Canadians Connected
Canadiens branchés

Cyber Security Consumer Tip Sheet
Protecting yourself from Malware

Malware is a general term to describe destructive programs that can harm your computer or any other device that connects to the Internet, including smart phones, mp3 players and tablets.

What does Malware do?

There are many different forms of malware: viruses, trojans, worms and rootkits. What they all have in common is they can carry out one or more of the following actions once they are on your digital device:

Damage your system. The most basic form of malware is a program which, once it infects your system, damages it in some way. This can be by rewriting or overwriting programs or data on your hard drive (such as your email address book), or by running one or more copies of itself. Both of these actions make your computer run less efficiently: in the first case because there is less free space on the hard drive (and in some cases because important files have been changed or deleted), in the second because the malware is using your device's processor to run itself.

Change how your system works. One common form of malware changes your Internet browser (Internet Explorer, Firefox, Chrome or Safari) so that you see altered Web content (such as different ad banners); have your home page changed; or are directed to false websites in order to gather your personal information.

Compromise your personal information. Some types of malware can read data on your system, such as financial information or account logins and passwords, and send them back to the program's author. One form of malware, called a keylogger, automatically records and transmits anything you type.

Use your system to spread itself. Whatever other purposes it might have, nearly all malware is designed to spread itself to other systems. For instance, the "ILOVEYOU" virus sent copies of itself to the first fifty contacts in the Microsoft Outlook address book of any system it infected.

Take control of your computer. While some malware is created simply as a prank, some is used to recruit computers into a botnet, a group of computers that have all been infected by the same piece of malware and are being used for such things as making coordinated attacks on websites and sending out spam email.

How Malware Infects Your Devices

Any contact between your computer or other devices and another system—even one as innocent as visiting a website—can lead to an infection with malware. However, some activities are more risky than others:

Downloading files. When you download files you are giving another computer permission to save something onto your hard drive. Many types of malware take advantage of this by either disguising themselves as something else or "piggybacking" on a legitimate file. Never download a file unless you are sure that the file and the source are legitimate.

Opening email attachments. Though it may feel safer, opening email attachments is exactly the same as downloading a file. Since malware often is designed to email copies of itself to anyone in the contact list of an infected system, do not assume that an attachment is safe just because it comes from someone you know. Never open an attachment unless you have confirmed that the sender meant to send it.

Visiting suspicious websites. Opening a website in your browser can infect your system through malicious scripts (programs that give your browser instructions). Malware sites often offer free content or other inducements to draw users. While file-sharing, pornography and other "grey market" sites are most likely to host malicious scripts, it's important to know that even the most well-established sites can be "hacked" and used to spread malware. Avoid sites with offers that seem "too good to be true."

Clicking unknown links. Even if you don't surf to a malware site intentionally, clicking the wrong link can send you there. Before clicking on a link, "hover" your cursor over it and make sure that the URL (Web address) that appears is the same. Users of social networks like Facebook and Twitter make heavy use of URL shorteners such as Bit.ly, so you should always be extra-cautious with these links: if a link appears by itself or with content that seems odd, it's best to be wary. As well, some programs (such as the Verify extension for Firefox) allow you to see the full URL.

Using unsafe storage devices. Storage devices—such as USB drives, portable hard drives or even digital music or video players—can contain malware as well. For example, in 2008 the US Department of Defense was infected by a virus carried on a USB drive. Do not use a USB drive or other storage device from an untrusted source. Before using any storage device, even one you bought new, run an antivirus scan on it using a computer that is not connected to the Internet and does not contain sensitive data. You can also verify with your antivirus manufacturer that their software supports scanning of storage devices before launching (Malware on USB drives may run automatically the moment you plug them into your computer not giving you the opportunity to run an antivirus scan.)

How You Can Protect Your System

As well as avoiding risky activities, you can reduce the risk of infecting your system in several important ways:

Update your system and browser regularly. Software makers regularly 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 (for Windows: Control Panel – Security Center – Automatic Updates; for Mac: Apple – Software Update). You should periodically check your third-party software applications as well. While these are often updated through the default auto-update, that's not always the case. The standard place to check that auto-update is enabled on both Mac and Windows computers is either under the "Help" or "?" menus or in "Preferences" or "Properties".

Use antivirus software. There are many programs designed specifically to detect, block and remove malware, such as Norton, Symantec, AVG and Avast. All of these are commercial software, but AVG and Avast both offer free versions which provide protection from most forms of malware (but lack other features such as blocking spam and phishing emails). Microsoft also offers Microsoft Security Essentials, a free antivirus program for Windows systems.

Set firewalls and router security. Your system's most basic defense is its firewall, which keeps other computers it contacts from making changes to it. Your firewall can be located and activated from your computer's control panel. As well, if you use a wireless router to access the Internet make sure that you have enabled security and set a password so that other people cannot access it.

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.