

## Internet Security for Home Users

### How vulnerable is your home computer?

Not long ago, Internet users were advised that they were safe as long as they were running antivirus software. At present, this is not completely true. To be better protected, internet enabled computers should use additional measures such as firewalls and anti-spyware programs in addition to antivirus software.

### What changed?

Connection time is a big change. High speed Internet connections allow computers to be connected at all times. Unfortunately, this generally means that your connection is visible and exposed for that time. Hackers and malicious programs such as Trojans constantly try to access machines that are openly broadcasting IP addresses. Each home computer has an IP address which is like a 'mailing address' that other computers can use to connect to your computer.

Firewalls help protect users from these threats. Also limiting your computer's exposure reduces the chances that you may be affected.

**Tip #1** - When you are not using your computer, turn it **off** or unplug your network connection (often a CAT-5 network cable) from the back of the computer.

Also, new threats such as Spyware, Malware, Browser Hijackers, and Dialers have become prevalent.

### How does Spyware, Malware, Browser Hijackers, and Dialers infect systems?

Spyware, Malware, Browser Hijackers, and Dialers are developed to track your movements on the Internet, create statistics of what you do on your computer, or even worse, actually hijack your web connections to direct you to pages that you did not ask for. In general, they infect your system through security 'holes' in your web browser.

**Tip #2** - Be smart about what you click, what attachments and files you open, and sites you visit. Learn to recognize suspicious messages!

### Do I have a problem?

Quite frankly, all unprotected internet users will have to deal with these threats at some time. Some problems have symptoms while others are quite sneaky. Here's a summary of just some of the effects that you may or may not notice:

Symptom	Potential Cause
<i>none</i>	Tracking cookies collect information on your surfing habits
Computer runs much slower than you were used to	Spyware or Dialer is using a process or service to send your data back to a collection server; or (rarely) malware has deleted system files, changed settings, or installed a malicious program
Your home page is different	Browser Hijacker has infected your system
Your browser crashes often	Browser Hijacker or Malware has infected your system
Your browser is redirected to a site other than the one intended	Browser Hijacker has infected your system
Your browser has a toolbar installed without your permission	Spyware has infected your system
You experience constant annoying Pop-Ups	Spyware has infected your system
Your search results appear in a different site than expected	Browser Hijacker has infected your system
You get a "can't find file" error at startup or your settings appear	Malware has possible deleted system files or changed your computer's settings

different	
-----------	--

### How do I find and remove Spyware and other malicious programs?

Learn how to use free programs such as [Lavasoft Ad-Aware SE](#) and [Spybot Search and Destroy](#) to detect and remove these programs about once a week. Some programs such as [SpywareBlaster](#) help prevent infection in the first place.

### How can hardware firewalls help?

A hardware firewall is a physical piece of equipment usually called a 'router.' At any time on the Internet, remote computers or worms scan large blocks of IP addresses looking for computers with security holes. When you connect your computer, if one of these scans find you, it will be able to infect your computer as you do not have the latest security updates. You may be thinking, "What are the chances of my computer getting scanned with all the millions of computers active on the Internet?" The truth is that your chances are extremely high as there are thousands, if not more, computers scanning at any given time. The best solution is installing a hardware router/firewall.

A hardware firewall 'hides' your home computer's specific IP address. It functions similarly to 'call blocking.' Hackers or malicious programs must make a determined effort to bypass its protection.

### How can software firewalls help?

A software firewall is a software program that runs on your computer. It gives you an extra layer of protection against malicious threats. Windows XP (SP2) is packaged with one, so turn it on! Other popular firewalls include [ZoneAlarm](#) and those packaged with [Norton Antivirus](#) and [McAfee Antivirus](#) programs.

### Is your operating system up to date?

To limit potential 'holes' in your operating system and web browser, ensure you have downloaded and installed critical updates from Microsoft <http://www.windowsupdate.com> or if you are an Apple user, [Apple Security Site](#). Windows Update has options to automate downloads to make the process easier.

## Internet Security checklist

Item	Complete
Hardware Firewall	✓
Software Firewall	✓
Antivirus Software installed and updated frequently	✓
Microsoft / Apple Critical Updates updated frequently	✓
Spyware removal/Protection programs installed and run once a week	✓
Continuously learn about safe 'clicking'	✓

### More information

Check with your high speed internet provider. For example, visit [Comcast Support Help](#) at <http://www.comcast.net/help/?CM.src=helpcomcast>

### Highly recommended...

Much of this information was derived with assistance from [www.bleepingcomputer.com](http://www.bleepingcomputer.com). Read the [tutorials](#) for much more information on all of these topics!

Have a safe and secure online experience!

**ITMC**