

---

## Privacy Issues



We use computers for everything from banking and investing to shopping and communicating with others through email or chat programs. Although you may not consider your communications "top secret," you probably do not want strangers reading your email, using your computer to attack other systems, sending forged email from your computer, or examining personal information

stored on your computer, such as financial statements. Generally, when people use the Internet, their activities and their personal information are not private anymore. Most of these online activities are habitual processes you do without even thinking twice. For example, whenever you fill out a magazine subscription, complete a product registration card, apply for a bank account or a credit card, rent or purchase a property, make a purchase by using a credit card at a grocery store, data about your personal information and your lifestyle/shopping habits is collected.

On the Internet, all of these activities can be saved to a database and then can be sold later to various national marketing organizations against your wish. For example, your credit history is stored as an electronic record and many companies check against it before opening a new account for you. Or worse, a doctor can check your record to find out if you have ever filed a malpractice suit before they accept you as a new patient. So your data is subject to be legally sold for marketing purposes, stolen through internet piracy, or hacked from the databases of legitimate marketers or service providers.

## **Why is computer security important?**

Computer security is the process of preventing and detecting unauthorized use of your computer. Prevention measures help you to stop unauthorized users (also known as "intruders") from accessing any part of your computer system. Detection helps you to determine whether or not someone attempted to break into your system, if they were successful, and what they may have done. The following information will assist you in understanding computer security threats and the measures you can take to ensure that your PC is protected.

## **Types of Security Threats**

Intruders, also referred to as hackers, attackers, or crackers, can exploit any weaknesses in your system to plant malware (malicious software designed to infiltrate or damage a computer system, without the owner's informed consent) that can use your PC as a gateway to attack other PC's or networks or allow the intruders to steal your personal identification information (identity theft).

## **Types of Malware**

**Viruses** - A virus is a small piece of software that attaches itself to real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.

**E-mail viruses** - e-mail virus moves around in e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book.

**Worms** - A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copies itself to the new machine using the security hole, and then starts replicating from there, as well.

**Trojan horses** - A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Though they have no way to replicate automatically, Trojan horse programs are a common way for intruders to trick you into installing "back door" programs. These can allow intruders easy access to your computer without your knowledge, change your system configurations, or infect your computer with a computer virus.

**Spyware & Adware (Parasites)** – Other types of strictly for-profit malware that have emerged in which programs are designed to monitor users' Web browsing, display unsolicited advertisements, and redirect affiliate marketing<sup>1</sup> revenues to the spyware creator. These programs don't spread like viruses; usually they are installed by exploiting browser security holes, or are installed like a Trojan horse when the user installs other software.

Though difficult to draw a clear distinction, Spyware and Adware are not the same type of programs. **Spyware** generally refers to a class of unsolicited programs that invade a system, monitor computing behavior, and report their findings to a third party. **Adware**, on the other hand, generally refers to any program that features built-in advertisements for third-party products and services; it's these ads that generate income for the software developer, allowing it to distribute its wares without charging a licensing fee.

### **How do Spyware and Adware affect us?**

- All information you enter via the web can be intercepted
- Unauthorized sites can add themselves to your desktop (icons) and your computer will experience unwanted pop-up windows
- Unauthorized sites can add themselves to your internet favorites
- Your browsing activity can be tracked and monitored

---

<sup>1</sup> **Affiliate Marketing** is a popular method of promoting web businesses in which an affiliate is rewarded for every visitor, subscriber and/or customer provided through his efforts. It is a modern variation of the practice of paying finder's-fees for the introduction of new clients to a business. Compensation may be made based on a certain value for each visit (Pay per click), registrant (Pay per lead), or a commission for each customer or sale (Pay per Sale), or any combination.

