

Best Practices for Keeping Your Computer Secure

By Michael J. McEvoy, Founder, Home Technology Solutions of Marin

Threats to the security and integrity of personal computers continue to increase at a rapid rate. Viruses, worms, spyware, Trojan horses, adware, browser hijackers, and other malevolent pieces of software can cause a wide range of problems and unwanted system behavior. Home Technology Solutions of Marin continues to strive to assist our clients in understanding current technology issues by providing in-depth information. This article is also available in PDF form and may be downloaded by clicking this link: ["Keeping your Computer Secure.pdf"](#)

Who Should Read This Newsletter? Anyone using a computer.

Why This Issue Is Important to You: Computer security breaches can result in data loss, systems crashes, very slow system performance, files and personal information being taken from your system. In a worst-case scenario, computer security breaches can lead to identity theft.

Important Security Steps: There are a number of steps that people can take to prevent problems from malevolent software programs such as viruses and spyware. Below is a list of defensive measures followed by expanded explanations.

1. Install all Windows updates and Service Packs as they become available
2. Use Internet security software. Internet Security Suite software is the most effective solution and include antivirus, firewall, antispyware, and intrusion prevention modules.
3. Keep your antivirus software and virus definitions up to date
4. Run a full system scan for viruses and spyware every week
5. Use a Spam filter for all incoming email

Read below for six important steps in protecting your computer system, data and personal information.

Step 1. -- Microsoft Windows Updates and Service Packs

Microsoft produces software updates for the Windows operating system and Internet Explorer on a regular basis. Updates are free and by default Windows is set to automatically download and install them. These updates include bug fixes, patches for security "holes" and enhancements in functionality.

Periodically Microsoft combines a group of these "updates," adds some additional functionality and features, and packages them in as a Service Pack (SP). Microsoft has issued three services packs for Windows XP – SP1 included mainly patches and bug fixes; SP2 was focused on improving and enhancing security; SP3 contained additional patches, fixes and enhancements. Microsoft has also issued SP1 for Windows Vista that provided a large number of patches, fixes and enhancements.

We strongly recommend that you install all service packs. Without the benefits that these service packs provide your system will be much more susceptible to problems from instability, degraded performance, and security breaches. For instance, Without XP SP2, some spyware is extremely difficult to remove even with the best removal tools currently available. In addition, without XP SP3 or Vista SP1 installed Windows may not be able to install future updates. This would increase your system's security vulnerability.

Step 2. -- Use Internet Security Software including Antivirus, Firewall and Antispyware.

A. Firewall Software

Firewall software acts as a gatekeeper to your PC and monitors which Internet traffic is allowed in and out of your system, hides the presence of your PC from online hackers looking for systems to invade, and prevents unwanted software from hijacking your PC for malicious purposes. Firewalls, mainly hardware-based, have long been a fixtures at large companies which must protect their networks. However, the rapid growth of email and web-based threats has made software firewalls an essential element of protection for home and small business PCs as well.

A common threat blocked by firewall software is a Trojan horse. This type of threat can open up a "backdoor" that allows the program to communicate from your system to other systems and servers, download other malicious software, and transfer data from your system to other systems. In general, the longer a Trojan horse program exist on a system, the more embedded it becomes and the greater the amount of other malicious software it will download.

In situations where one or more Trojan horse programs have become embedded on a system, they become increasingly difficult to contain, control, and remove permanently without the use of firewall software. The eradication process can take multiple removal tools and several hours of time. When these types of malicious programs run unchecked for too long they can seriously corrupt, and even crash a system, sometimes requiring a complete re-installation of the Windows operating system.

With the release of Windows XP Service Pack 2 Microsoft included an enhancement known as the Windows Firewall. While this firewall is better than nothing, it is limited in its functionality. The Windows Firewall focuses mainly on blocking unwanted incoming traffic from your system. Firewall software from publishers such as Symantec/Norton, Zone Alarm, Trend Micro, and McAfee provide a much more robust set of security features including the ability to monitor and block outbound traffic from your system to the Internet.

B. Antivirus Software

The most well known security tool for PCs and the one that has been available the longest is antivirus software. The most popular packages include Norton Antivirus, McAfee ViruScan, and Trend Micro's PC-cillin. It is very simple: if you do not have antivirus software, get it ASAP, use it to run regular system scans, and check it periodically to make sure the components are up to date.

