FACT SHEET

Computer Safety
Operating Safety & Security

Operating a computer without anti-virus software

is like

driving a car without seatbelts and airbags!

The risk of computer operating problems greatly increases once you're on the internet. The internet is a two-way form of communication with a culture of anonymity and/or false identities that can facilitate criminal activity. This can lead to serious problems including loss of privacy and/or control. Computer "hackers" can electronically access and use your computer by virtue of it just being left on without your even knowing it. Protecting your computer from external risks, such as viruses, spyware, phishing and malicious hackers is a necessary step in safe surfing of the internet.

For more on safe use of the internet, see Fact Sheet Internet Safety.

When you are considering what software to use, think about:

- What kind of info am I trying to protect?
- Educate myself on current risks and what products are available to minimize those risks.
- Purchase quality software; remember, you get what you pay for.

No one product will afford complete protection from all risks. You may have to use more than one.

Some basic things you can do to protect yourself include:

- Keep your browser updated.
- Update protection programs; i.e. spyware, anti-spam, etc. An anti-virus program is not a one time purchase. Most programs require annual updates with annual fees.

PASSWORDS

Basic computer security starts with a password. Care should be taken when choosing a password so that the password is unique and not predictable. Avoid the obvious, such as: "password", a birthdate, 12345, or, a phone number.

Instead:

- Make sure each password is different from your other passwords.
- Don't tack it on your computer/desk with a sticky note.
- Use a phrase or line from a poem that is easy to remember "I get up at 6:15 but am sometimes late." becomes Igua615BasL8,
- Never share your password with anyone.
- Regularly change your password.

E-MAIL

E-mail is a convenient way to send someone a message, schedule an appointment or ask a question. E-mail messages however can also be altered and/or forwarded. Sharing private information or opinions can lead to embarrassing circumstances. Once the "SEND" button is pressed, you can't take it back. If you want to have a discussion, go old fashioned; use a telephone.

FRAUDULENT MESSAGES & SOLICITATIONS

Almost any crime committed in society can be enhanced through the use of computers. One of the most common forms of cyber-crime is fraud. The internet has created a virtual "shopping centre" for fraud artists. Posting personal information on public sites such as social networking sites or blogs can result in identity theft. Most common are fraudulent e-mail messages from what appear to be a financial institutions with "urgent" notices. Never respond to these messages and never click on any links. If you think you have a problem with your bank, go to your branch and speak to a representative.

FOR MORE INFORMATION ON THIS SUBJECT, PLEASE CONTACT:

PEEL REGIONAL POLICE
Crime Prevention Services
7750 Hurontario Street
Brampton, Ontario
L6V 3W6

Tel. 905-453-2121 ext. 4021
Fax 905-456-6106

You may also want to examine our Internet site at:
www.peelpolice.ca

HOAX E-MAILS

Hoax e-mails usually contain an urgent message and may appear to originate from an enforcement or other legitimate agency, forwarded by a friend. i.e. "Warning from Police." Hoax e-mails are designed to raise alarm and induce the reader to warn, or forward, to as many friends as possible. In many cases, these e-mails contain viruses.

The rules to remember are:

- Don't open any e-mail from someone you are not familiar with.
- Don't forward any email from an originator you are not familiar with.
- Any e-mail that asks you to forward to "ten other" people, delete it. Don't forward.
- You can verify hoax e-mails at www.snopes.com or at www.scambusters.org.

PHISHING

"Phishing" is the term commonly used to refer to e-mails that appear to come from legitimate financial institutions, online retailers or a government agency regarding some type of security threat and is written with a sense of urgency.

The e-mails usually solicit confidential data such as credit/debit card information or social insurance numbers and are used for the purpose of perpetuating identity theft. Never respond to these messages and report them directly to the affected company or institution. For further information about frauds, see the Frauds fact sheet.

SPAM

"Spam" is the term used to commonly refer to unwanted or unsolicited e-mails. Unwanted e-mails typically result from having visited a website (an electronic record having being made of your computer's "signature") or leaving your personal e-mail behind.

Tips to manage spam:

- Purchase software that works like anti-virus software.
- Never open or reply to spam messages (this includes responding to the "click here to remove me from the list" messages, as this tells the person who sent it that their message is getting through).
- Limit use of your personal e-mail by setting up a generic e-mail address and using this instead.
- Activate privacy controls on your browser.
- Use IP blocking software when surfing the net.

NETWORKING

Most homes today have more than one computer in the house and operate on a wireless router system. A wireless router operates like radio waves. The first line of defence in a network is the router.

Here are some tips to help secure your access to the internet:

- To limit leakage, position the router in a central part of your home but not near windows.
- Activate router security features and change the default password. Without security features, unauthorized computers; i.e. neighbour, drive-by, can access your signal without your knowledge.
- Turn off the network while away for extended periods of time.

FIREWALLS

In order to protect yourself against people trying to "hack" their way into your computer, you should consider obtaining software commonly known as a firewall, particularly if you store sensitive information on your computer (such as bank account numbers) or use high speed internet access.

