

Viruses

Viruses are software programs that mostly come as attachments to spam email. Once the attachment is opened from your system, it unleashes its havoc -from erasing your hard drive to rendering it uselessly slow. Trojan Horses are email attachments that look innocent, but carry viruses hidden inside. They should be treated just like viruses.

How can I get more information about securing my computer?

Here are a list of sites that provide more detailed information about securing your home computer from outside threats.

http://www.cert.org/tech_tips/home_networks.html

<http://www.staysafeonline.org/>

http://www.cheycobb.com/home_security.html

<http://iserloh.com/oped/safecomputing>

<http://security.uwo.ca/homecomputer.html>

<http://www.markusjansson.net/eselecting.html>



LABRADOR
DISTRICT SCHOOL BOARD

Protecting Your Computer



LABRADOR SCHOOL BOARD
www.lsb.ca

What threats do I have to protect against?

As more and more consumers took advantage of rock-bottom prices for new desktop systems and as the number of household using broadband access (vs. dial-up) vastly increased, it has simultaneously opened the door to much mischief by unscrupulous hackers. Here is a list of the most common threats to your computer.

Hackers

Hackers are computer experts that try to break into your computer system to obtain confidential information or anything else of value. Hacking attempts have become easier, as many consumers have a constantly on connection to the internet, such as cable or DSL-modem.

Phishing

Phishing is luring of sensitive information, such as password and other personal information, from a victim by masquerading as someone trustworthy with a real need for such information. Phishers usually work by sending out spam e-mail to large numbers of potential victims. These direct the recipient to a web page which appears to belong to their online bank, for instance, but in fact captures their account information for the phisher's use.

Pharming

Pharming is a form of phishing, when the thieves hijack a legitimate web address, and redirect you to a phony website that looks very much like the original. This is also termed "spoofing". It's another way to steal personal information.

Worms

Worms are programs (or groups of programs) that "burrow" into your computer and can spread copies of themselves from your computer to others via email attachments, network connections, file-sharing, or by working as a partner with other forms of malware. Worms can steal licenses of your software, including installed games. Some can prevent you from securely accessing websites.

Spammers

Spammers send out millions of unsolicited email offers in attempt to get a unsuspecting few to send them money for services or products.

Spyware or adware

This is software that was inadvertently installed on your computer while you installed other software. The spyware logs all your keystrokes and sends the information back to the phisher.

How can I protect my computer from these threats?

Here is a short list of things to do to protect against the threats listed on the previous page. While this is not a complete or comprehensive list it can be used as a guideline for securing your computer.

Back up your data

Back up your data to removable media. Copy your data so that everything you care about is stored in at least two places.

Understand that Electronic mail can be forged and snooped easily.

Do not assume that a message was sent by the person named in the From field. Your electronic mail travels across the Internet unprotected, strangers can read and change it, so do not send personal details, valuable passwords, or credit card numbers in regular email.

Don't run or install programs from strangers.

You may think this is obvious, but many people don't understand that clicking on an email attachment often runs something.

Use a firewall

Use a firewall if you have a cable or DSL line.

Even if you have only one computer, a firewall helps isolate your machine from the bad guys on the outside, kind of like a surge protector.

Install a virus checker and keep its definitions up-to-date.

- AVG: <http://www.grisoft.com> (free for home use)
- Panda: <http://www.pandasecurity.com/canada-eng>
- Avast: <http://avast.com> (free for home use)
- TrendMicro: <http://us.trendmicro.com/us/home>

Install Spyware/Adware and keep its definitions up-to-date.

- Spybot: : <http://www.safer-networking.org/en/index.html> (free)
- Ad-Aware: : <http://www.lavasoftusa.com/software/adaware> (free)
- Hijack This: <http://us.trendmicro.com/us/home/home-user>
- Spyware Doctor: <http://www.pctools.com> (free)

Install security patches

Install security patches from your software providers regularly. This is important, because many machines get infected by virus that exploit holes for which patches have been available for months.

*****Note: Update Spyware and Virus checker weekly and ensure they are not expired.**