CENTRE CANADIEN *de* PROTECTION DE L'ENFANCE
Aider les familles. Protéger les enfants.

L'usage sécuritaire des téléphones intelligents

Un guide pour les parents

mobilite.protegeonsnosenfants.ca

Avec le soutien de : TELUS

LA SÉCURITÉ DAN
L'ESPACE NU

NS
MÉRIQUE

Pour les parents et les préados/ados*, le **téléphone intelligent** s'avère utile à la fois comme moyen de communication et dispositif de sécurité; or, comme la plupart des technologies, il comporte des risques pour la sécurité de son utilisateur. Comme parent, vous devez être en mesure d'expliquer à votre préado/ado les consignes de sécurité à respecter avec son téléphone. En observant la façon dont votre préado/ado utilise son appareil vous lui montrez que sa sécurité et son bien-être vous tiennent à cœur.

Le site Sécurité mobile, réalisé conjointement par le Centre canadien de protection de l'enfance et TELUS, se veut un complément au présent guide. Il vous renseignera sur les risques auxquels sont exposés les jeunes utilisateurs de téléphones intelligents et vous expliquera les mesures préventives qui s'imposent. Cliquez mobilite.protegeonsnosenfants.ca pour vous renseigner sur les risques et les mesures de sécurité propres à chaque tranche d'âge.

*Le Centre canadien de protection de l'enfance déconseille aux parents d'acheter un téléphone intelligent à un enfant de moins de 10 ans.

L'USAGE DU TÉLÉPHONE INTELLIGENT CHEZ LES PRÉADOS ET LES ADOS

Navigation et applications

Les préados/ados utilisent principalement leur téléphone intelligent pour jouer à des jeux, interagir sur les réseaux sociaux et écouter de la musique au moyen d'applications (ou applis). Facebook[MD], Twitter[MD] et Kik Messenger[MD] comptent parmi les applis les plus populaires.

Communications et textos

Les préados/ados utilisent souvent leur téléphone intelligent pour envoyer des textos, car c'est là pour eux un moyen rapide, facile et discret d'échanger de l'information. BBM[MD] et iMessage[MC] sont deux applis préinstallées qui s'utilisent largement pour texter. Skype[MC], Kik Messenger[MD] et Facebook[MD] Messenger sont aussi des applis de textage populaires offertes en téléchargement. En 2012 seulement, les Canadiens ont envoyé un nombre époustouflant de 96,5 milliards de textos[1].

Prise et partage de photos et vidéos

Les préados/ados aiment prendre des photos et des vidéos d'eux-mêmes et de leurs amis avec la caméra de leur téléphone. Ces images finissent habituellement par aboutir sur les réseaux sociaux ou sont envoyées à d'autres jeunes par texto. Instagram[MD], Snapchat[MC] et Vine[MD] sont des applis populaires pour la prise et le partage de photos et de vidéos. En date de septembre 2013, les Canadiens envoyaient en moyenne 3,5 millions de messages MMS par jour[2].

[1]Association canadienne des télécommunications sans fil, http://www.txt.ca/french/business/statspressfr.php, page consultée le 12 novembre 2014.

[2]Association canadienne des télécommunications sans fil, http://www.txt.ca/french/business/statspressfr.php, page consultée le 12 novembre 2014.

Abonnez-vous aux Alertes Cyberaide.ca à l'adresse cyberaide.ca/alertes pour vous renseigner sur les utilisations inquiétantes du numérique et les nouvelles ressources pour mieux protéger les enfants.

Comment les préados/ados communiquent entre eux

CE QU'IL FAUT SAVOIR SUR LES APPLIS

1. **La plupart des applis sont offertes en téléchargement gratuit.** La seule condition pour télécharger des applis gratuites, c'est d'avoir un compte chez un fournisseur d'applis comme iTunes[MD], Google Play[MD] ou BlackBerry App World[MC]. Certaines applis ont un processus d'inscription, mais il suffit parfois d'indiquer un nom d'utilisateur et un mot de passe pour s'inscrire.

2. **Les applis de textage, de clavardage et de réseautage social permettent de communiquer facilement avec des correspondants inconnus.** Certaines applis de textage sont préinstallées dans l'appareil (p. ex. SMS, iMessage[MC] ou BBM[MD]), d'autres peuvent être téléchargées et utilisées gratuitement (p. ex. Skype[MC], Kik Messenger[MD] et Facebook[MD] Messenger). Ces applis permettent de communiquer avec d'autres utilisateurs de téléphone intelligent et de toutes sortes d'autres appareils connectés à Internet. La plupart permettent aux utilisateurs de communiquer entre eux en s'identifiant seulement par un nom d'utilisateur, sans fournir aucun renseignement d'identification.

