

THE HAWK I VIEW



Hawk iSolutions Group, Inc.

What's
Inside

**Don't Let
Mother
Nature Fry
Your
Computer!**

**How To Choose A Good
Surge Protector**

**Three
Dangerous
Threats You
Must Be
Aware Of**

**The Four Most
Costly
Misconceptions
About Spyware,
Malware, And
Other Threats**

How To Protect Your Computer From Mother Nature

Summer is here and with it comes sudden (and sometimes severe) lightning storms. That's why protecting your computer and printer with a surge suppressor is more than a good idea—it's an absolute must.

While a home circuit breaker can protect some of your appliances, they were not built to protect the sensitive electronic equipment in a computer. If a high electrical surge hits your computer, it could fry your motherboard and CPU in seconds causing you to lose data AND the use of your computer.

The biggest mistake most computer users make is thinking that their "power strip" will protect them, when it won't. To adequately protect your sensitive electronic investments, you need a quality, high-end surge suppressor designed to handle the job.

There are main 2 things to look for in a surge suppressor:

First is response time. This is the amount of time it takes this device to react to a power surge. This should be 10 nanoseconds or less; any longer and you run the risk of damaging your PC. The second thing to look for is the amount of energy it can absorb and dissipate

before it blows, measured in joules. I recommend at least 800 joules or more.

Another feature to look for is a failure indicator light. This light will come on when the suppressor is fried and no longer protecting your computer. Most surge suppressors will have this.

If you are using a dial-up modem, be sure the suppressor blocks electricity that can come in from the phone lines. If you have a fax or cable line, make sure the suppressor you choose handles those too. You also want to make sure the suppressor you choose meets the UL 1449 specifications (this will be listed on the box).

There are three levels of protection: 330, 400 and 500. This number refers to the maximum voltage that the suppressor will allow to pass through the line. The lower the number, the better off you are. Finally, unplug your computer and all computer equipment, telephone, and modem lines during a lightning storm. This is the ultimate protection against sudden and devastating power surges.

Need Help In Choosing A Surge Protector For Your Computer?

Please keep in mind that there is going to be a variety of prices for the surge suppressors. The one thing that will set them apart is usually the warranty coverage the company provides in case of a failure with their equipment. APC and TrippLite are just a few that we recommend to our customers.

If you want to make sure you are getting the right surge protector for your PC or network AND setting it up properly, give us a call. We would be happy to answer your questions.



"You guys go ahead. I think I've found something here on ebay."

Three Dangerous Threats You Must Be Aware Of

One of the most dangerous aspects of online threats is their ability to cloak their existence. Hackers and the authors of malicious spyware and malware programs go to great lengths to create programs that are difficult to identify and remove.

That means a malicious program can be downloaded and doing its dirty work on your computer long before you are aware of it. Below are the two most common threats you'll need to guard against with a brief explanation of what they are:

Spyware: Spyware is Internet jargon for hidden programs advertisers install on your PC without your permission to "spy" on you, gather information, and report this information about you and your online activities to some outside person.

Spyware is NOT harmless; it can be responsible for delivering a boatload of spam, altering your web browser, slowing down your PC, and serving up a bounty of pop up ads. In some of the more extreme cases, spyware can also steal your identify, passwords, e-mail address book, and even use your PC for illegal activities.

Most spyware finds its way onto your computer via file downloads including free programs, music files, and screen savers. While you *think* you are only downloading a legitimate program to add emoticons to your e-mails, you are unknowingly also downloading a heaping spoonful of spyware programs.

Spyware piggybacks the download and runs undetected in the background collecting information about you and sending it back to its originator. Although spyware has malicious components, it is not illegal, and it is not considered a virus because it doesn't replicate itself or destroy data.

Malware: Malware is short for **malicious software** and represents all programs, viruses, Trojans, and worms that have malicious intent to damage or disrupt a system. Malware is harder to remove and will "fight back" when you try to clean it from your system. In some extreme cases, we have had to completely wipe out all of the information on the computers' hard disk and start with a complete re-install of the operating system.