- Unwanted toolbars and search bars can attach themselves to your browser without your knowledge or approval
- Your personal information can be sold to other parties without your knowledge or consent<sup>1</sup>
- Your default homepage and settings can be hijacked so you can't change them
- They can also slow down the processing speed of your computer, take over system and memory resources, and clog network connections
- These programs also threaten PC security by secretly deactivating firewalls, antivirus utilities, and other protective measures

### **What other damage can viruses do?**

**DoS Attacks (Denial of Service)** - Having control of your computer gives intruders the ability to hide their true location as they launch attacks, often against high-profile computer systems such as government or financial systems, in which a user or organization is deprived of the services of a resource they would normally expect to have. Typically, the loss of service is the inability of a particular network service, such as e-mail, to be available or the temporary loss of all network connectivity and services. In the worst cases, for example, a Web site accessed by millions of people can occasionally be forced to temporarily cease operation. It is important to note that in addition to being the target of a DoS attack, it is possible for your computer to be used as a participant in a denial-of-service attack on another system.

**Spamming** - Spamming is when a sender sends out hundreds, thousands, or even tens of thousands of email messages to recipients across a wide geographic area. Spammers can obtain email addresses of their recipients by purchasing from legitimate sources or by hacking. Others simply use computer programs that generate addresses randomly based on the domain names of known Internet Service Providers. Regardless of how they obtain your email addresses you have unsolicited emails in your mailbox which require your energy to review or remove those unwanted messages. Or worse,

your computer can be flooded with viruses upon opening those spammed emails. While the most widely recognized form of spam is e-mail spam, the term is applied to similar abuses in other media: instant messaging spam, Usenet newsgroup spam, Web search engine spam, spam in blogs, and mobile phone messaging spam.

**Spoofing** - Email spoofing is when you receive an email message that appears to be from someone other than the actual sender. This method enables the junk e-mailer to hide his or her identity from the recipient. In spoofing, the sender places a false return address on the junk message. When spoofed, the recipient has no idea who sent the message and has no way of responding or stopping the problem. Phishing is an example of spoofing.

**Phishing** - A method of online identity theft. In addition to stealing personal and financial data, "phishers" can infect computers with viruses and convince people to participate unwittingly in money laundering. Most people associate phishing with e-mail messages that spoof banks, credit card companies or other business like Amazon and eBay. These messages look authentic and attempt to get victims to reveal their personal information. But e-mail messages are only one small piece of a phishing scam. The process of phishing involves:

1. **Planning.** Phishers decide which business to target and determine how to get e-mail addresses for the customers of that business. They often use the same mass-mailing and address collection techniques as spammers.
2. **Setup.** Once they know which business to spoof and who their victims are, phishers create methods for delivering the message and collecting the data. Most often, this involves e-mail address and a web page.
3. **Attack.** This is the step people are most familiar with -- the phisher sends a phony message that appears to be from a reputable source.
4. **Collection.** Phishers record the information victims enter into web pages or popup windows.
5. **Identity Theft and Fraud.** The phishers use the information they've gathered to make illegal purchases or otherwise commit fraud. As many as a fourth of the victims never fully recover.

**ActiveX Controls** - These controls link to any object--traditionally dynamic content such as tables and buttons that react to mouse clicks--embedded within a Web page. Although they help Web pages spring to life, malicious programmers can easily download spyware through ActiveX. Install a sturdy browser and firewall that screens your ActiveX Controls, and download them with care, accepting ActiveX only from trusted Web sites.

### **Is My PC Infected?**

After you open and run an infected program or attachment on your computer, you might not realize that you've introduced a virus until you notice something isn't quite right.

Here are a few primary indicators that your computer might be infected:

- Your computer runs more slowly than normal
- Your computer stops responding or locks up often
- Your computer crashes and restarts every few minutes
- Application on your computer don't work correctly
- Disk or disk drives are inaccessible
- You can't print correctly
- You see unusual error messages
- You see distorted menus and dialog boxes
- File size changes for no apparent reason
- Date of last access does not match date of last use
- An increase in the number of files on the system when nothing has been added
- Un-commanded disk drive activity
- System slows down, freezes or crashes
- Increase or decrease memory size
- Randomly change file or memory size
- Extended boot times
- Increase disk access times
- Cause computer to make strange noises, make music, clicking noises or beeps
- Display pictures

These are common signs of infection—but they might also indicate hardware or software problems that have nothing to do with a virus. **Tip:** Beware of messages warning you that you sent e-mail that contained a virus. This can indicate that the virus has listed your e-mail address as the sender of tainted e-mail. This does not necessarily mean you have a virus. Some viruses have the ability to forge e-mail addresses.

