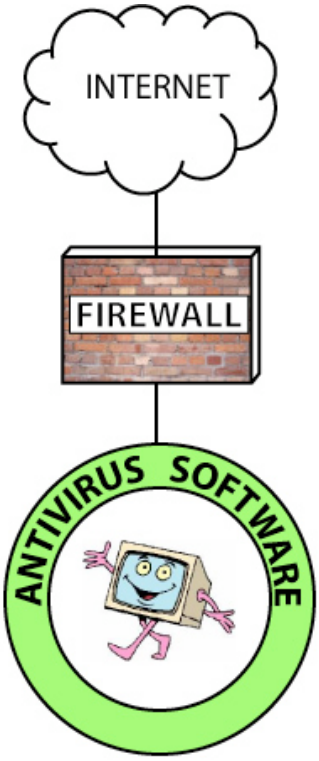
emily carr
university of art + design

1399 Johnston Street, Vancouver, BC, Canada V6H 3R9

SECURING YOUR COMPUTER AGAINST HACKERS AND VIRUSES

This purpose of this info sheet is to provide you with a brief introduction to the topic of computer security and to offer some basic security tips to help make your PC more secure against hackers and viruses. For additional information on securing your computer, see the ITS info sheet "*Securing your computer against Spyware / Adware / Malware*" which is available from the ITS website.

"I already have enough to worry about !!!"



For many people, learning how to use all the features of your computer and various computer software programs is a task difficult enough. Having also to deal with the computer security risks from invisible hackers, malicious viruses and Internet "worms" seems too complex to even begin to comprehend.

In the not too distant past, many computer software and hardware manufacturers largely ignored the issue of computer security. The widespread, costly and damaging effects that computer viruses, hackers and "worms" have had on computers worldwide have led them to take the issue more seriously. There are now a wealth of products on the market dedicated to computer security and some modern operating systems now come with built-in support for dealing with some of these threats so you don't have to worry about them as much.

Note: Users of Microsoft Windows systems are more often plagued with these issues than other operating systems. One site which is highly recommended for Microsoft Windows users is the "*Securing Your PC*" site. This site provides excellent information and automated tools to help configure your Windows PC with optimal security settings: http://www.microsoft.com/athome/security/protect/default.aspx

"So what can I do ?"

There are three things you can do to help protect your PC:

1) **Install a firewall**

2) **Install antivirus software**

3) **Keep your operating system software and antivirus software up to date**

What is a Firewall ?

Connecting to the Internet without a firewall is like leaving the keys in your car with the engine running and the doors unlocked while you run into the store. Although you may be able to get in and out before anyone notices, someone may take advantage of the opportunity. On the Internet, hackers use malicious code, such as viruses, worms, and Trojan Horses, to try to find those unlocked doors—an unprotected computer. A firewall can help protect your computer against these and other security attacks.

A firewall works by examining information coming from and going to the Internet. It identifies and ignores information that comes from a dangerous location or seems suspicious. If you set up your firewall properly, hackers searching for vulnerable computers can't detect your computer.

There are three basic types of firewalls available today. The first step in choosing a firewall is to determine which one is best for you. Your options include:

1. **Software firewalls**
   Software firewalls are usually a good choice if you only have one computer hooked up to the Internet. There are many software firewalls available today. Most anti-virus or “Internet Security” software packages include both antivirus and firewall software as the two usually go hand in hand. You may find that your operating system already includes a built-in software firewall. Mac OS X has a software firewall built-in which is turned on by default. Windows XP includes a very simple software firewall which by default is turned off (though this default will be changed to *on* with the release of Service Pack 2 in fall 2004). Please consult your operating system help function for information on configuring these built-in network firewalls. You may also want to visit the Apple and Microsoft security pages which provide more detailed information on securing your PC (links available at the end of this document).

2. **Hardware routers**
   Hardware routers are a good choice for home networks (more than one linked computer or network device) that will be connected to the Internet.

3. **Wireless routers**
   If you have or are planning to use a wireless network, you will need a wireless router. Only a few wireless routers come equipped with a built-in firewall, so you may need to purchase a firewall separately.

Different firewall manufacturers offer different features with their firewalls. It is always a good idea to do some research of your own and read some software reviews to find out as much as you can about the available options and what will work best for you.

What is Antivirus Software ?

Antivirus software helps protect your computer against viruses. Many computers come with antivirus software installed. You can also purchase antivirus software and install it yourself. Many antivirus software packages also come with additional software like software firewalls to help secure your computer.

Just having an antivirus program installed is not enough, however. You also need to keep your antivirus software up-to-date. Most programs have an "automatic update" feature which you should ensure is enabled. Not keeping your software up-to-date leaves your computer vulnerable to new types of viruses. If you already have antivirus software installed, consult the help manual to find out how to ensure it is kept up-to-date.

Keeping things up-to-date

Keeping your operating system up-to-date

The software which operates your computer is one of the most complex systems invented by humanity. Many operating systems contain over 30 million lines of computer code. For a computer to work flawlessly, every one of these lines of code must work correctly. Even when the computer code is working as designed, problems may still occur through faults in the design itself or through the unforeseen side effects with other software on the system. Ensuring that you have the latest updates for your operating system helps to keep potential problems minimized. Most operating systems offer a way to automatically update your system with the latest security patches. Visit these sites to find out how you can keep your system up to date:

- **Microsoft Security**
  http://www.microsoft.com/athome/security/protect/default.aspx

- **Apple Security**
  http://www.apple.com/support/security/

Keeping your antivirus software up-to-date

Ensuring that you have the latest virus definitions for your antivirus software is *one of the most important things you can do to help keep your computer secure*. New viruses are appearing constantly and if your antivirus software is not up-to-date, your computer is vulnerable. Consult the help manual for your antivirus software to find out how to ensure it is up-to-date.

Resources

- **Microsoft Security : Protecting your PC**
  This is an excellent site for Microsoft Windows users for helping them to protect their computers.
  http://www.microsoft.com/athome/security/protect/default.aspx

- **Apple Security pages**
  http://www.apple.com/support/security/

Definitions

- **Hacker**
  Individuals so computer literate they are able to 'hack' into computers (i.e. access and/or manipulate data held in them) usually employing a cunning ability to bypass or override password protection and other security strategies. Hackers often work at a distance physically from their target computers by abusing the facilities of the Internet.

- **Trojan Horse**
  A Trojan (also called a Trojan horse) is a software program in which harmful or malicious code is contained within another (seemingly harmless) program. When this program executes, the Trojan performs a specific set of actions, usually working toward the goal of allowing itself to persist on the target system. Trojans can allow hackers to open backdoors on your system, giving them access to your files and even network connectivity.

- **Virus**
  A piece of programming code inserted into other programming to cause some unexpected and usually undesirable event, such as lost or damaged files. Viruses can be transmitted by downloading programming from other sites or be present on a diskette. The source of the file you're downloading or of a diskette you've received is often unaware of the virus. The virus lies dormant until circumstances cause its code to be executed by the computer.

- **Worm**
  A computer program, which replicates itself and is self-propagating. Worms, as opposed to viruses, are

meant to spawn in network environments. Worms usually are designed to slow down a network or even crash it.

Disclaimer

Emily Carr University assumes no liability for personal or workplace computing equipment used during your course of study. We are not liable for damages caused by or thought to have been caused by the installation of software purchased from us, provided by us or obtained through links posted on our website. We are not accountable for issues you may have surrounding the installation and/or use of said software.