3. **Certaines applis permettent de publier ou d'envoyer des messages anonymes.** Il y a des applis qui permettent de publier un message sur un babillard à la vue de tous ou d'envoyer un message directement à un utilisateur, le tout anonymement. Certaines applis offrent beaucoup de souplesse à l'utilisateur pour créer des règles qui empêcheront certaines personnes de le contacter.

4. **L'historique des communications n'est pas nécessairement conservé.** Certaines applis de clavardage et de réseautage social enregistrent les conversations, mais permettent aussi de les effacer facilement. D'autres enregistrent les conversations par défaut ou peuvent être paramétrées – quoique pas toujours facilement – pour conserver l'historique des messages. Certaines permettent d'échanger par texto, par vidéo ou par audio sans qu'aucune trace des communications ne soit conservée.

5. **De nombreuses applis de textage, de clavardage et de réseautage social permettent de créer un profil aussi garni ou dégarni que l'utilisateur le souhaite.** Dans la plupart des cas, il n'y a pas de limite à ce que l'on peut mettre dans son profil (renseignements personnels, photos, etc.). Ces informations sont accessibles aux autres utilisateurs du même service, quoique certains services offrent des paramètres de confidentialité (réglés par l'utilisateur) permettant d'en limiter l'accès. Parfois, les photos sont géolocalisées ou situées sur une carte, de sorte que les autres utilisateurs puissent voir à quel endroit elles ont été prises.

6. **Les applis de jeu permettent aussi de jouer avec des inconnus.** De nombreuses applis offrent un environnement multijoueur dans lequel on peut trouver d'autres personnes avec qui jouer. Certaines permettent même de se connecter à d'autres services comme Facebook[MD] pour jouer avec des abonnés de ces services. Les utilisateurs ont souvent accès à des informations assez limitées sur l'un et l'autre, mais ont la possibilité de clavarder en jouant. En règle générale, aucun historique de ces conversations n'est conservé.

7. **Certaines applis créent chez l'utilisateur l'assurance qu'il ne restera aucune trace des informations échangées.** Ces applis offrent la possibilité de partager des photos et des vidéos pour un temps limité, mais elles ne sont pas toujours aussi sûres que leur fabricant le prétend. De nouvelles façons de capturer les informations échangées sont constamment mises au point.

8. **Certaines applis peuvent être « cachées » sur l'appareil**. Sur la plupart des appareils, les applis sont représentées par des icônes affichées sur des pages ou dans des dossiers. Ces icônes peuvent être dissimulées dans des dossiers, de sorte qu'elles ne seront plus facilement visibles au premier coup d'œil.

▸ Pour plus de détails, cliquez **mobilite.protegeonsnosenfants.ca.**

CONNAÎTRE LES **RISQUES** ►

Avant d'acheter un téléphone, renseignez-vous sur les capacités techniques de l'appareil et les risques qui en découlent. On peut répartir les risques inhérents à la technologie en trois catégories, selon qu'ils se rapportent au **contenu** qui est mis en circulation, à l'instantanéité des **communications** avec autrui et à la **conduite** des jeunes internautes lorsqu'elle risque de les mettre en danger ou de mettre une autre personne en danger.

Muni d'un téléphone intelligent, votre préado/ado devient potentiellement joignable via Internet à toute heure du jour ou de la nuit, sept jours sur sept. Tâchez le plus possible de savoir qui sont les personnes qui communiquent avec votre enfant et par quelles applis.

Textage

- Un texto contenant des renseignements personnels ou des photos peut être retransmis à d'autres utilisateurs.
- Des textos de harcèlement et des textos indésirables (p. ex. des pourriels inappropriés) peuvent être transmis à l'appareil.
- L'auteur d'un message peut parfois camoufler son identité et être difficile à retracer.

Photos et vidéos

- Il est possible de reproduire une photo ou une vidéo transmise par téléphone, de la modifier ou de la diffuser sur Internet à l'insu de l'envoyeur ou sans son consentement.
- Une photo ou une vidéo transmise par téléphone pourrait révéler l'apparence d'une personne et l'endroit où elle se trouve.
- Il est facile de prendre ou de capturer des photos et des vidéos, parfois même à l'insu de la personne.
- Il est facile de prendre et d'enregistrer des photos à caractère sexuel et de les partager avec d'autres personnes.