## Protecting Your PC - How can I avoid contracting or spreading viruses?

There are three basic components that you need to build a virtual shield against becoming a victim to hackers and crooks on Cyber space.

1. Firewall (Windows XP and Internet Explorer 6.0)
2. Anti-Virus Software (Norton as well as free versions such as ZoneAlarm)  
make sure you perform updates!
3. Anti-Spyware & Anti-Adware Programs

### 1. Firewall:

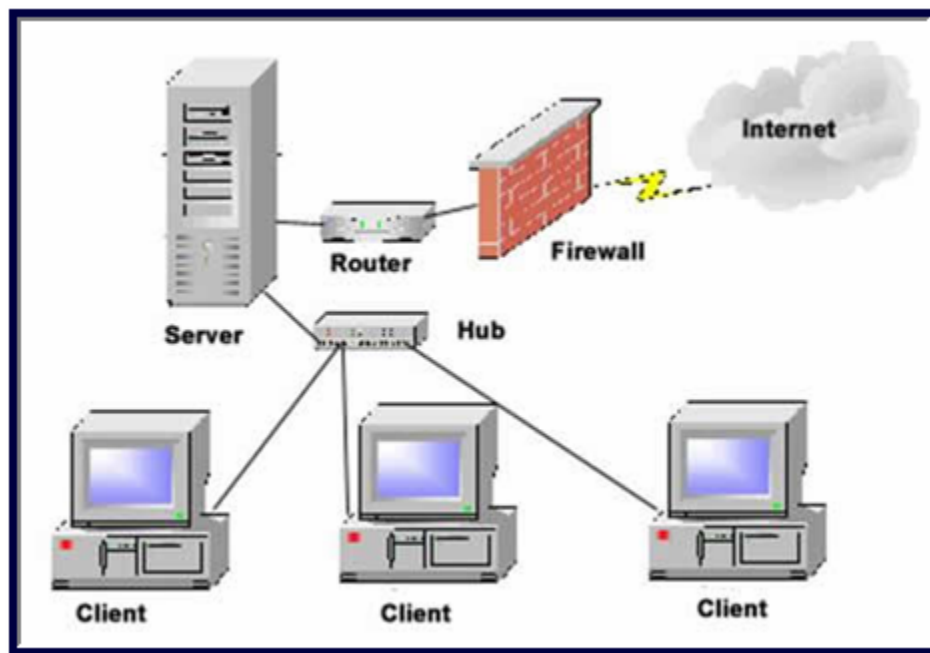


Image: [www.networkdictionary.com](http://www.networkdictionary.com)

Firewalls block unauthorized entry into a network or into your computer that is connected to the Internet. If a request or data does not pass the firewall's security inspection, it is stopped from traveling any further. A firewall can be hardware-based, software-based, or both. A firewall inspects the requests and data that pass between the private network and the Internet. On business and organization networks, it allows outsiders to access public areas but prevent them from exploring private areas of the network. Your modem or router likely includes a built-in firewall, but you have to make sure that it's turned on and up-to-date. If you have Microsoft XP Operating System, it comes with Windows

Firewall but many industry security experts says it falls short of the standard of protection expected of commercial firewalls. Experts claim that it does not block outbound traffic, and it can be switched off by another application, possibly even by a clever worm. Also, some software applications have default settings that allow other users to access your computer unless you change the settings to be more secure. Examples include chat programs that let outsiders execute commands on your computer or web browsers that could allow someone to place harmful programs on your computer that run when you click on them. For more information on bundled packages including firewall and anti-virus softwares, check out at PCWorld.com's review on Security Suites at <http://www.pcworld.com/reviews/article/0,aid,125857,00.asp>.

