



CANADIAN CENTRE for CHILD PROTECTION®
Helping families. Protecting children.



Smartphone Safety

A guide for parents/guardians



mobility.protectchildren.ca

Supported by:



SAFETY & TECHNOLOGY



TECHNOLOGY



Smartphones offer both communication and safety benefits for parents and tweens/teens.* However, like most technologies, they also pose some safety risks. Parents need to be able to talk to their tweens/teens about phone safety in a way that shows an understanding of the issues and the technology. Learning about your tween's/teen's phone use sends the message that you care and are concerned about them.

In addition to this booklet, the **Canadian Centre for Child Protection/ TELUS Mobile Safety site** provides parents with information about the potential risks posed to tweens/teens using smartphones, and highlights strategies that can be used to help keep them safe. We encourage you to visit mobility.protectchildren.ca for more information about age-specific risks and safety strategies.

* The Canadian Centre for Child Protection does not recommend that parents purchase smartphones for children under the age of 10.

SMARTPHONE

USE WITH TWEENS AND TEENS

Accessing browsers and apps

Tweens/teens spend most of their time on smartphones accessing games, social networking sites, and music through apps. Some of the popular apps include Facebook®, Twitter® and Kik Messenger®.

Communicating and messaging

Tweens/teens regularly use smartphones to send text messages as a quick, easy and discrete way to share information. Popular pre-installed messaging apps include BBM® and iMessage™. Other popular messaging apps available for download include Skype™, Kik Messenger®, and Facebook® Messenger. In 2012 alone, Canadians sent a staggering total of 96.5 billion text messages¹.

Capturing photos/videos and sharing them with peers

Tweens/teens commonly take photos/videos of themselves or their peers using cameras built into their phones – the content typically ends up on social networking sites or is sent to peers through messaging. Some of the popular photo/video sharing apps include Instagram®, Snapchat™ and Vine®. As of September 2013, Canadians were sending an average of 3.5 million MMS messages per day².

¹ Canadian Wireless Telecommunications Association, <http://www.txt.ca/english/business/statspress.php>, accessed online November 12, 2014.

² Canadian Wireless Telecommunications Association, <http://www.txt.ca/english/business/statspress.php>, accessed online November 12, 2014.

Sign up to receive
Cybertip.ca
ALERTS

Sign up for Cybertip.ca Alerts at cybertip.ca/alerts to learn about concerning technology trends and new resources designed to increase children's personal safety.

WHAT YOU MIGHT WANT TO

KNOW ABOUT APPS

- 1. Most apps are available to download for free.** The only requirement to download free apps is to have an account with an app service such as iTunes®, Google Play®, or BlackBerry App World™. Some apps have a registration process but may only require a username and password to register.
- 2. Messaging, chat and social networking apps allow you to easily connect with random individuals.** There are messaging apps that are included with the device (e.g. SMS, iMessage™ or BBM®) as well as those that can be downloaded and used for free (e.g. Skype™, Kik Messenger®, and Facebook® Messenger). These apps provide the ability to communicate with other smartphone users and users on a variety of other devices connected to the Internet. Most allow you to connect with individuals using only a username, without providing any identifying information.
- 3. Some apps allow posting or sending of anonymous messages.** In some cases, information can be posted anonymously to a message board for everyone to view - while in others, the message can be sent directly to a specific user. Some apps enable a user to control settings or create restrictions about who can contact them.
- 4. The history of the communication through apps may not be saved.** Some chat and social networking apps log conversations but allow them to be easily deleted. Other apps may log conversations by default or offer settings to save message logs, however, may be difficult to navigate. Others may allow text/video/voice chat without any record of the messages sent between users.
- 5. Many messaging, chat or social networking apps allow you to create a profile with as much or as little information about yourself as you choose.** In most cases, there are no restrictions on what can be entered into or added to a profile, including personal information and photos. This information is made available to other users of the service, although some services may provide privacy settings (set by the user) to limit what is shared. Many also permit geo-tagged photos to be saved and/or identified on a map which may allow other users to view the location the photos were taken.
- 6. Gaming apps also provide a method to connect with individuals randomly.** Many apps provide a multi-player environment allowing you to connect with other users to play games. Some gaming apps even allow users to connect to other services such as Facebook® to play with individuals on these services. Users may be given limited information about each other but are allowed to chat while in the game environment. In most cases, records of these chats are not saved.
- 7. Some apps give the user a sense of security that their information is only shared temporarily.** These apps may provide an opportunity to share photos or videos on a time limited basis, however, these may not be as secure as the claims they make. Innovative ways to capture the shared information are always being developed.
- 8. Apps can be 'hidden' on the device.** Most devices provide pages and folders to display and store the icons for apps on the device. These icons can be arranged to be more discreet and can be placed in folders where they are no longer visible to a quick view of the device.