A major reason viruses continue to infect systems is due to some users not updating the virus "definitions" or data files. A virus definition data file is a virus-identification "catalog" which provides the anti-virus software with the information necessary to identify viruses when they enter your system. Software developers like Symantec/Norton, McAfee, Trend Micro and others create new virus definitions on a weekly, and sometimes daily, basis.

Registered users can download up-to-date definitions and apply them to their systems. Most anti-virus software packages provide an "automatic update" feature that will transparently update the virus definition data whenever new updates become available.

There are also a couple very good free antivirus packages such as AVG from Grisoft and Avast Home Edition from ALWIL Software. However having an integrated internet security package (Internet Security Suite) that includes antivirus, firewall, intrusion detection, and other security features in a common interface is generally the most effective security solution.

C. Anti-spyware and Spyware Removal software

"Spyware" is a type of malicious software that ends up on users' systems without the user's knowledge or consent. Spyware transmits or redirects data from your system to another system or web site via the Internet. In the vast majority of situations, this happens without the user's knowledge. Systems used by children and teenagers consistently have the highest concentration of spyware.

The best Internet Security Suites will catch and remove spyware and other malicious software without the need for additional software. If your spyware problems are significant, there are also a number of standalone spyware detection and removal programs available. Some products can run in a mode similar to anti-virus software where they are loaded at the time the system is started and continually monitor the system to prevent new spyware from being loaded. Most free antispyware products do not run in this mode.

If you do use antispyware products, it is important that you update the "spyware definition" or "signature file" before each scan. New forms of spyware are released frequently - you need to use the most current spyware definitions to catch the most current spyware.

Three products that we use and recommend are Spysweeper by Webroot (paid for), Ad-Aware Personal SE by Lavasoft (free), and PC Doctor from PC Tools (paid for). These products get consistently high grades in product reviews.

Step 4. – Spam Filtering and Blocking

A very significant percentage of viruses, spyware, and other malicious software get on computers via unwanted and unrequested email. Call it spam or call it junk, but you can definitely call it nasty. Have a good spam-blocking program and have it set to a high enough level. Some email packages such as Outlook, Yahoo mail and Gmail have built in spam blocking/capturing functionality. If your email program does not provide effective spam blocking there are a number of effective and relatively inexpensive spam blocking programs available.

Spam filters are not 100% effective and some junk will get through, so it best to follow some email self-protection rules of thumb. Do not open email or email attachments unless you know the sender of the email. Never download an attached file from an email that you weren't expecting to receive. Never click on "Unsubscribe" on an email that you suspect to be spam or junk mail. This will just tell spammers that your email address is active and you will likely end up getting more junk mail. Never click on an email attachment with an .exe file extension such as "myfile.exe". These are program files and clicking on them will begin running a program that could be nasty. Never click on a link within a suspected spam email – just delete the message immediately.

Step 5. – Hardware Firewalls for directly connected broadband connections

Computer users with a broadband Internet connection such as a cable modem or DSL connection and are not on a local (private) network have a direct Internet connection and a public IP address on the Internet. Using a hardware firewall provides an easy-to-use added level of protection. If you have a network in your home or office you most likely already have a hardware firewall built into your router that links your multiple PCs. Wireless router products manufacturers such as Netgear, Linksys and D-Link provide excellent protection against external threats.

Step 6. – Diligence - Keep all components up to date!

Most of your security components require periodic updating and most are updated automatically. However, it is highly recommended that you check occasionally to make sure that these updates are taking place and that your components are up-to-date. New viruses, spyware and other security threats are released daily. If your software expires or gets out-of-date, your system becomes susceptible to new threats.

An Ounce of Prevention...

The Good Old Days before users needed all this "protection stuff" are gone. While state and federal governments are trying to control some of these problems through laws and legislation, it is a rather slippery slope and it changes rapidly. The reality is that with the advent of the Internet you are not just concerned with security attacks coming just from within the United States. As the term "World Wide Web" implies you are connected to any point in the World. Security attacks can come from Romania, Cambodia, Nigeria, Russia, or any other point in the world - many places where U.S laws have little effect. That old saying, "An ounce of prevention is worth a pound of cure" definitely holds true with computer security.

Michael J. McEvoy has over twenty years of professional experience in the technology world and is the founder of **Home Technology Solutions of Marin**, a business that simplifies computer, Internet, and digital technology for individuals, families, home offices, and small businesses. HTS saves clients time, money, energy, and frustration when selecting, installing, integrating, using, and managing digital technology. Contact us at (415) 924-5373 or mike@htsmarin.com Visit us on the web at www.htsmarin.com or at our "Tech Tips, Computer Support and Technology News" blog – www.htstechtips.com.