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

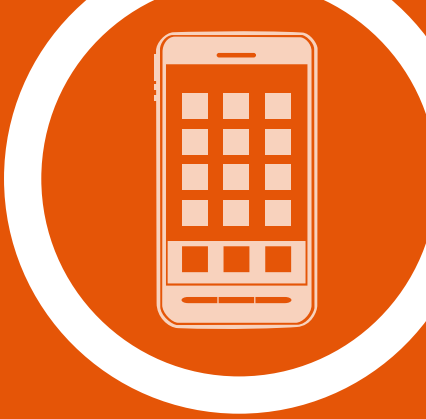
Smartphone Safety

A guide for parents/guardians

mobility.protectchildren.ca

Supported by: TELUS[MD]

LIVING IN A WIRELESS



WORLD

Smartphones offer both communication and safety benefits for parents and teens.* However, like most technologies, they also pose some safety risks. Parents need to be able to talk to their teens about phone safety in a way that shows an understanding of the issues and the technology. Learning about your adolescent'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 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.

WHAT ARE TEENS DOING ON THEIR SMARTPHONES?

SMARTPHONES

Communicating and messaging

Teens regularly utilize smartphones to send texts/instant messages as a quick, easy and discrete way to share information. Popular pre-installed instant messaging apps include BBM™ and iMessage®. In 2011 alone, Canadians sent a staggering total of 78 billion text messages[1].

Accessing browsers and apps

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

Capturing images/videos and sharing them with peers

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. As of June 2012, Canadians were sending an average of 1.5 million MMS messages per day[2].

Smartphones provide some important practical benefits — they allow teens to easily stay in contact with you (and you with them) and provide them with a handheld tool for learning and broadening their knowledge about the world, among other advantages. At the same time, reports to Cybertip.ca (Canada's national tipline for reporting the online sexual exploitation of children) indicate there are **some safety concerns that parents need to be mindful of.**

1. "stats," txt.ca, accessed January 4, 2013, http://txt.ca/english/business/statspress.php
2. "stats," txt.ca, accessed January 4, 2013, http://txt.ca/english/business/statspress.php

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 available to a specific device (e.g. SMS, iMessage® or BBM™). However, there are also a large number of apps that can be downloaded and used for free. These apps provide the ability to communicate not only with other smartphone users but also users from a variety of locations on the Internet. Most allow you to connect with individuals using only a username, without providing any identifying information.

3. **The history of the communication through apps may not be saved.** Some chat and social networking apps log the conversations but allow them to be easily deleted with the swipe of a finger. 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.

4. **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 images to be saved and/or identified on a map which may allow other users to view the location the images were taken.

5. **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 Twitter® and Facebook® to play with individuals on these services. Users connecting through game apps to play one another 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.

6. **Some apps give the user a sense of security that their information is only shared temporarily.** These apps may provide an opportunity to share images 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.

7. **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.

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 teens.

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

Text messaging

- Texts containing personal information or pictures 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 use to conceal an individual's identity — the origins of which can be hard to trace.

Camera/video phone

- 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 recorded, potentially without another person's knowledge.
- Sexual pictures can be taken and easily shared with others.

ECHNOLOGY

what you should know

Bluetooth® and WiFi

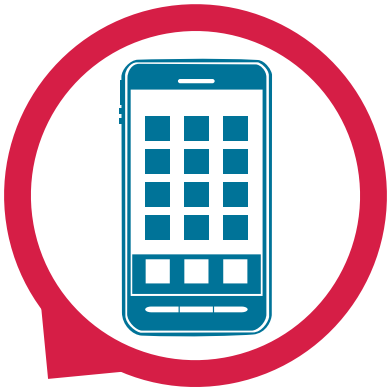
- Many mobile devices are Bluetooth-enabled. Data can be transferred between Bluetooth-enabled devices when they are within a short distance of each other. On a misconfigured device, there is the possibility that data, including personal information, viruses, malware, or inappropriate content can be transferred to and from a mobile device without the user being aware.
- WiFi-enabled mobile devices pose similar risks as Bluetooth-enabled devices; however, data is transferred at greater distances than Bluetooth through a connection to a wireless network, increasing the risk of compromise.

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.
- Phones can impact learning at school if restrictions aren't placed upon their use.

Global Positioning System (GPS)

- 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.