► For more information, visit mobility.protectchildren.ca.

KNOW THE RISKS ▶

Prior to purchasing a smartphone, parents/guardians should educate themselves on the technical capability of the device along with the associated risks. There are three areas of risk that exist in the technology itself: the **content** it delivers, the instant **contact** it provides with others, and the **conduct** of youth online that may cause harm to either themselves or another person.

Smartphones provide those on the Internet with potential 24/7 access to your tween/teen. Do your best to learn who is communicating with your child and through which apps the contact is occurring.

Text messaging

- ▶ Texts containing personal information or photos can be shared with other users.
- ▶ Harassing or unwanted texts, including spam with inappropriate material, can be sent to the device.
- ▶ Messaging apps can be used to conceal an individual's identity — the origins of which can be hard to trace.

Camera/video

- ▶ Photos/videos sent from a phone can be reproduced, altered, or posted online without the sender's consent or knowledge.
- ▶ Photos/videos sent from a phone may disclose a user's location.
- ▶ Photos/videos can be easily taken or captured, potentially without another person's knowledge.
- ▶ Sexual photos can be taken, saved and easily shared with others.

TECHNOLOGY

what you should know

Wi-Fi

- ▶ Wi-Fi enabled mobile devices allow an electronic device to exchange data wirelessly. Even if you do not pay for a data plan for your tween's/teen's smartphone, they can still connect to free Wi-Fi hotspots to use the Internet.

Mobile web

- ▶ Smartphones can be the target of spam, viruses and malware. Malware and viruses not only affect the performance of phones but may also harvest valuable personal information and data. Malware may also display sexually explicit content.

Location Services

- ▶ Most phones come equipped with GPS. Depending on the GPS applications subscribed to by the user and the capabilities of the device, users can be located and pinpointed within a few metres.



CONTENT

what are the risks?

Exposure to inappropriate material

- ▶ Receiving sexually explicit texts, photos or videos.
- ▶ Viewing sexually explicit/inappropriate websites.

Losing control of photos or videos

- ▶ Photos/videos or personal information can be sent to peers or to someone unknown.
- ▶ Photos/videos can be easily and quickly posted online. Photo-sharing apps (e.g. Instagram®), online video sites (e.g. YouTube®) and social networking sites (e.g. Facebook®) make reproducing and distributing photos/videos extremely simple.
- ▶ Photos can be reproduced, printed and posted in a public place (e.g. a school) for anyone to see.



CONTACT

what are the risks?

Being bullied/harassed by someone

With smartphones as the primary tool tweens/teens use to communicate with one another, hurtful or harassing calls/texts can be especially distressing and disruptive. Individuals may use this tactic to control a person and monitor her/his whereabouts. If the situation becomes serious, it may require police involvement.

Connecting online

Relationships that start online seem to progress faster than they do offline. These online relationships can quickly progress to the desire to meet up in person or may lead to requests for intimate photos/private information. Tweens/teens may not perceive any threat or need for safety precautions. It's important to remind your tween/teen not to meet up with anyone s/he only knows online without parental permission. Talk with your tween/teen about the risks of sharing private information/photos.

Did you know? There is a growing issue on the Internet involving sextortion. This involves individuals who coerce youth into sending sexual images or engaging in sexual acts via webcam and then blackmailing them with the threat of distributing the images/videos if they do not provide more sexual content or pay money.

CONDUCT

what are the risks?