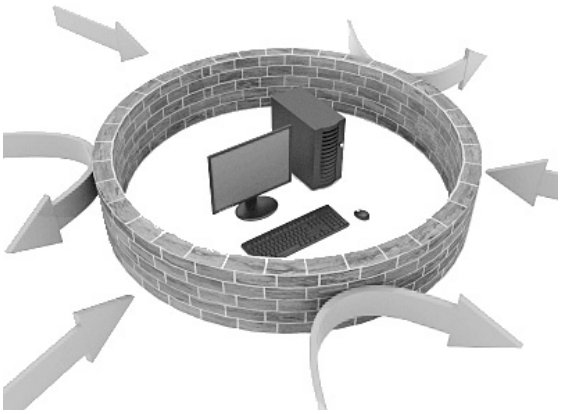
The primary purpose of the firewall is to act as a filter to discourage "hackers" from breaking into your computer.

Firewalls can also:

- Help to minimize "cookies" (tiny scraps of program code placed on your computer when you visit web sites),
- Block / alert you to spyware.
- Guard against viruses that use a direct attack.

Some firewalls can be downloaded for free, but they are not as effective as store bought filters. If you don't have firewall software, unplug your internet connection when not in use.

This will limit your exposure to the times that you are actually using the internet.



HACKING

Hacking is a term associated with someone who re-configures or re-programs a computer in a fashion not intended by the owner. Hackers are commonly employed by business to identify weaknesses in computer systems.

Malicious hackers are associated with illegal activities. Hacking may occur through on-line games or social networking sites. Malicious hacking may constitute a criminal offence.

To safeguard your computer:

- Harden your system by activating the system's, security controls.
- Keep your system updated with available patches.
- Use a firewall and anti-virus programs.

SPYWARE

Spyware is the main reason why your computer is slowing down. Spyware monitors what you do on line, keep stats, track habits and can even result in identity theft.

Signs of spyware can include:

- Barrage of pop-up ads.
- Hijacked browser.
- Sudden or repeated change in your computer's internet home page.
- New and unexpected toolbars and icons.
- Sluggish/slow performance.

Spyware can be eliminated by installing a firewall and an anti-spyware program from a reputable vendor.

Other tips for dealing with spyware include:

- Set your operating system and web browser software for automatic updates.
- Set your browser security setting no lower than medium.
- Download free software only from sites you know and trust.
- Never install any software without knowing exactly what it is.
- Don't click on any links within pop-up ads.
- Don't click on links in spam that claim to offer anti-spyware software.

VIRUSES

Viruses are a criminal act of mischief that can do considerable damage (steal personal information, steal stored information, impair the use of your computer, etc.). Viruses can include worms and Trojan horses.

To protect yourself against viruses, follow these Do's & Don'ts:

DO

- Install a firewall.
- Install current anti-virus software.
- Make sure the settings are set for automatic updates.
- Update your browser.

DON'T

- Open an e-mail from a source you do not recognize.
- Open any files attached to an email unless you know what it is, even if it appears to come from a friend or someone you know.
- Forward chain emails or junk email. Delete them.
- Execute unsolicited files, even if they appear legitimate; i.e. "Click here to update your Windows program."

DOWNLOADING

Downloading information and files from the internet is a common practice. Downloading free programs is unwise unless downloaded from reputable sites. Many free downloads can include viruses that can monitor your activity on the net, result in spam or other serious breach of your system

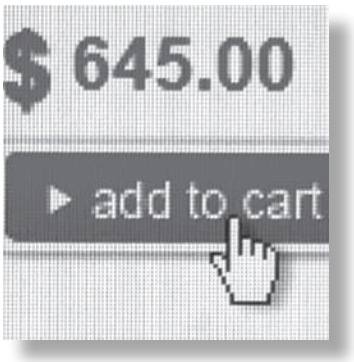
With the prevalent use of mp3's, iPods and similar devices, unauthorized music and movie downloads can present their own risks, such as personal liability. The internet offers many free download programs, including file sharing, or peer to peer (P2P). These programs can download copyrighted material. Such illegal downloads can result in both civil and criminal prosecution. When downloading from a P2P program you are simultaneously identifying yourself by exposing your computer's signature, or IP number, leading to your personal identity and location. Parents and caregivers are particularly vulnerable if their children should engage in illegal downloading unknown to the parent. Civil judgements can leave a family financially bankrupt. Music companies and other digital services offer legal downloading through membership fees or gift cards.

SHOPPING ON THE INTERNET

The internet has become a popular place to buy and sell goods.

Problems can develop as a result of:

- Fraudulent/bogus auction sites or the purchase of precious metals.
- International boundaries.
- Dealing with a site that is not "secure".
- Limited insurance on legitimate auction sites.



In order to protect yourself against fraud, follow these Do's & Don'ts:

DO

- Use a separate credit card to track your purchases.
- Make sure your browser is updated.
- If you have a concern, call the company.
- Keep copies of your transactions.
- Check your statement.
- Avoid impulse buying.

DON'T

- "Copy & paste" credit card numbers.
- Enter any personal information on any site to register or to purchase, unless the IP address in the URL (universal resource locator) begins with https:// and the lock beside the URL (or bottom right hand corner of your start bar) is closed.

LAST RESORT

If a serious breach of your computer has been inflicted, such as passwords or identity stolen, or infected with a severe virus, you will want to consider reformatting your computer. You can do this yourself or use professional services.

Before doing so, remember to copy all relevant or important files that you want to keep; reformatting will erase all files and programs.

NOTES