Among other things, a malware infection can corrupt your files, alter or delete data, distribute confidential information such as bank accounts, credit cards, and other personal data, disable hardware, prevent you from using your computer, and cause a hard drive to crash.

Frequently, malware is also designed to send itself from your e-mail account to all the friends and colleagues in your address book without your knowledge or consent.

Hackers: Hackers are computer programmers turned evil. They are the people who design the spyware and malware programs that attack your computer. Why do they do it?

Who knows...

Some of them have criminal intent and use these programs to steal money from individuals and companies. Some have a grudge against the big software vendors (like Microsoft) and seek to harm them by attacking their customers (you). Others do it purely for fun. Whatever the reason, hackers are getting more intelligent and sophisticated in their ability to access computer systems and networks.



Surefire Signs That You Are Infected With Spyware, Malware, and Viruses

Since most malicious programs are designed to hide themselves, detecting their existence is not always easy. However, there are a few surefire signs that you have been infected:

- * You start getting swamped with pop-up ads that seem to come from nowhere and constantly interrupt your use of the computer.
- * Your computer is unstable, sluggish, locks up, or crashes frequently.
- * Your web browser's home page changes on its own and you cannot modify the settings. You may also see toolbars on your web browser that you did not set up.
- * You get a second or third web browser popping up behind your main browser that you didn't open or request.
- * Mysterious files suddenly start appearing.
- * Your CD drawer starts opening and closing by itself.
- * You get constant runtime errors in MS Outlook/Outlook Express.
- * You find emails in your "Sent Items" folder that you didn't send.

Some of your files are moved or deleted or the icons on your desktop or toolbars are blank or missing.

If you are experiencing one or more of the above when using your computer, you are infected and should seek help from a senior computer technician. But before I talk about getting rid of it, let me share with you 4 costly misconceptions about spyware, malware, hackers, and other threats that you will also need to know...

Continued on page 3..

www.hawkisg.com

Bits N Bytes

Thanks For The Kind Words...

"When we call with problems, we receive immediate service, Thanks!"

-Steve Perini, Office Manager,
Rehabilitation Medicine Specialist

It Can Always Be Worse...

A father was surprised to see his son's bedroom looking orderly. His son had left a note on the bed which said, "I'm sorry to say that I am leaving. I'm 15 now and have to elope with my girlfriend. She's pregnant. Don't worry; she already has a trailer and firewood for the whole winter. She has taught me that marijuana is good. "

P.S. Actually none of this is true. I'm at Joe's. Just wanted to remind you that some things are worse than a bad report card. It's in my dresser drawer. Call me when it's safe to come home

It's Printed On The Bottom...

A little boy returned from a trip with his father to visit the neighbor's new puppies. He excitedly told his mother there were four new puppies: two boys and two girls. The mother asked him how he knew which were boys and which were girls. The little boy replied, "Dad picked them up, looked under them, and then told me. I guess it's printed on the bottom."

I'd Love To Hear From YOU!

Is there an article you would like to comment on? Is there a topic you want me to research? Have a funny story or a resource you want to share with the other subscribers? Then write to me! We are always looking for new and useful content to add to The Hawk I View.

Hawk iSolutions Group, Inc.

Michele Antone

(636) 256-7534

michele@hawkisg.com

www.hawkisg.com

The Four Most Costly Misconceptions About Spyware, Malware, and Other Threats

Three Dangerous Threats you Must Be Aware Of Continued...

#1: Spyware and Malware is easy to remove.

Some spyware and malware CAN be easily removed using a program such as Spybot's Search & Destroy (you can download it for free at: www.cnet.com) or Ad-Aware (you can download it at www.lavasoftusa.com/support/download). You can also run Microsoft's Beta Program.

However, not all malicious programs can be removed – or even detected – using the above software. Many programs integrate so deeply into the operating system that it takes a skilled technician several hours to fully diagnose and remove the malicious program. In some extreme cases, we have had no alternative but to wipe the hard disk clean by deleting all of the files on it and re-installing the operating system.