2. **Anti-Virus Software:** Why do you need one? It defends against virus or bugs that can slow your computer down making it difficult to open applications or even crashes your hard drive – deleting everything you've stored there. Most new computers have anti-virus software preinstalled, but it's up to you to renew the service or buy another program before the trial period ends. You can set your program to update automatically, and check the "status page" to make sure you have the latest version running. Norton Anti-Virus and McAfee Anti-Virus Softwares are two reputable programs. Check out PCWorld.com's reviews on top anti-virus softwares at <http://www.pcworld.com/reviews/article/0,aid,124475,00.asp>.
3. **Anti-Spyware & Anti-Adware Programs:** Spyware and Adware usually reach the computer via downloaded programs especially via file sharing or file swapping programs. Both can result in data corruption, personal profiling, hacker attacks, pop-up ads, spying, and identity theft. Spywares/Adwares track your online activities and capture everything you type, including passwords without your knowledge and transmit the data to a predefined address. Anti-Spyware/Adware programs protect you from those uninviting activities. These programs can be purchased separately or bundled with anti-virus software and a firewall. Some of the most popular titles include Lavasoft's AD-Adware SE Personal (free; [www.lavasoft.com](http://www.lavasoft.com)), CA's eTrust Pest-Patrol Anti-Spyware (\$29.99; [www.ca.com](http://www.ca.com)), and Spybot Search and Destroy, a.k.a. Spybot-S&D (or

just plain Spybot). Spybot is one of the most capable anti-spyware packages available free at [www.safer-networking.org](http://www.safer-networking.org).

The majority of new anti-virus programs (programs or computers purchased after the year 2000) enable users to update their anti-virus program through the software. Open the Virus program and look for "Update", "Check for updates", "Live Update", or something similar. Below are some examples of how a user may update their anti-virus program.

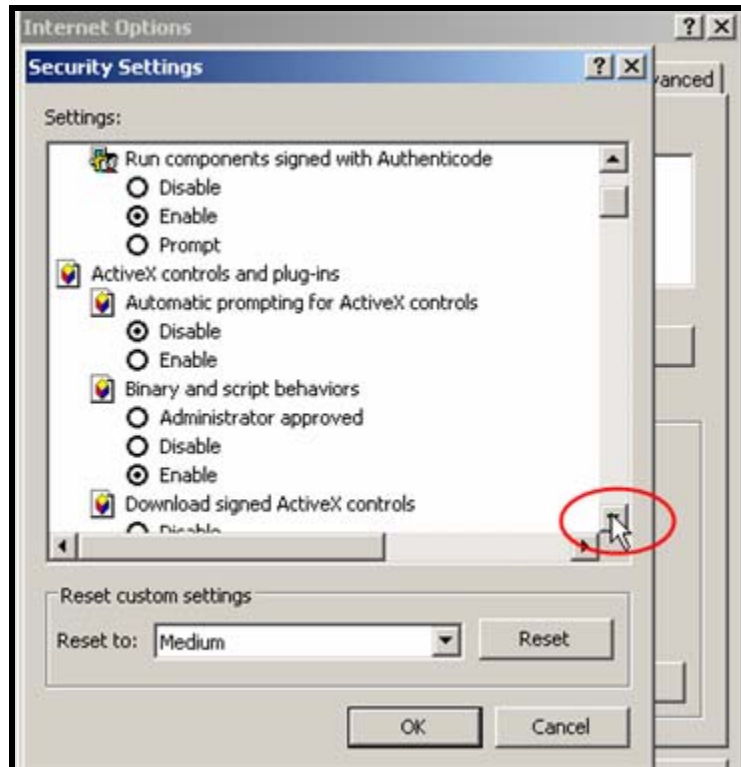
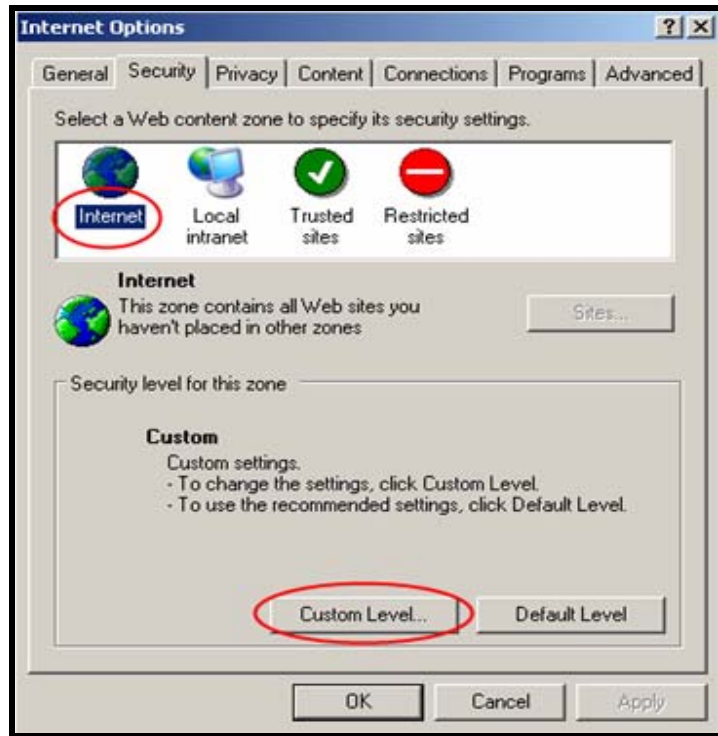
- Microsoft Windows users running recent versions of McAfee can double-click on the Vshield icon in their Taskbar Status area on the lower right-hand of their browser and click "Check for VirusScan update" to check for available updates.
- Microsoft Windows users running recent versions of Norton can double-click on the Norton icon in their Taskbar Status area and click the "Live Update" to check for available updates.