ECHNOLOGIE

Bon à savoir

Wi-Fi

- Les appareils mobiles compatibles Wi-Fi peuvent échanger des données par la voie des airs. Même si vous ne souscrivez pas un plan de données pour son téléphone intelligent, votre préado/ado pourra quand même se connecter à des réseaux Wi-Fi pour aller sur Internet.

Navigation mobile

- Il est possible de transmettre des pourriels, des virus et des programmes malveillants à un téléphone intelligent. Un programme malveillant ou un virus peut perturber le fonctionnement de l'appareil et même collecter des données et des informations personnelles importantes. Un programme malveillant peut aussi afficher du matériel sexuellement explicite.

Services de géolocalisation

- La plupart des téléphones sont munis d'un récepteur GPS. La présence de certaines applis GPS sur l'appareil peut permettre de localiser l'utilisateur à quelques mètres près.

▸ Pour des consignes de sécurité âge par âge, cliquez **mobilite.protegeonsnosenfants.ca**.

CONTENU

Quels sont les risques?

Exposition à des contenus inappropriés

- Votre ado pourrait recevoir des textos, des photos ou des vidéos sexuellement explicites.
- Votre ado pourrait voir des sites sexuellement explicites ou inappropriés.

Diffusion incontrôlée de photos ou de vidéos

- Des photos, des vidéos ou des renseignements personnels peuvent être envoyés à d'autres jeunes ou à une personne inconnue.
- Une photo ou une vidéo peut facilement et rapidement se retrouver sur Internet. Reproduire et diffuser des photos et des vidéos est un jeu d'enfant depuis l'avènement des applis de partage de photos (p. ex. Instagram[MD]), des sites de partage de vidéos (p. ex. YouTube[MD]) et des réseaux sociaux (p. ex. Facebook[MD]).
- Des photos peuvent être reproduites, imprimées et être exposées à la vue de tous dans un lieu public (p. ex. à l'école).

COMMUNICATIONS
Quels sont les risques?

Se faire intimider ou harceler

Le téléphone intelligent est devenu l'outil de communication privilégié des préados/ados, et le fait de recevoir des appels ou des textos blessants ou importuns peut s'avérer particulièrement pénible et déstabilisant. Pareille tactique peut s'utiliser pour manipuler quelqu'un et suivre ses allées et venues. Si la situation devient problématique, il y aura peut-être lieu de faire intervenir la police.

Rapports sociaux sur Internet

Les relations qui naissent sur Internet évoluent généralement plus vite que dans la vraie vie. Dans ces relations virtuelles, l'envie de rencontrer l'autre en personne se manifeste parfois rapidement; il arrive aussi que ces relations donnent lieu à des demandes de photos intimes ou d'informations personnelles. Certains préados/ados n'y voient aucun danger ou ne jugent pas nécessaire de prendre des précautions. Il est important de rappeler à votre préado/ado de ne jamais aller rencontrer quelqu'un qu'il ne connaît que par Internet sans vous demander la permission. Parlez à votre préado/ado des risques associés au partage d'informations personnelles et de photos.

Le saviez-vous? La sextorsion est un problème grandissant sur Internet. Cette pratique consiste à contraindre des jeunes à transmettre des images à caractère sexuel ou à se livrer à des actes sexuels à la webcam, pour ensuite les faire chanter en les menaçant de diffuser les photos ou les vidéos ainsi obtenues s'ils refusent de verser une somme d'argent ou d'envoyer d'autres images à caractère sexuel.

CONDUITE

Quels sont les risques?

Violation des limites sociales et émotionnelles

Les médias sociaux, les textos et le partage de photos et de vidéos permettent aux préados/ados d'interagir avec d'autres personnes sans être en leur présence, ce qui élimine certains codes sociaux qui les inciteraient autrement à se conduire de façon appropriée. Les communications dans l'espace numérique semblent réduire les inhibitions à transgresser les limites sociales. Tout ce qui est échangé (photos, vidéos, textos), même en confidence, peut facilement être utilisé de façon mal intentionnée par d'autres personnes.

Participation à des échanges potentiellement illégaux

- Selon les circonstances entourant l'incident, les actes associés à la prise et à l'échange de photos ou de vidéos de nudité ou d'images à caractère sexuel (où les sujets ont moins de 18 ans) peuvent s'avérer illégaux.
- Un comportement intimidant ou coercitif peut s'avérer illégal.

