

# Computer Security

When you connect your computer to the Internet, you open up a world of information, but you also open up a world of potential dangers---viruses, spam, computer attacks and more.

There are ways to protect your computer and yourself from these dangers. All you need are a few software utilities and a lot of **common sense!**

## Viruses

A computer virus is a malicious software program designed to do damage to your computer system by deleting files or even taking over your PC to launch attacks on other systems.

### Signs of infection

How do you know whether your computer system has been infected with a virus? In general, whenever your computer starts acting different from normal, it's possible that you have a virus. Here's a short list of possibilities:

- Your computer runs more slowly than normal
- Your computer stops responding or locks up often
- Your computer crashes and restarts every few minutes
- Your computer restarts on its own and then fails to run normally
- Applications on your computer don't work correctly
- Disks or disk drives are inaccessible
- You can't print correctly
- You see unusual error messages
- You see distorted menus and dialog boxes.

## **How to Catch a Virus**

Whenever you share data with another computer you risk exposing your computer to potential viruses.

- Opening an infected file attached to an email message
- Launching an infected program file downloaded from the Internet
- Sharing a floppy disk that contains an infected file
- Sharing a computer file over a network that contains an infect file.

The most common means of virus infection is via email. Don't open an attachment from people you don't know and don't open a file from people you do know unless you were expecting it. That's because some viruses can hijack the address book on an infected PC, thus sending out infected email that the owner isn't even aware of.

## **Common Sense**

- Don't open an attachment from an unknown or unexpected email.
- Don't click links sent to you from strangers via email, instant messaging or in a chat room.
- Download files only from reliable websites.
- Share disks and files only with users you know and trust.
- Use antivirus software.

## **Antivirus Software**

Antivirus Software is a program capable of detecting known viruses and protecting your system against new, unknown viruses. These programs check your system for viruses each time your system is booted.

You must update your virus program weekly. An outdated antivirus program won't be capable of recognizing and protecting against the very latest computer viruses.

## **Spyware and Adware**

Spyware and adware are similar to viruses in that they are undesirable programs that may sneak onto your computer. Unlike a virus, however, spyware and adware aren't designed just to do damage to computers. Spyware is used to collect information such as account numbers, passwords, or even simply browsing history. Adware is used to show ads on your computer. In effect, it opens popup windows even when you're not on the Internet.

Programs exist to find and block spyware and adware just like viruses.

## **Spam**

Spam is the online equivalent of the junk mail you receive in your postal mailbox. The first way to reduce the amount of spam you receive is to limit the public use of your email address. Another way is to have two email addresses. Use the one your ISP provides as the important one; give that address to family and close friends, and have another email address from a free provider to use more widely. Most email programs will try to filter spam to a separate folder.

## **Firewall**

Connecting to the Internet is a two-way street—not only can your PC access other computers online, but other computers can also access your PC. You protect your system against outside attack by blocking the path of attack with a firewall. A firewall is a software program that forms a virtual barrier between your computer and the Internet. The firewall selectively filters the data that is passed between both ends of the connection and protects your system against outside attack. If you are running Windows XP you already have a firewall program installed on your system.

## Security on the Internet

Generally, information sent between computers on the Internet is not secure. It can be intercepted and read by third parties. Some sites, however, encrypt information coming from their site to protect their users. In Internet Explorer there are two clear ways to know if you're on a secure site.



The address for a secure address will always start with “https” instead of “http” (the “s” stands for “secured”). Also, whenever Internet Explorer opens a secure site it pops up an icon of a small padlock.

If you're on a secure site you can feel safe to give personal information such as credit card numbers. If you're not on a secure site you should not give such information. Any reputable online business will provide a secure site. If they do not, take your business elsewhere.

## Email

Generally speaking, email is not secure. Messages can be intercepted and information can be stolen. Never send personal information such as account or credit card numbers over email.