#### **Additional precautions to take**

1. You can run the **(Microsoft Malicious Software Removal Tool** at [www.microsoft.com/downloads](http://www.microsoft.com/downloads)) and install industry-standard, up-to-date antivirus software on your computer. There is no way to be certain if your computer is infected with a virus or not. If you don't have current antivirus software installed or if you're interested in installing a different brand, visit PC's world.com recommendation at <http://www.pcworld.com/reviews/article/0,aid,124475,00.asp>.
2. **Set your security settings.** Spyware or adware infection could have modified your computer security settings. Restore your settings by opening Internet Explorer, accessing the Tools menu, and selecting Internet Options. On the Security tab of the resulting dialog box, select the Internet content zone icon and position the security level setting to Medium or High. Next, click the Privacy tab and set the privacy level setting to Medium or higher. Clicking OK will close the dialog box to activate your new security and privacy settings.
3. **Keep all applications, including your operating system, patched.** For Microsoft Windows XP check at [www.microsoft.com/downloads](http://www.microsoft.com/downloads). Vendors will usually release patches for their software when vulnerability has been

discovered. Most product documentation offers a method to get updates and patches. You should be able to obtain updates from the vendor's web site. Read the manuals or browse the vendor's web site for more information. Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look on your vendor's web site for information about automatic notification. If no mailing list or other automated notification mechanism is offered you may need to check periodically for updates. Unfortunately, intruders are always discovering new vulnerabilities (informally called "holes") to exploit in computer software. The complexity of software makes it increasingly difficult to thoroughly test the security of computer systems.

4. **Don't run programs of unknown origin.** Never run a program unless you know it to be authored by a person or company that you trust. Also, don't send programs of unknown origin to your friends or coworkers simply because they are amusing -- they might contain a Trojan horse program. These programs seriously hurt Internet Security.
5. **Turn off your computer or disconnect from the network when not in use.** Turn off your computer or disconnect its Ethernet interface when you are not using it. An intruder cannot attack your computer if it is powered off or otherwise completely disconnected from the network.
6. **Disable Java, JavaScript, and ActiveX if possible.** Be aware of the risks involved in the use of "mobile code" such as ActiveX, Java, and JavaScript. A malicious web developer may attach a script to something sent to a web site, such as a URL, an element in a form, or a database inquiry. Later, when the web site responds to you, the malicious script is transferred to your browser. The most significant impact of this vulnerability can be avoided by disabling all scripting languages. Turning off these options will keep you from being vulnerable to malicious scripts. However, it will limit the interaction you can have with some web sites. Many legitimate sites use scripts running within the browser to add useful features. Disabling scripting may degrade the functionality of these sites. To limit scripting, open your Internet Explorer browser, select Tools, and Internet Options. In the Internet Options dialog box, click on the Security tab. Select Internet for your Web content zone and click on Custom Level for that zone.



In the Security Settings dialog box, scroll down to see your options and make a decision on how much security level that you want to customized for your

Internet option. If you do not understand the choice, place your mouse on an option and right-click to see the description of a particular option.