▸ For age-appropriate safety strategies, visit **mobility.protectchildren.ca.**

CONTENT

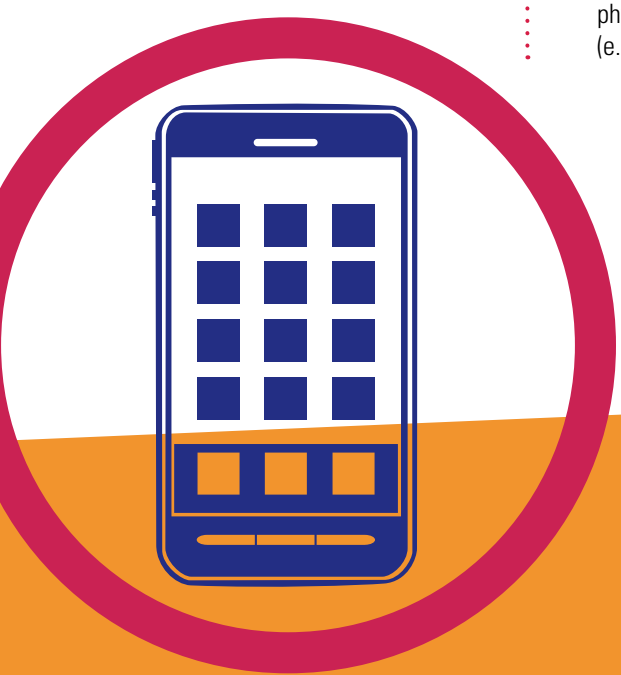
what are the risks?

Exposure to inappropriate material (receiving and viewing)

- 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 websites (e.g. Photobucket®), 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 and physically posted in a public place (e.g. a school) for anyone to see.



CONTACT

what are the risks?

Being bothered/harassed by someone

With smartphones as the primary tool 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 bothering turns to harassment it may require involvement from the police.

Meeting someone

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. Teens may not perceive any threat or need for safety precautions. It's important to remind your child not to meet up with anyone s/he only knows online without parental permission.

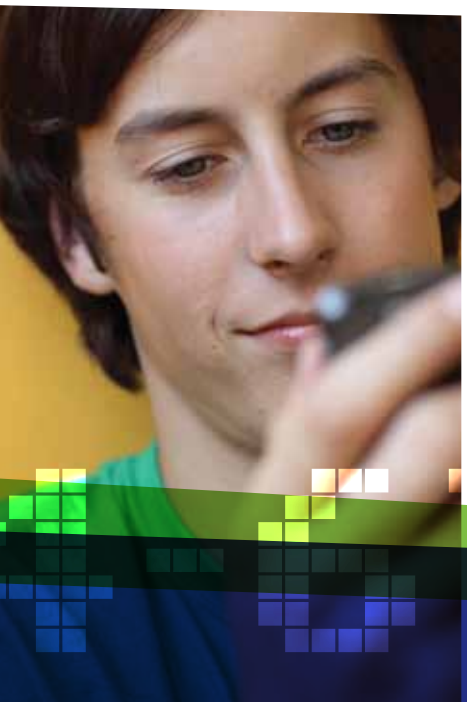
Did you know? There is a growing issue on the Internet with individuals named "cappers", who sit in chatrooms to secretly record sexual images/videos. Whatever they are able to screen capture in these chatrooms is then used to extort further sexual content, for the sole purpose of relentlessly humiliating the teen in various spaces on the Internet.

CONDUCT

What are the risks?

Breaking social/emotional boundaries

All teens want to belong and many do this by texting with friends. Texting allows teens to interact without a face-to-face exchange and therefore removes some social cues that help guide appropriate behaviour and conduct when meeting in person. Communicating through technology seems to reduce inhibitions to cross social boundaries. Information (pictures, 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 images/ 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 teen with building her/his capacity to be critical and handle different situations. It is important to remember that 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 enforcing guidelines for their teen. General safety strategies include:

1. **Taking the time to learn what features are included on the smartphone before purchasing it.** Of particular interest should be whether the phone has pre-installed apps, games, Internet access, photo/video capability, and whether it is Bluetooth-enabled.
2. **Exploring the possibility of potentially questionable 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.
3. **Placing limits on phone use (i.e. guidelines around messaging and/or gaming at bedtime, guidelines related to multiplayer gaming, etc.).**
4. **Discussing the importance of boundaries when using technology.** Protecting information and respecting privacy (their own and others) is critical. Explain that although some apps may give a false sense of security, they may be more vulnerable than claimed.
5. **Discussing the meaning of friendship.** Explain that in healthy friendships, friends protect and respect information that has been shared with them and would not misuse it to intentionally hurt their friend.
6. **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.
7. **Telling your 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.**
8. **Reminding your 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 teen's critical thinking skills.
9. **Reminding your teen that s/he has the ability to cut off communication with any individual who is harassing her/him.** Explain that this may mean involving a safe adult to help address the concerns.
10. **Reminding your teen that it may be illegal to send nude/sexual photographs to others, and if sent, can result in significant humiliation or worse.**

▸ 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

January 2013

cybertip!ca®

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.