ces conséquences avec votre enfant et montrez l'exemple en obtenant toujours le consentement de façon légale : quelques dollars de plus pourraient vous éviter de gros maux de tête plus tard.
- **Respectez vos valeurs.** Les parents devraient communiquer leurs valeurs à leurs enfants et leur montrer comment être de bons cybercitoyens. Tous les jours nous sommes amenés à faire des choix éthiques, et le fait d'utiliser la technologie n'y change rien. Ne partagez que les renseignements que vous voulez que d'autres voient, ne divulguez pas vos mots de passe et adoptez un comportement approprié dans votre utilisation des téléphones intelligents et des réseaux sociaux. Lorsque l'on parle de valeurs et d'éthique, on parle des répercussions de nos actions sur les autres. N'oubliez jamais ce qui est important pour vous et vos enfants feront de même.

Il est toujours bon d'activer la fonction de contrôle parental et d'accorder des autorisations limitées sur les comptes de votre enfant. Cela étant dit, une des meilleures façons d'aider votre enfant à être un cybercitoyen qui agit avec éthique et en toute sécurité, c'est de maintenir le dialogue et de fixer des règles de base concernant leurs activités en ligne.

Pour obtenir de plus amples renseignements sur la cybersécurité, visitez pensezcybersécurité.gc.ca

6. Mesures pour protéger d'avantage vos jeunes lorsqu'ils utilisent un téléphone intelligent

Si vous perdez votre téléphone intelligent

Votre téléphone intelligent et celui de votre enfant contiennent probablement une application permettant de localiser le téléphone au moyen de la technologie GPS si vous le perdez. Par exemple, la fonction Localiser mon iPhone d'Apple ou Where's my Droid d'Android. Si l'application ne vous permet pas de localiser votre téléphone, n'essayez pas de le repérer à l'aide de l'outil de localisation GPS, car vous pourriez vous retrouver dans une mauvaise situation. Faites plutôt ce qui suit :

- **Numéro de série de votre téléphone intelligent :** Lorsque vous achetez un téléphone intelligent pour votre enfant ou que vous lui donnez votre ancien téléphone, notez le numéro IMEI (international mobile equipment identification) et le numéro de série électronique du téléphone (ESN) et conservez-les en lieu sûr, car vous devrez fournir ces numéros à votre fournisseur de services et au service de police en cas de perte ou de vol de votre téléphone. Pour connaître votre numéro IMEI, composez ***#06#** et le numéro s'affichera à l'écran. Vous le trouverez également sur l'étiquette blanche de la pile.
- **Mots de passe difficiles à deviner :** Avant de donner un téléphone à votre enfant, assurez-vous de créer un mot de passe difficile à deviner que vous et lui connaîtrez. Demandez aussi à votre enfant de vous informer lorsqu'il change le mot de passe.
- **Communiquez avec votre fournisseur de services :** La première chose à faire si vous perdez ou vous faites voler votre téléphone est de communiquer avec votre fournisseur de services mobiles. Il vous aidera à désactiver votre appareil, à supprimer toutes les données qu'il contient et à rétablir les paramètres d'usine. De plus, votre fournisseur de services placera votre téléphone sur une liste noire nationale, le rendant non fonctionnel sur tous les réseaux mobiles canadiens.
- **Signalez le vol de votre téléphone :** Communiquez avec votre service de police local pour les informer du vol de votre téléphone et donnez-leur votre numéro IMEI.

"Quel est le numéro IMEI de votre appareil?"

7. Ressources additionnelles

- Pour obtenir des ressources pour assurer votre sécurité et celle de votre famille en ligne, visitez TELUS AVERTI (utilisation d'Internet et des téléphones intelligents en toute sécurité).
- Réservez une séance d'une heure gratuite avec un spécialiste du Centre de formation TELUS pour vous et votre enfant afin de découvrir toutes les fonctions et options de sécurité de votre téléphone intelligent.
- TELUS AVERTI offre d'autres guides qui pourraient s'avérer utiles :
  - TELUS AVERTI – Guide sur l'usage des téléphones intelligents et la distraction au volant (en anglais)
  - TELUS AVERTI – Aider nos jeunes à naviguer dans un monde branché
  - TELUS AVERTI – Une question de confidentialité

Comment vous pouvez participer au programme TELUS AVERTI

Si vous avez des questions ou désirez réserver une séance TELUS AVERTI gratuite pour l'école de votre enfant ou votre groupe de parents.

- Visitez-nous à **telus.com/wise**
- Communiquez avec nous à **averti@telus.com**
- Joignez-vous à la discussion en ligne avec @TELUS sur Twitter en utilisant **#TELUSAVERTI**

TELUS[MD]