7. **Disable scripting features in email programs.** Because many email programs use the same code as web browsers to display HTML, vulnerabilities that affect ActiveX, Java, and JavaScript are often applicable to email as well as web pages. Therefore, in addition to disabling scripting features in web browsers, we recommend that users also disable these features in their email programs. It is important to Internet security. If you use Yahoo email, for example, go to Options and set your Spam Protection and General Preference to block images and HTML graphics.
8. **Make regular backups of critical data.** Keep a copy of important files on removable media such as ZIP disks or recordable CD-ROM disks (CD-R or CD-RW disks). Use software backup tools if available, and store the backup disks somewhere away from the computer. Go to [www.Smartcomputing.com](http://www.Smartcomputing.com) and click on Tech Support Center. Click the Backups & Data Recovery link and learn how to back up data on your system.
9. **Make a boot disk in case your computer is damaged or compromised.** To aid in recovering from a security breach or hard disk failure, create a boot disk on a floppy disk which will help when recovering a computer after such an event has occurred (if you do not have a floppy drive you can purchase an external unit for about \$40 from a computer retailer). A boot disk is a diskette from which you can boot your computer. Normally, your computer boots from a hard disk, but if the hard disk is damaged (for example, by a virus), you can boot the computer from a bootable diskette. For this reason, it's a good idea to make sure you always have a bootable diskette on hand. Remember, however, you must create this disk before you have a security event. Go to [www.smartcomputing.com](http://www.smartcomputing.com) and click on Tech Support Center. Click the Backups & Data Recovery link and select Create Emergency Boot Disks and follow instructions.

10. **Don't open unknown email attachments.** Before opening any email attachments, be sure you know the source of the attachment. It is not enough that the mail originated from an address you recognize. Malicious code might be distributed in amusing or enticing programs. If you must open an attachment before you can verify the source, do the following procedure:

- a. save the file to your hard disk
- b. scan the file using your antivirus software
- c. open the file

For additional protection, you can disconnect or lock your computer's network connection before opening the file. Following these steps will reduce, but not wholly eliminate, the chance that any malicious code contained in the attachment might spread from your computer to others.

11. **Phonies:** One of the most common hacker tricks is to forge links that promise to take you to one place (like eBay or your bank website or an interesting video) but really connect to "spoof websites" that steal your passwords or install spyware on your computer. Never click on a link in an unsolicited e-mail, even if it seems to be from your bank or another familiar source. How do you know whether you are entering a secure e-commerce website? How can you make sure that your online purchase is safe?

- a. **Check the URL.** If the page's URL begins with https://, then the page is secure. The letter S indicates security measures. It means that the website uses Secure Sockets Layer (SSL) technology, which encrypts data by converting into a code that is unusable by anyone who does not possesses a key to the code.
- b. **Check your browser's status bar.** If you use Microsoft Internet Explorer or Netscape Navigator, a small padlock symbol  will appear in the browser's status bar when a secure web page is open.

12. **Baits:** Do not take any free offers lightly. Think twice before responding to unsolicited offers such as free screensavers, free downloads such as pirated software and pornographic images, icons or even virus and spyware protection. Along with the promised goodies, you may also get "Adware" or "Spyware" that

monitors your online activities and floods your screen with pop-ups. If someone invites you to share the fortune of a Nigerian prince or redeem winnings from a contest you've never entered, don't do it! Finally, beware of messages urging you to "update" or "validate" your account information online. No legitimate company will ever request your account number and password via e-mail. When in doubt, call the company involved on the phone.

13. **Kids and the Internet:** Kids are most likely to be vulnerable to respond to chain mail requests, visit high-risk Web sites and use file-sharing programs. Consider parental filtering software to control access, and put computers in a common area where you can monitor your kids' online activities. Check out this website to see reviews on parental filtering softwares.

<http://familyinternet.about.com/cs/productreviews/tp/filteringsoft.htm>.

14. **Uninstall unwanted programs from Windows XP.** Follow the following steps to full uninstall unwanted spyware and adware programs. Click on Start menu and All Programs. Click on Control Panel and select Add or Remove Programs. From the resulting list, selecting a particular program tells you how much you use that program and the last date of the usage. If you wish to remove, click on change/remove button to uninstall.