Comme parent, il est important de veiller sur la sécurité de votre préado/ado tout en développant sa capacité d'utiliser son jugement et de faire face à diverses situations. Il est important de se rappeler que les préados/ados font des erreurs. Rappelez souvent à votre ado qu'il peut vous parler sans crainte de tout ce qu'il vit.

UTILISER UN TÉLÉPHONE INTELLIGENT EN TOUTE SÉCURITÉ

Les parents et les responsables d'enfants doivent s'engager activement auprès de leur préado/ado pour fixer les règles à suivre et entretenir le dialogue à ce sujet. Voici quelques conseils généraux de prévention :

1. Voyez s'il est possible de paramétrer l'appareil de façon à bloquer les contenus de mauvais goût (sites, images, propos destinés à un public adulte, matériel sexuellement explicite, etc.) ou de le faire au moyen d'applis de contrôle parental ou par l'entremise du fournisseur de services. Voyez aussi s'il est possible d'empêcher le téléchargement d'applis sans permission sur l'appareil (avec ou sans appli de contrôle parental).
2. Imposez des balises (fixez des règles pour les textos ou les jeux à l'heure du coucher, les jeux multijoueurs, etc.).
3. Discutez avec votre ado de l'importance du respect des limites avec la technologie. La protection des renseignements personnels et de la vie privée est primordiale, autant pour votre ado que pour les autres. Expliquez-lui que certaines applis sont plus vulnérables que leur fabricant le prétend et peuvent donner une fausse impression de sûreté.
4. Expliquez la différence entre une relation saine et une relation malsaine. Expliquez que le matériel sexuellement explicite qui se trouve sur Internet n'a rien à voir avec l'intimité. Une relation saine repose sur différents facteurs comme la bienveillance, le respect et la confiance.
5. Dites à votre préado/ado de ne jamais répondre à des appels ou à des messages importuns, dérangeants ou indésirables quelle que soit l'application utilisée pour les transmettre, d'essayer de conserver ces messages (vocaux ou texte) et de prévenir un adulte de confiance qui saura l'aider.
6. Parlez-lui des mécanismes qui permettent aux utilisateurs d'un site ou d'une appli de signaler des contenus, des messages ou des utilisateurs qui dérangent. Un signalement peut mener au retrait du contenu ou à l'expulsion de l'utilisateur.
7. Rappelez à votre préado/ado que les textos, photos et vidéos peuvent facilement faire l'objet d'une diffusion incontrôlée. Expliquez-lui les risques et pensez à vous inspirer d'incidents rapportés par les médias pour aider votre ado à développer son esprit critique.
8. Voyez avec lui comment paramétrer les applis de façon à bloquer les messages venant d'utilisateurs anonymes. Plusieurs applis offrent beaucoup de souplesse à l'utilisateur pour créer des règles qui empêcheront certaines personnes de le contacter. Il est recommandé de paramétrer les réglages de sorte que toute interaction venant d'un utilisateur anonyme soit bloquée.
9. Rappelez à votre préado/ado qu'il est possible de bloquer toute communication venant d'une personne qui l'ennuie. Expliquez-lui qu'il peut être nécessaire de faire intervenir un adulte de confiance pour tenter de résoudre le problème.
10. Rappelez à votre préado/ado qu'envoyer des photos de nudité ou des photos à caractère sexuel à d'autres personnes est un geste potentiellement illégal qui pourrait causer une humiliation considérable ou entraîner une situation dangereuse.

▸ Pour des consignes de sécurité âge par âge, cliquez **mobilite.protegeonsnosenfants.ca**

CENTRE CANADIEN *de* PROTECTION DE L'ENFANCE™
Aider les familles. Protéger les enfants.

Le Centre canadien de protection de l'enfance est un organisme caritatif voué à la protection personnelle des enfants. Il offre des programmes et des services à la population canadienne dans le but de réduire la violence faite aux enfants. Consultez le site **protegeonsnosenfants.ca** pour plus de détails.

Notre mission :

- Réduire les cas de disparition et d'exploitation sexuelle d'enfants
- Sensibiliser la population à la protection personnelle et à l'exploitation sexuelle des enfants
- Soutenir les recherches d'enfants disparus
- Représenter et promouvoir la cause des enfants disparus ou exploités sexuellement

decembre 2014

cyberaide!ca™

Signalez les cas d'abus à Cyberaide.ca

Cyberaide.ca est la centrale canadienne de signalement des cas d'exploitation sexuelle d'enfants sur Internet. C'est aussi un centre d'information, d'orientation et de ressources en ce qui a trait à la sécurité des enfants sur Internet.