

Protecting Your Computer - Summary

In September 2007, we talked about “System Maintenance”, comprising Disk cleanup, Defrag, Registry cleaner, Startup programs, and Nasties. This month we will discuss the “Nasties” (malware, viruses, trojan horses, worms, adware, spyware) in detail. See Appendix A for the Glossary.

Virus has become the generic term for any malicious program that spreads itself from one computer system to another. Accurately speaking, however, there are three broad categories of such software: viruses, worms, and Trojan horses. See Appendix A for the Glossary.

Throughout this discussion, we'll be using the term "virus" in a generic sense incorporating true viruses, worms, and Trojan horses.

Too many PC users treat security as an event rather than a process. For these users, security software is installed, partially configured once, and then never touched again. The problem is that Internet threats are constantly changing, so the files and filters you're using today may not protect you tomorrow. Users that seek real protection must take the time to understand their security tools and use them aggressively.

Some of the information in this paper came from “Smart Computing” (a great magazine and computer resource) <http://www.smartcomputing.com/>.

Spyware tests were run by PC World (another great magazine and computer resource) <http://www.pcworld.com/>.

The following appendixes are in the file named “Protecting Your Computer – Details”

See Appendix A for the Glossary. (Page 6)

See Appendix B for signs of an infection. (Page 8)

See Appendix C for staying ahead of virus outbreaks. (Page 9)

See Appendix D for information on Spam. (Page 11)

Prevent & Fight Viruses.

Here are some tips on how to fight viruses.

Watch your downloads. The best way to fight a virus is to not catch it in the first place. You can avoid the vast majority of viruses by following one very simple rule: Never open any program file if you are not 100% certain what it is. Ever!

That means when you get the email message from YourPalFred that says, "This is the best game I've ever seen, you'll love it!" do not open the attached file. Email YourPalFred, or better, call him to see if he really sent it and if he knows for certain that the message is safe.

Avoid files that have double extensions. The **extension** is the part of the file name that comes after the period. For example, in the file MapGraphic.jpg, the extension is .JPG(Joint Photographic Experts Group). This indicates a common graphic file format that cannot carry a virus. Other file extensions that indicate formats unable to carry viruses include .GIF (Graphics Inter-change Format) files and .TXT (plain text). Because many people know that these formats are safe from viruses, some virus makers will give their files names such as Mypicture.jpg.exe or Information.txt.pif.

Protecting Your Computer - Summary

Without knowing better, you may see the .JPG or .TXT extension and think the file is safe. But those second extensions (.EXE and .PIF) indicate executable files. These are not graphic or text files; they are programs and probably viruses.

Then, even when you have every reason to believe that a file is probably safe, don't open it until you've checked it out with up-to-date antivirus software.

Always run antivirus software.

If you don't have antivirus software, then stop reading right now and buy some before finishing this article. You can buy it online. The two leading antivirus programs are Symantec's Norton AntiVirus (\$49.95, http://www.symantec.com/nav/nav_9xnt) and McAfee Virusscan (\$49.99, <http://us.mcafee.com>). Norton even offers a 60-day free trial. Other options are posted in the sidebar, "Other Antivirus Software." Whichever program you select, set it to scan all incoming email and files and to do full scans of your computer at least once a week.

It's important to note that just having antivirus software is not enough. It must be up to date. New viruses are detected every day, and during times of heavy virus activity, last week's antivirus software is next to worthless. That's why antivirus software comes with a subscription for free updates to the catalog of viruses the software will detect and defend against. Select the automatic update option and your software will check its company's Web server regularly for newly added virus definitions and will install them without any effort from you. Most subscriptions are for one year, so be sure to renew when your subscription is up.

Do you have reason to suspect a virus infection? (See Appendix B – Signs of an infection) Then, if you already have antivirus software, make sure you have the latest definitions installed and run it right away. If you don't have any, both McAfee and Norton let you do an online scan for viruses at no charge. Run either scan immediately.

The McAfee free online service is called FreeScan. You'll find it at the bottom of the company's home page at <http://us.mcafee.com>. You will need to register and download an ActiveX control before running the scan.

Norton's version is its Free Online Virus And Security Check. You'll find it at <http://securityresponse.symantec.com/> under Virus Definitions.

<http://www.pcmag.com/article2/0,1895,2186662,00.asp>

One of these days, if you haven't already, you'll receive an email message telling you of some dire new virus. It probably will tell you not to open email with a certain name because that will activate a virus that will do terrible things, and that no antivirus software yet knows how to protect against it. It will tell you that the author of the message checked it out with Norton or McAfee or Microsoft or IBM and received verification that this tale of horror is true. It will then tell you to forward the email to all of your relatives, friends, associates, and co-workers

Please heed this: That email message will be a hoax. A lie. A total fabrication. If you get one, ignore it. If you can't help but worry, "What if *this* one is real?" you can check out the web site run by the U.S. Department of Energy. It keeps a database of hoaxes at <http://hoaxbusters.ciac.org>.

