Canadians Connected
Canadiens branchés

Cyber Security Consumer Tip Sheet

Most of what we do online falls into one of three categories: Talk, Shop and Play. There are risks associated with all these activities that consumers need to be aware of so they can take the necessary steps to protect themselves and their computers.

The Canadian Internet Registration Authority (CIRA), in partnership with MediaSmarts wants to make sure you stay safe online. We have developed the following list of potential risks you may encounter during your online experience and suggested tools that may assist in lowering the level of risk.

Cybersquatting

Scammers may register a Web address that looks like it belongs to a legitimate business, or one that can easily be typed be accident when navigating to a legitimate Web site.
Tools to use: Bookmarks, Content Filters

Cookies

Small files your Browser saves on your computer. They often include data like your login and password.
Tools to use: Browser and antivirus updates, Clearing browser cache, Privacy policies, Private browsing tools, Secure sites.

Data theft

Your financial and personal data can be very valuable in the wrong hands.
Tools to use: Bookmarks, Browser and antivirus updates, Clearing browser cache, Creating strong pass words, E-mail encryption, Firewalls, Privacy policies, Privacy settings, Private browsing tools, Reporting online crime, Secure sites.

Excessive spending

The ability to buy real or virtual things instantly can make it easy to lose track of how much money you're spending.
Tools to use: Prepaid credit, Content filters

Griefing

Some people enjoy annoying other people on purpose and ruining experiences that should be fun.
Tools to use: Blocking other users, Contacting sites and ISPs, Content filters, Privacy settings, User/vendor rating systems

Identity spoofing

It's easy to pretend to be someone else online. There are lots of fake Facebook profiles and Twitter accounts that pretend to be from someone they're not.

Tools to use: Blocking other users, Browser and antivirus updates, E-mail encryption, Firewalls, Managing reputation, Privacy policies, Privacy settings.

Identity theft

Scammers can steal your online identity by getting access to your credit card or bank information or to other data you use to verify your identity.

Tools to use: Bookmarks, Browser and antivirus updates, Clearing browser cache, Firewalls, Privacy policies, Private browsing tools, Reporting online crime, Secure sites.

Malware

These programs — which may pretend to be something useful or install themselves by getting you to click a box — can hurt your computer or even take control of it.

Tools to use: Bookmarks, Browser and antivirus updates, Firewalls, Secure sites.

Online fraud

It's easy to be taken in by people online who promise more than they intend to deliver. You can see a complete list of online frauds at http://www.rcmp-grc.gc.ca/scams-fraudes/index-eng.htm.

Tools to use: Bookmarks, Contacting sites and ISPs, Prepaid credit, Reporting online crime, Secure sites, User/vendor rating systems.

Phishing scams

E-mails that try to get data from you by pretending to be from a bank or other business.

Tools to use: E-mail encryption, Reporting online crime.

Spyware

Malware that collects data from your computer. Some spyware records everything you type

Tools to use: Bookmarks, Browser and antivirus updates, Firewalls, Secure sites.

Tools to use – definitions

Bookmarks: Most browsers let you set Bookmarks or Favorites so you can go straight to your favorite Web sites.

Blocking other users: Almost every kind of online communication lets you block other users from contacting you.

Browser, firmware and antivirus updates: Your Browser is your first line of defence against malware, but you need to keep updating it. The same is true for free or commercial antivirus software. Internet-connected devices can also be vulnerable: make a habit of checking the manufacturer's site at least twice a year to see if there have been any updates to the firmware.

Clearing browser cache: The cache is where your Browser saves cookies, so you should clear it often.

Contacting sites and ISPs: Bad behaviour that is not criminal can be reported to a site or the ISP that hosts it.

Content filters: Browsers, ISPs, Web sites and special software all offer ways of filtering out unwanted content.

Creating strong passwords: Choose a password that is at least seven characters long and is based on a word with no personal connection to you. Change some of the letters to numbers or punctuation marks and use a mix of upper– and lower-case letters. Then customize the password for each site by adding the first and last letters of the site. (bananas becomes b@nAn2s and then fb@nAn2sk as your Facebook password.) Besides your online accounts, make sure that every networked device your family owns -- computers, phones, tablets, and Internet-connected devices like fitness trackers -- is protected by its own unique password.

E-mail encryption: E-mails can be intercepted and read. Encryption software and some e-mail services allow you to encrypt your e-mails so they remain private.

Firewalls: These block unauthorized access to your computer. Make sure yours is activated in your Control Panel.

Managing reputation: Do a search for your name to see what picture of you is on the Internet. If you find things that you don’t like, try to get them taken down. You can also publish things that reflect the image that you want to be the dominant picture of you. Consider registering your name as a Web address (www.yourname.ca).

Prepaid credit: Some banks and credit cards offer prepaid credit cards which only let you spend a set amount.

Private browsing tools: Most browsers have a function that lets you surf without saving anything in your cache.

Privacy policies: Any site that collects information should have a privacy policy. This should be written in easily readable language and should explain what will be done with any information you give them as

well as how you can get your information deleted if you want to. Make sure to check the privacy policy of any Internet-connected devices you're thinking of buying, as well: many of them collect a lot of data, both on their own and through access to your other accounts.

Privacy settings: Social networking sites such as Facebook have privacy settings that allow you to decide who can see what on your profile. The default settings are often not the most secure, so make sure yours are set to show your content only to your friends.

Reporting online crime: Online crime can only be stopped if it's reported. If you know about successful or attempted crime online, visit http://www.recol.ca/ to report it.

Secure sites: Secure Web sites use methods like encryption to keep your data safe. Look for a Web address that starts with "https" and a padlock icon at the top or bottom right of your browser window (not the Web site itself.)

User/vendor rating systems: Some online commerce sites allow users to rate vendors based on their experience with them. Look for a good rating and positive comments. As well, some online games and virtual worlds rate users based on other users' feedback. You can use these systems to help fight griefing.

About Us

The Canadian Internet Registration Authority (CIRA) is the organization that manages Canada's .CA domain name registry, develops and implements policies that support Canada's Internet community and represents the .CA registry internationally.

MediaSmarts is a Canadian not-for-profit centre for digital and media literacy. Its vision is that young people have the critical thinking skills to engage with media as active and informed digital citizens. MediaSmarts offers hundreds of digital and media literacy resources for librarians, parents and educators on its website http://mediasmarts.ca. @mediasmarts