



MTS Home Solutions

<http://www.mtshomesolutions.com>

260 Byers Road, Chester Springs, PA 19425 (484) 341-0053

E-mail: services@mtshomesolutions.com

What Do I Need to Protect My Computer From Viruses and Spyware?

Computer viruses, spyware and malware are all too common on many home computers today. Many times, folks do not even realize that they have some type of infection on their system until it starts to display common symptoms of a virus or malware infection, including slowness, pop-up ads and file corruption. Fortunately, many products are available on the market today which can adequately protect a user's home computer from most spyware and malware infections.

What is a Computer Virus?

- **Viruses** - A virus is a small piece of software that piggybacks on 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** - An e-mail virus travels as an attachment to [e-mail messages](#), and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. Some e-mail viruses don't even require a double-click -- they launch when you view the infected message in the preview pane of your e-mail software [source: [Johnson](#)].
- **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](#)). Trojan horses have no way to replicate automatically.
- **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.

(from *How Computer Viruses work* - <http://www.howstuffworks.com/virus.htm>)

What is Spyware?

Spyware is a category of computer programs that attach themselves to your [operating system](#) in nefarious ways. They can suck the life out of your computer's processing power. They're designed to track your Internet habits, nag you with unwanted sales offers or generate traffic for their host Web site.

(from *How Spyware Works* - <http://computer.howstuffworks.com/spyware.htm>)

How Can I Protect my Computer?

Every computer needs **at least 4 elements of basic protection** to prevent infection by a computer virus, spyware or malware:

- **A Good, Legitimate Antivirus Product.** Like a locks on the door of your house, a quality antivirus program will prevent most viruses from executing or starting on your computer (sometimes called real-time scanning), will have the ability to scan your system for infections on a regular basis (scheduled scans) and will have the ability to update itself with new virus definitions at least daily. Many home users assume that they have to pay a big name software company (examples, McAfee, Symantec/Norton, etc.) an annual fee to use their antivirus product in order to be adequately protected. Many of my customers report, however, that McAfee and Norton tend to use a fair amount of system resources and tend to slow their computers down. For home users, though, several good **free** products are available which will adequately protect a user's system. Some of the most reliable programs include:

Microsoft Security Essentials (http://www.microsoft.com/Security_Essentials)

AVG (<http://free.avg.com/>)

Avira (<http://www.free-av.com/>)

Avast! ([\">http://www.avast.com/eng/download-avast-home.html](http://www.avast.com/eng/download-avast-home.html))

BEWARE OF COUNTERFEITS! There are many rogue antivirus and antispyware products on the internet (e.g. Antivirus 360, Anti-Virus-1) which claim to have found an infection on your computer and will guarantee (for a fee) to clean your system. A good rule of thumb is this: if you do not recognize or did not install a particular antivirus program, then the warning, and the software, is not legitimate.

A computer can only have 1 antivirus program installed at a time. If more than one product is installed, the programs will conflict with one another and cause problems on your system.

- **At Least 2 Good, Legitimate Anti-Spyware Products.** While many of the commercial antivirus products are now offering a **suite** of products which include both antivirus and antispyware, it is possible to protect your system by using one of the free products below:
 - Windows Defender (<http://www.microsoft.com/windows/products/winfamily/defender/default.mspx>) (included in Microsoft Windows Vista and Windows 7)
 - Spybot Search and Destroy (<http://www.safer-networking.org>)
 - Ad-Aware (www.lavasoft.com/products/ad_aware_free.php)

Also, there are a couple of legitimate products which are available which can scan your system for spyware & malware and remove it, but do not provide real-time scanning or scheduled scanning protection. Included in these are:

- Malwarebytes (<http://www.malwarebytes.org/mbam.php>)
- Superantispyware (<http://www.superantispyware.com/download.html>)

- **A Quality software firewall product.** A firewall prevents unauthorized network connections from being made to or from your computer. The firewall which is included in the Microsoft Windows XP operating system (service pack 2) is decent, but is not totally sufficient for protecting most home computers, primarily because it only blocks incoming connections but not outgoing connections. The firewall included in the newer Windows Vista operating system is more robust and is probably sufficient for most home users. Many of the "suite" antivirus/antispyware products include a good software firewall which will sufficiently protect your system. Home users can also download and install a free firewall product, such as one of these below:

- Comodo (<http://personalfirewall.comodo.com/> also includes free antivirus software. Customers can install just the firewall, if they wish)
- Outpost Firewall (<http://free.agnitum.com/>)

Like antivirus software, it is recommended that users install and use only 1 software firewall on each computer. However, users can add another layer of protection by enabling the hardware firewall which is available on many home routers.

