Cyber Security Consumer Tip Sheet
Safe Surfing

Visiting websites is the most basic part of using the Internet. It can open up a world of fun and opportunity or a lot of unexpected problems, depending on how careful and well-prepared you are.

Most Web surfing is done through **browsers** such as *Internet Explorer*, *Firefox*, *Chrome* and *Safari*. While these browsers are updated regularly, our use of the Web has evolved to the point where we now do many things online, such as shopping and banking. For that reason, there are a number of potential risks that come with using the Web.

Types of Risk

There are two main types of risk relating to Web surfing: **technological** risks, which come as a result of dangerous software and "bugs" in the programs we use, and **behavioural** risks, which relate to decisions we make online.

Luckily, there are a lot of things you can do to protect yourself, your network, and your computer from these risks. Both kinds can be minimized by avoiding websites that you're not sure are legitimate and by not engaging in activities that expose your computer to unknown files, such as file-sharing and illegally downloading music or videos. If you share your computer with other people, make sure that they follow these precautions as well.

Technological Risks

The Bad News:
- Security issues may arise due to a design flaw in the product you are using.
- Handling these issues requires that you spend a little time learning about the software and hardware that you use. Luckily, it mostly boils down to a few simple precautions.

The Good News:
- Once you have learned how to take advantage of built-in security and privacy tools, it becomes much easier.
- You don't have to go far to look for many of these security solutions as they are often built right in to your browser and your computer.
- Technological flaws are often caught by the developers early on and fixed quickly through patches and software updates.

- Technologically-based cyber-security practices usually require only minor updating once they are put in place.

Ways to protect yourself:

Keep your software up to date: Software makers often release patches, fixes, and updates to address newly discovered bugs and security threats. By routinely updating your software, you are making certain that you are not vulnerable to known risks in your software. **It is particularly important to update your browser on a regular basis, since this is the main gateway between your computer and the Internet.** You can set your software update frequency in your computer's settings.

Secure your router and wireless network: Set a **strong password** or passphrase on your wireless router so that nobody outside of your household can access it. This protects you in two ways: 1) it bars access to storage and devices on your network, 2) it protects you from other people using up your monthly bandwidth limit.

Learn to manage your firewall: Firewalls allow you to control data connections coming in to your network from other computers. You can do this in your current operating system by turning off certain port numbers. Both Mac and Windows PCs currently have built-in firewall capabilities.

Use antivirus/anti-malware software: Invest in this powerful line of defense, learn to set it up, keep it updated, and let it do its thing. Some well-known brands of antivirus software include *Norton*, *Symantec* and *Avast*.

Know how to recognize a secure site: A secure site encrypts the data that is transmitted between it and your computer. This means that for the duration of the transmission, information being transmitted is secure. Secure sites are indicated by a Web address that starts with "https" (instead of just "http") and a padlock icon at the top or bottom right of your browser window (**not** the Web site itself).

However, using a secure site does not guarantee that your information is protected *after* your data is transmitted – for example, if the website stores your credit card number for future purchases – so it's a good idea to opt out of permanently storing this information as part of your customer profile.

Block what you don't want: Web browsers and email applications allow you to stop contact with specific individuals or sites. Most browsers have a content filtering feature which allows you to block sites based on the type of content.

Eat your cookies: Cookies are small files stored on your computer tracking your use of specific sites such as user preferences, login information, activity history, credit card information, and so on. It's a good idea to delete cookie files on a regular basis.

Use privacy tools: Social media sites and browsers offer tools that allow you to customize the amount of personal information you share with other users. Take the time to read,

understand and use these settings. Another privacy tool provided by browsers – private browsing – lets you surf the Web without leaving personally identifying records in cache files on the computer of where you've been. (It's important to keep in mind, though, that private browsing applies only to the computer you are using. Your internet service provider or other applications may still save records.)

Behavioral Risks

The Bad News:
- These risks can be hard to detect because you may accidentally be exposed to them by friends or family.
- There are no easy solutions to avoiding these risks. The only way to protect yourself is to always be careful and skeptical and to learn to recognize the most common scams.

The Good News:
- The solution to many behavior-based issues is often as simple as pausing for a moment and thinking before taking a given action.
- Behavior-based solutions are easy to implement and help make your Internet experience better for you and those around you.
- Learning to combat these kinds of security issues can allow you to help your family, friends, and coworkers to become more secure as well.
- The more you learn to think around these kinds of issues, the better you will become at spotting other behavior-based security pitfalls in the future.

Ways to protect yourself:

Stop and think: Before clicking on something or filling out a form, take a moment to ask yourself if what you're seeing really makes sense. How is it possible that this company you've never heard of can afford to give out all these free electronics devices in exchange for playing a short Web-based game? If something looks too good to be true, you already know that it is.

Get a second opinion: While there are many scam sites operating out there, your strongest weapon against them is sitting right at your fingertips. Anti-hoax websites can help you recognize scams or tell you if the story in that email is really true. The most famous is probably *Snopes* (www.snopes.com) but there are others such as www.hoaxbusters.org, www.truthorfiction.com, and www.nonprofit.net/hoax.

Don't participate: Many security threats become large problems because people forward them on to their friends and co-workers. Take an active stance against these kinds of attacks and make the buck stop with you.

Speak up: Did someone forward you a hoax? Sometimes, the people in our social circles forward false information to us with the best of intentions. Not everyone takes the time to be diligent about authenticating information before passing it on. You can help by saying something. Always be polite, and always back up what you say with evidence. Likewise, warn

other people about hoaxes and frauds when you come across them. Give them a heads up that something underhanded is going around. The more people point out these kinds of issues, the fewer victims will fall prey to them.

<u>Make strong passwords or passphrases</u>: You can make a strong password by taking a word (eight letters or longer) and changing some of the letters into numbers and characters (such as @ and !). For instance, the word "chandelier" can be changed to "c4@nd3l!er". It is also a good idea to diversify your passwords so that you aren't using the same one for every type of account you have. One easy way to do this is to add the first and last letters of the name of the site you're logging into; if your standard password were "c4@nd3l!er", for instance, your *Facebook* password would be "Fc4@nd3l!erk".

<u>Clear your cache, erase your history, and log out</u>: You should get into the habit of regularly clearing out information you would otherwise leave behind – especially on shared computers. It is also important to actually log out (via a "log out" or "exit" link) of Web services you were using so that subsequent users don't have access to your accounts.

<u>Don't take the bait</u>: Remember that banks and reputable companies will **never** ask you to send them account information by email. Do not respond to *phishing* emails that try to get your passwords or personal information by pretending to be a trusted source or authority. Common methods include sending emails under the guise of being a clerk from the user's bank, or emailing the user links to false websites. Not sure? Call the company or your bank to double check.

<u>Follow the crowd</u>: Take advantage of user-created lists or discussions that identify problem sites, companies, or individuals. (For example, online vendors on sites such as *Amazon* and *eBay* are rated by the people they have done business with.)

<u>Set limits</u>: Use alternative forms of online payment that are limited to a finite amount of money – such as prepaid credit cards, gift cards or timecards. If the card or its data is stolen or misused, only the amount of money on the card will be lost.

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.