Canadians Connected
Canadiens branchés

Cyber Security Consumer Tip Sheet

Mobile Devices

As well as invaluable tools for keeping in touch with our friends, families and our work, mobile devices have become an increasingly big part of how we access the Internet. Unfortunately, while many smartphones are nearly as powerful as computers, we often don't use the same caution with them as we do with our computers—and they often don't have the privacy and security safeguards that come built into computers. As well, the fact that we're never far from our mobile devices can bring a host of opportunities for us to be distracted and to make poor choices.

Risks to Using Mobile Devices

Data theft

Because mobile devices are so convenient, they are often the main tool we use to do both our work and our personal errands online. Unfortunately, this means that the device is typically packed with personal information related to the device owner. You don't need to be a hacker to get information off of someone's mobile device, either: people leave phones and tablets in cabs, airplanes and restaurants every day, and according to the Office of the Privacy Commissioner fewer than half of Canadians password-lock their devices or tighten their privacy settings. Once someone has access to your data they can use it to access your online accounts, buy things with your credit cards or even pretend to be you online.

Malware

While it is possible for malware to gain access to a mobile phone, in most cases when a mobile device is compromised it's because the user downloaded an app that contained some kind of malware. While most of us have become cautious about downloading to our computers, we are often distracted when using digital devices. —the one-click process makes it easier to download apps without thinking twice. Unlike malware designed for computers, which is typically delivered through illegal or "grey-market" venues such as file-sharing sites, mobile malware can often be found among the many legitimate apps available for little to nothing—often masquerading as games or even security software. There are two main types of known mobile malware: those that steal your data as you use your phone and those that charge money to your accounts without you knowing it.

Bullying

Bullying and harassment by mobile devices are at least as big an issue as they are on social networks. Research has found that teens who are heavy cell phone users are more likely both to be targets and perpetrators of online bullying, and the cameras found on almost every phone now make it possible for every embarrassing moment to be captured and uploaded.

Sexting

Because we mostly use phones to talk to or text a single person at a time, we sometimes forget that anything we do over a mobile device can be saved, copied and forwarded to any number of people. Sexting (and sharing sexts sent to you) can have consequences ranging from embarrassment to criminal prosecution, and is not just a problem for teenagers: in fact, a 2012 study found that adults are twice as likely as teens to do it.

Overspending

The convenience of buying things on a phone or tablet—whether it's apps for the device or merchandise in an online shop—can lead us to make purchases without thinking about them. As well, many game apps—especially those for children—encourage users to spend real money to advance in the game, and if a parent isn't careful kids may be able to use their credit card information. Finally, just using the phone can cost an unexpected amount as the price of making calls, sending texts and surfing the Web through mobile devices adds up.

Distraction

Many places have passed laws against using mobile devices while driving, but they can also cause accidents for cyclists and pedestrians. As well, having a mobile device handy while you're doing other things increases the temptation to multitask—which makes you less efficient at all the things you're doing. Mobile devices can also lead to sleep problems, especially for teenagers who feel a pressure to respond to texts right away and worry about missing what's going on among their friends.

Inappropriate content

Many of the issues faced by parents in moderating their children's online experience on the Internet are found with mobile devices as well. Many of the apps available are aimed at young children and teens, but because new apps are often rushed to the marketplace—and because app developers rate their own products –it can be hard to know what you're going to find.

Privacy Invasions

Even if you don't use your phone to store personal information, it's gathering data all the time about who and where you are. Many legitimate apps will communicate to your phone's device ID and your location to the app's developers or to third parties. Most often, this data gathering is spelled out in terms of service you agree to when you download it, but some invasions of privacy are done secretly and maliciously—including spyware that allows someone to turn on your device's camera or microphone remotely, even when it's is turned off.

How You Can Protect Yourself

Educate yourself. Make sure you understand what features are on a mobile phone before buying it for yourself or for a child. Find out what privacy and security options a device has and activate them; even better, find out before you buy a device which has the best security tools. Before downloading an app, read the Terms of Service to find out what data it's gathering about you.

Be polite. Treat people you talk to or text with the same way you would treat people offline. Remember that a lot of the cues we use to understand what someone means—their facial expression, their body language, their tone of voice—aren't present when you're texting, so phrase what you say carefully and don't jump to conclusions about what someone else means.

Think ahead. Imagine who might see any texts or pictures you send or forward with your device. Before you send a text or forward a picture, think about how the person receiving it—or the person who sent it to you—might feel.

Get an eraser. Software is available for nearly every mobile device that lets you track a device, disable it or wipe its memory remotely. Use this immediately if your device is lost or stolen. If you get a new device, make sure the old one has had its memory fully wiped before selling it, giving it away or throwing it out. (Your device's manufacturer should have this information on their website.)

Be secure. Set your Web accounts to use only secure connections by going to the "https" version of the site.

Be cautious. Do research on an app before you download it to make sure it's reliable and doesn't contain any undesirable content. Don't follow links sent in emails or text messages.

Turn off what you're not using. Bluetooth, WiFi and other ways of connecting devices can all be targeted by hackers; turn them off when you're not using them. Also, set all Bluetooth-enabled devices to "non-discoverable" so they don't appear to other Bluetooth users around you.

Don't expose your data. Never send any sensitive information, buy anything online, or do online banking when using a public hotspot. These are very vulnerable to hacking.

Set spending limits. To make online purchases, use prepaid or low-limit credit cards to keep from spending too much. If you share a device with someone else, make sure that your credit card information is out of the device's memory each time you finish an online purchase. Teach small children that purchases in games cost real money and that they need to ask for permission before buying anything. For children and teens, get a plan that either sets hard limits for texting (so that once they reach their limit they can't send texts, instead of paying an increased price) or get an unlimited texting plan.

Don't multitask. Never use a mobile device while you're driving, cycling, or walking. When you're working, set your device out of reach so you won't be tempted to check it. Establish "no phone zones" in your home—in bedrooms, for instance, or at the dinner table.

Start talking. Before a child or teen begins using a mobile device, make sure you have a conversation about these issues. Reassure them that they should come to you if anything happens and that you won't "freak out" and take away the device.

For more information:

See *Cyber Security Consumer Tip Sheet* from the Canadian Internet Registry Authority (CIRA) and MediaSmarts available at www.cira.ca and on the MediaSmarts website at www.mediasmarts.ca, as well as other digital literacy resources.

CIRA is a proud sponsor of MediaSmarts and the important work they do on behalf of Canadians.