Canadians Connected
Canadiens branchés

Cyber Security Consumer Tip Sheet
Socializing and Interacting Online

For most of us, the Internet has become an indispensable part of our social lives: we use it to keep up with old friends, keep in touch with our families and meet new people. Unfortunately, not all online interactions are as positive as these. This tip sheet will explain some of the issues we face when we socialize online and provide tips for dealing with them.

Risks to Your Privacy and Identity

Identity theft

Any time you add personal details to your online profile, there is the risk that a scammer may steal them. Though many may seem innocuous, it may only take a few details—your full name and your full date of birth, for instance—to open the door to your online accounts. As well, if your status updates aren't kept private scammers may watch them to gather details that will let them guess your password or your security question. On social networks such as Facebook, you can give scammers access to your account just by "liking" or "sharing" a scam page, or giving a malicious application access to your profile.

Phishing

Most phishing messages are fairly obvious scams: an e-mail or message asking you to send your password and login to one of your online accounts. Sharing personal details online, however—even talking about things like your job or your hobbies—can lead to you receiving socially engineered or "spear-phishing" messages. Because these have been customized to appeal to you, they can be much more convincing. They may, for instance, pretend to be from an online service you use, a game you play online or a site you visit regularly.

Identity spoofing

Going one step past identity theft, identity spoofing involves actually pretending to be someone else online. This may involve someone taking control of an existing online profile or creating a new one in your name. Identity spoofing is often just the first step in a larger fraud: for instance, scammers have been known to use hacked Facebook or e-mail accounts to send fake messages to that person's friends, where they claim to be in some circumstance and need money quickly (stranded in a foreign country, for instance).

Negative Interactions with Other Users

Trolling

This has become the umbrella term for anything done online to make someone's life difficult. It can range from being merely irritating to campaigns of libel, harassment and even threats of violence. Some players of online games enjoy making other players unhappy, for instance, making racist or misogynist comments or killing their game characters. Trolling is also often an issue in other interactive environments such as social networks or popular websites' comment forums.

Hostile environments

Along with specific individuals being trolled, many online environments can be hostile to women, visible minorities and other groups due to the language and attitudes that are common there.

Scams

The Internet has made life easier for a lot of people, including scam artists. While most online scams are fairly obvious, some of them may be tempting or frightening enough to get you on the hook: a notification that you've won a contest, for instance, or a warning that your computer is infected with malware.

Hoaxes

These can have a long life on the Internet because people often spread them without knowing they're hoaxes. While they're rarely harmful, they may lead you to make bad choices about your health or may unjustly influence your opinion of a particular product, company or person (celebrities and politicians are popular targets of online hoaxes).

Tips for Safe and Secure Surfing

Log off. Always log out of any online accounts after using them. This makes it more difficult for other users to access them (for instance, if you close your browser without logging off of Facebook, someone using the same computer will not need to log in to access your account).

Use privacy settings. Nearly all social networks have tools that allow you limit who can see your profile information and what you post online. At the very least, make sure that your account is not set to "public."

Practice good password habits. Use a strong password that's at least eight characters long, with a mix of upper- and lower-case letters and using some non-letter characters such as numbers or typographical signs. Customize your password for each account (you can do this by adding a first and last character that's unique to each account) and never share your passwords with anyone.

Play it cool. If you think you're being trolled by someone you know, don't respond: get a screen capture (hit Print Screen and then paste it into a graphics program) and wait until you can talk to the person offline. If it's someone you don't know or if the trolling continues, block the person and report the incident.

Stand up. If you witness harassment or if you don't like the language or attitudes you encounter in an online forum, let people know that you object. Report any kind of harassment or abuse; nearly all online games have moderators to whom you can make a report, and most social networks allow you to flag or report a post as being abusive. Even a private website can be reported to the site's Internet Service Provider, which will often refuse to host harassing or hateful material.

Keep it private. Don't give out personally identifying details in online environments—your full date of birth, your full name, your social insurance number, your home phone number—online. Remember, scammers may have hacked any one of your friends and may be watching everything you post. Be especially careful what personal details you give out on "public-by-default" networks such as Twitter. Remember to be careful with your data when using professional networking or job search sites as well, not just social networks.

Protect yourself. Use security software and browser extensions that notify you when you're being tracked online. Some security software will also notify you if a site is malicious before go there.

Be stingy with your data. Don't give out personal information when you don't absolutely have to: even if you're giving it to someone trustworthy, there's no guarantee they won't be hacked. Don't fill out online surveys, and teach kids not to share information about themselves and your family, even if a source seems trustworthy (scammers have used "Letters to Santa" sites to harvest information from kids).

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.

Be watchful. Check your bank accounts and credit cards periodically to make sure they're not being misused. As well, search for your own name every now and then (you can set up a Google Alert to do this automatically) to make sure that nobody is pretending to be you online.

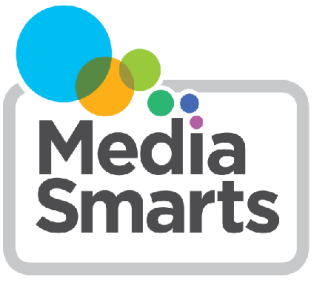
Be cautious. Almost all online scams can be avoided by remembering the saying "if it looks too good to be true, it probably is."

Think twice. Before believing, repeating or forwarding something, check it out: you can use a search engine to research it or go directly to hoax-busting sites like Snopes (www.snopes.com) and About Urban Legends (www.urbanlegends.about.com).

Check the source. Before responding to a message, make sure it really did come from the listed sender. Don't reply or click on any links until you've confirmed that. Even if a message comes from someone you know, trust your instinct if anything seems fishy.

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.