Some users dislike having a firewall active on their system because it occasionally alerts the users when suspicious network activity is detected, especially after the firewall is first installed. While this might seem like a nuisance, this is a small price to pay to ensure that your system is not being hacked by someone seeking to gain access to your sensitive personal data.

- **Operating System and Software Updates** One of the most common ways that hackers, spammers and virus makers gain access to computers is by utilizing security flaws or “holes” in a user’s operating system, web browser or other software installed on the computer. While some feel that Microsoft Windows is more vulnerable than other operating systems, the reality is that most of the security attacks focus on Microsoft systems and software primarily because it garners the lion’s share of the home & corporate computer market. That is, Microsoft is by far the biggest target on the block; therefore, it is worth a hacker’s time to create malware for the majority of systems.

The best way to combat this type of attack is to ensure that your computer’s software is up to date. Microsoft makes it fairly easy to do this through their Automatic Updates feature in Windows XP/Vista/7. MTS can also run a small audit utility which will determine whether or not a computer contains all of the current Microsoft updates. Also, there are some third-party utilities which will scan other software on your computer to determine if you have the most up to date (and usually most secure) version of the software. If any updates are recommended, MTS can help you to download and install those as well.

A Chain is Only as Good as Its Weakest Link

Though a home computer may have antivirus and antispyware software installed, may be running a firewall and may have current software updates, it is still possible for a system to become infected. Just as the best locks and the most high-tech security system will not prevent a homeowner from opening the door to an intruder, these computer safeguards will not provide protection if the user allows a virus or piece of spyware to be installed on his or her system. Therefore, it is wise to follow these suggestions:

1. Do not open e-mail attachments from senders if you were not expecting something. Though attachments are no longer the primary way of spreading viruses, this still happens. Many Trojans attack a user’s address book and e-mails themselves out to all of a user’s contacts. Scan an attachment with your antivirus software first if you are unsure.
2. Be careful where you click. The most prevalent way that malware is spread currently is through hyperlinks in e-mail or on an infected web page. What you think may be an innocent click may actually be opening a door to download a nefarious program onto your computer. If you are unsure of the link, check the website out first. Some newer web browsers and antivirus software (e.g. Internet Explorer 8, AVG Linkscanner) help you to test if a website is legitimate or not.
3. Avoid peer-to-peer file sharing sites, such as Limewire and BitTorrent. Many folks use these sites to share music or video files. However, these sites are known for virus and spyware-injected files. If you choose to use one of these sites, you are potentially opening up your computer to malware. Surf at your own risk!
4. Be wary of applications and links on social networking sites such as Facebook, Myspace and Twitter. Because these sites have grown so quickly in popularity over the last couple of years, many of the links and applications

which appear have not been properly vetted. As a result, it has become increasingly easy to download various types of malware onto your computer by a seemingly innocuous click.

Some Final Recommendations

MTS Home Solutions confidently recommends [Comodo Internet Security Pro](#) as a strong, affordable tool to protect your computer. CIS combines a high-quality firewall with [antivirus and antispyware protection](#), [wireless network security](#) and 24x7 tech support through [LivePC Support](#). All of this is available for a very reasonable price of **\$39.00 per year**. MTS can come to your home to install CIS and will configure it to assure your computer is well-protected. Comodo Internet Security Pro is also included in our Silver and Gold [Home Computer Support Plans](#).

MTS Home Solutions would be happy to assist you in assessing your current computer system's security level. We offer a 1-Hour Security Audit to determine the current status of antivirus, antispyware and firewall software, as well as your current Microsoft patch levels. We can complete this audit either on-site (\$70 for 1 hour) or by connecting remotely to your computer (\$40 for 1 hour). If we detect the presence of viruses or malware on your system, we can work remotely or on-site to remove them at these standard hourly rates. It is not necessary for home users to be paranoid about computer security, but users do need to give it serious attention.