## Virus Myths

Below are common misconceptions when it comes to computer viruses and other malware:

- 1) **"If I download a file onto a disk, I don't have to worry about viruses."** - This is not true, just because you've placed a file on a diskette or moved a file from a diskette to your hard drive does not mean that your computer cannot be infected. Many viruses are memory resident and capable of loading themselves into memory once a diskette is placed in the computer.
- 2) **"If I buy sealed software I don't have to worry about viruses."** or "If I just buy registered software I don't have to worry about viruses." - This is not always true. Just because the program may be surrounded in plastic doesn't mean that it cannot be infected with a virus. When a software program is saved onto a diskette or disk if that computer or program is infected the virus will attach itself. Although this issue very rarely occurs it is still a possibility.
- 3) **"If I don't download anything off of the Internet I don't have to worry about viruses."** - This is definitely not true. Although most companies and web sites will scan the files for viruses before they make them available to download some may not. In addition many people create a site or a file to download with the intention of spreading a virus, spyware, Trojan horses, or other malware.
- 4) **"If I just read my e-mail, I will not have to worry about viruses."** - Not true; there are viruses out there that are distributed through e-mail; also, files can be attached with e-mail and if executed can infect the computer. Today this is one of the most common ways computer viruses spread around the world.
- 5) **"If I don't get on the Internet I don't have to worry about viruses."** - This, unfortunately, is not the case. Although many viruses are spread over the Internet today it is still possible to contract a computer virus from any diskette or disk you put in the computer.
- 6) **"You can contract viruses from just looking at web pages."** - Not true. However, you can contract a virus if you download and execute a file from that web page. In addition spyware and other scripts can be executed from just viewing a web page. Although these programs are not designed to delete files on your computer they should be considered a privacy violation.

## Anti-Virus Software Producers

These websites also include lists of viruses, hoaxes, and the most current infectious threats.

F-Secure

<http://www.f-secure.com/>

Kaspersky

<http://www.kaspersky.com/>

McAfee

<http://us.mcafee.com/virusInfo/default.asp>

Panda Software <http://us.pandasoftware.com/>

Symantec (Norton Anti-Virus)

<http://www.symantec.com/>

Trend Micro (PC-cillin)

<http://www.trendmicro.com/en/home/us/personal.htm>

## Additional Virus and Hoax Lists

Hoaxbusters

<http://hoaxbusters.ciac.org/>

McAfee Virus Hoaxes

<http://vil.mcafee.com/hoax.asp>

Symantec Security Response

<http://securityresponse.symantec.com/>

Viruslist.com

<http://www.viruslist.com/eng/index.html>

## Other Resources

COMPUTER VIRUSES by Markus Hanhisalo

Department of Computer Science, Helsinki University of Technology

[www.tml.tkk.fi/Opinnot/Tik110.501/1997/viruses.html#1.](http://www.tml.tkk.fi/Opinnot/Tik110.501/1997/viruses.html#1.)

[Introduction%20to%20Computer%20Viruses](#)

Center for Information Technology, National Institutes of Health, Bethesda, MD

<http://www.alw.nih.gov/Security/security-faqs.html>

Armor2Net.Com

[http://www.armor2net.com/knowledge/computer\\_security.htm](http://www.armor2net.com/knowledge/computer_security.htm)

Wikipedia.Com

[http://en.wikipedia.org/wiki/Computer\\_virus](http://en.wikipedia.org/wiki/Computer_virus)

TrendMicro.Com

<http://www.trendmicro.com/vinfo/>

HowStuffWorks.Com

<http://www.howstuffworks.com/virus.htm>

Symantec.Com (Norton Anti-Virus)

[http://www.symantec.com/security\\_response/index.jsp](http://www.symantec.com/security_response/index.jsp)

Cnet.Com

[http://www.cnet.com/2001-11351\\_1-0.html](http://www.cnet.com/2001-11351_1-0.html)

Microsoft.Com

[http://www.microsoft.com/athome/security/viruses/intro\\_viruses\\_what.mspx](http://www.microsoft.com/athome/security/viruses/intro_viruses_what.mspx)