Protecting Your Computer - Summary

In Summary.

Computer viruses will rarely if ever be a real threat to you as long as you follow the rules:

- Never download a file until you're 100% sure of its safety
- Keep antivirus software up to date and running at all times
- Do frequent and regular scans of your full system

Then, your biggest problem with viruses will be deleting all the virus-carrying email messages from those who failed to be as careful as you.

Look to specific software packages such as Norton AntiVirus (\$39.99; www.symantec.com). However, if you're looking for something that won't cost a monthly fee or for a subscription, consider an open-source alternative such as ClamWin (free; www.clamwin.com) or Grisoft's AVG Antivirus Free Edition (<http://free.grisoft.com/doc/download-free-anti-virus/us/frt/0>). The ClamWin regular virus definitions don't update as frequently as they do for commercial vendors, but it should be enough for most users. The AVG virus definitions are frequently updated. Also, most antivirus software vendors also have a security suite that includes antivirus software and firewall software. The software will help keep out intruders and will let you know when programs on your computer are trying to access the internet.

Adware. This software might be picked up while using email, browsing the Web, or installing some software. One of the best-regarded tools for removing this software is Lavasoft's **Ad-Aware** 2007 (free; http://www.download.com/Ad-Aware-2007-Free/3000-8022_4-10045910.html?part=dl-ad-aware&subj=dl&tag=top5) which removes a great deal of malware by providing a mechanism to update its definitions, much like an anti-virus package. There are two other versions of Ad-aware (Plus and Pro) that are sold by Lavasoft.

This is a comparison chart of the three levels of Ad-aware:

http://www.lavasoftusa.com/download_and_buy/product_comparison_chart.php

Spybot – Search & Destroy

(<http://www.safer-networking.org/en/index.html>) will search for spyware and delete it. Spybot is free, but will function only if the included ad software is not deleted by Ad-Aware (see the above paragraph). Spyware silently tracks your surfing behavior to create a marketing profile for you that is transmitted without your knowledge to an outside computer and sold to advertising companies. Isn't it ironic that Spybot searches for spyware but won't run unless its own spyware is enabled!

Spyware Doctor 5.0

(<http://www.pctools.com/spyware-doctor/>) is the highest rated spyware program, as tested by PC World, with a rating of 95. Spybot – Search & Destroy had the lowest rating, at 59.

After running Spybot – Search & Destroy, Spyware Doctor still found 9 threats and 229 infections!

Protecting Your Computer - Summary

Windows Vista Defender

The free spyware program that comes with Windows Vista fared poorly on the PC World test, with a rating of 72. This was the second-worst program, ahead of only Spybot – Search & Destroy. Windows Defender is also available for the Windows XP operating system.

This is a summary of test results, as published in the October 2007, issue of PC World:

Software	Rating	Inactive adware detected	Inactive spyware detected	Inactive rootkits detected	Found changes to startup folder	Scan time, seconds
PC Tools Spyware Doctor	95	81%	38%	89%	Yes	380
Grisoft AVG Anti-Spyware	81	69%	80%	100%	Yes	496
Webroot SpySweeper	76	26%	10%	44%	Yes	132
Microsoft Windows Defender	72	48%	5%	0%	Yes	320
Safer Networking Spybot Search & Destroy	59	2%	0.4%	0%	No	588

Some of the information in this paper came from “Smart Computing” (a great magazine and computer resource) <http://www.smartcomputing.com/>.

Spyware tests were run by PC World (another great magazine and computer resource) <http://www.pcworld.com/>.

Consumer Reports has released their recommendations for the best anti spam [software](#), the best anti spyware remover, and the best [anti virus](#) software.

With respect to Consumer Reports’ recommends Allume’s [Spamcatcher](#). According to CR, Spamcatcher “beat others at detecting and blocking spam,” and “is an excellent performer and has lots of cool features.”

CR recommends Webroot’s [Spy Sweeper](#). Spy Sweeper, says Consumer Reports, does “a great job at detecting spyware” and is “easy to use.” You can [get Webroot Spy Sweeper](#) from Amazon for \$24.99.

Finally, there was a tie for the best anti virus software. According to Consumer Reports, both [BitDefender](#) (\$33.99 from [Amazon](#)) and [ZoneAlarm](#) (\$22.99 from [Amazon](#)) are excellent, and both “even recognized new viruses we created just for our tests.”

All of this information came from the January 2007 issue of Consumer Reports’ new magazine, *ShopSmart*, and is geared towards Windows users.