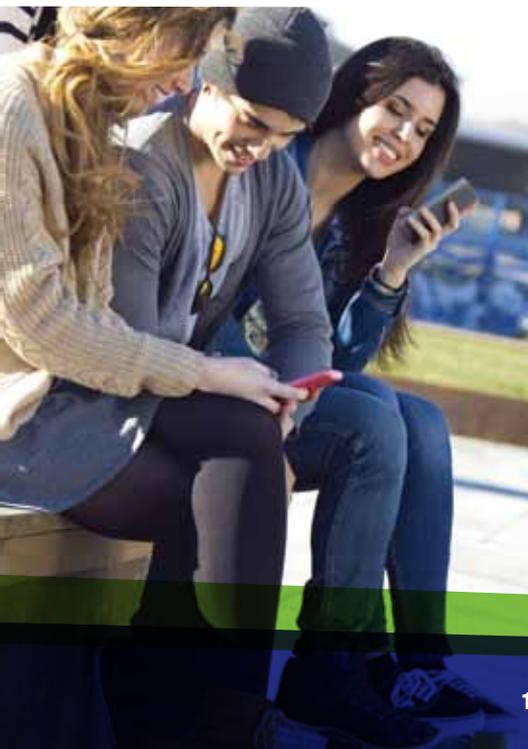
Breaking social/emotional boundaries

Social media, texting and photo/video sharing allows tweens/teens to interact without a face-to-face exchange and therefore removes some social cues that help guide appropriate behaviour and conduct. Communicating through technology seems to reduce inhibitions to cross social boundaries. Information (photos, videos, texts), even if shared in confidence, can easily be misused by others.

Engaging in exchanges that may be potentially illegal

- ▶ Depending upon the circumstances surrounding the incident, behaviours associated with the creation and exchange of nude or sexual photos/videos (of individuals who are under 18 years of age) may be illegal in nature.
- ▶ Engaging in behaviour that involves intimidation and/or coercion may be illegal in nature.

As a parent, it is important to balance efforts to protect your tween/teen with building her/his capacity to be critical and handle different situations. It is important to remember that tweens/teens make mistakes. Remind your child on a regular basis that s/he can talk to you about any issues s/he may be facing.



SMARTPHONE SAFETY TIPS

Parents should play an active role in establishing and regularly discussing guidelines for their tween/teen. General safety strategies include:

1. Exploring the possibility of concerning content (adult websites/images/language, sexually explicit content, etc.) being blocked using the settings on the device, through the use of parental control apps or by the carrier/service provider. Also explore the option of limiting the ability to download apps without permission on the device itself or with a parental control app.
2. Placing limits on phone use (i.e. guidelines around messaging and/or gaming at bedtime, guidelines related to multiplayer gaming, etc.).
3. Discussing the importance of boundaries when using technology. Protecting information and respecting privacy (their own and others) is crucial. Explain that although some apps may give a sense of security, they may be more vulnerable than claimed.
4. Discussing the difference between healthy and unhealthy relationships. Explain that sexually graphic material online does not represent intimacy. A healthy relationship involves many components such as caring, respect and trust.
5. Telling your tween/teen not to respond to bothering, harmful, or unsolicited calls or messages sent through any app, to save the messages where possible (voice or text), and to tell a safe adult who can help.
6. Discussing the built-in reporting options on sites/apps which enable users to report concerning content, messages, or users. Reporting content and users may result in such content being removed or users banned from a site/service.
7. Reminding your tween/teen that it is easy to lose control over what happens to texts, photos, and videos. Discuss the associated risks and consider utilizing scenarios in the media to develop your tween's/teen's critical thinking skills.
8. Adjusting control settings on apps to block communication from anonymous users. Many apps enable a user to manage settings and create restrictions about who can contact them. Adjusting settings so that interactions from anonymous user are blocked is recommended.
9. Reminding your tween/teen that s/he has the ability to cut off communication with any individual who is bothering her/him. Explain that this may mean involving a safe adult to help address the concerns.
10. Reminding your tween/teen that it may be illegal to send nude/sexual photos to others, and if sent, can result in significant humiliation or dangerous situations.

► For specific age-appropriate safety strategies, visit mobility.protectchildren.ca.



CANADIAN CENTRE *for* CHILD PROTECTION®
Helping families. Protecting children.

The Canadian Centre for Child Protection is a charitable organization dedicated to the personal safety of all children. Our goal is to reduce child victimization by providing programs and services to the Canadian public. Please visit protectchildren.ca for more information.

Our Mission:

- ▶ Reduce the incidence of missing and sexually exploited children
- ▶ Educate the public on child personal safety and sexual exploitation
- ▶ Assist in the location of missing children
- ▶ Advocate for and increase awareness about issues relating to missing and sexually exploited children

December 2014



Report online child sexual exploitation to Cybertip.ca

Cybertip.ca is Canada's national tipline for the public to report their concerns surrounding children being sexually exploited on the Internet. The tipline also provides the public with information, referrals and other resources to help keep children/youth safe while on the Internet.

© 2014 Canadian Centre for Child Protection Inc. All rights reserved. "CANADIAN CENTRE for CHILD PROTECTION" and "cybertip!ca" are registered in Canada as trade-marks of the Canadian Centre for Child Protection Inc. Telus is a registered trade-mark of Telus Corporation. All other trade-marks are the property of their respective owners.

mobility.protectchildren.ca