Obviously this is NOT an ideal situation and we do everything within our power to avoid it. Unfortunately there are some malicious programs that are so intelligent that there is simply no other way of removing them.

Of course you can use Spybot or Ad-Aware as a first attempt at cleaning your machine; however, if you continue to notice that your computer runs slow, if you continue to get crippling pop ups, or any other of the tell-tale signs discussed earlier, you will need to seek the help of an experienced computer technician.

#2: It is my computer's fault that I continue to get attacked by spyware, malware, and viruses.

In all cases, malware, spyware, and viruses are a result of some action taken by the user (you or a family member that uses your computer). Remember, cyber criminals are *incredibly clever* and gain access to your computer via some of the most innocent and common activities you are performing; that is why it SEEMS as though it is your computer's fault.

For example, many of the clients we see simply downloaded an emoticon software program. Emoticons are the smiley faces and action characters that you see at the bottom of many people's e-mails. In doing so they also (unknowingly) downloaded a payload of spyware and malware and before they knew it, could no longer use their computer due to the instability and pop ups.

Other deadly programs to avoid are free "enhanced" web browsers, screen savers, and just about any "cute" programs you come across that are free to download. Always read the terms and conditions before downloading ANY program to look for clauses that allow them (the software vendor) to install spyware programs on your computer.

But installing programs is not the only way a hacker or malware program can access your computer. If you do not have the most up-to-date security patches and virus definitions installed on your computer, hackers can access your PC through a banner ad on the web that you accidentally clicked on or through an e-mail attachment that you opened.

Just recently, hackers have even been able to figure out ways to install malicious programs on your computer via your IE web browser EVEN IF YOU DIDN'T CLICK ON ANYTHING OR DOWNLOAD A PROGRAM. Microsoft is constantly providing "patches" to their operating system software and all it takes is one missed update to leave you completely vulnerable.

Finally, you should COMPLETELY AVOID any and all peer to peer file sharing networks such as KaZaa. These sites are the absolute WORST online activities you can participate in for your computer's health because they are pure breeding grounds for hackers, spyware, malware, and other malicious attacks.

Continued on back page...



Hawk iSolutions Group, Inc.

Hawk iSolutions Group, Inc.
6439 Plymouth, Suite 112
St. Louis, MO 63133

Phone: 636-256-7534
Fax: 636-230-9905
www.hawkisg.com

We Make Your
Computer
Soar!

Services We Offer

- PC repair and troubleshooting
- Printer repair and troubleshooting
- Disaster recovery
- System back ups & data protection
- Virus protection & removal
- Network security
- E-mail & Internet setup help
- Wireless networking
- Consulting & support
- One-on-one computer training
- Hardware Sales

ATTENTION SMALL BUSINESSES:

Get all of the computer support you need without the expense of hiring a full time IT staff. Ask about our Small Business Computer Support Program.

Three Dangerous Threats You Must Be Aware Of Continued...

#3: If my computer is working fine right now, I don't need to perform maintenance on it.

This is probably one of the biggest and most deadly misconceptions that most computer users fall victim to. Computers are just like cars. If you don't change the oil, change the filter, rotate the tires, flush the transmission, and perform other regular maintenance on your car, it will eventually break down and cost you FAR MORE to repair than the cost of the basic maintenance. There are certain maintenance checks that need to be done daily (like virus updates and spam filtering), weekly (like system back ups and a spyware sweep), and monthly or quarterly like checking for and installing security patches and updates, disk defrag, spyware detection and removal, checking the surge suppressor and the integrity of the hard drive, and so on.

Your computer repair technician should be adamant that you have regular maintenance done on your computer and should offer to set up automatic virus definition updates, spam filtering (to avoid viruses), and automatic system backups that are stored on an OFF SITE location (this protects the back up from fire, flood, or other natural disasters).

If your technician does not press you to let him do this for you, then RUN – don't walk – out of their office. Lack of system maintenance is the NUMBER ONE reason most people end up losing valuable files and incurring heavy computer repair bills. If your technician isn't offering you these services, you need to find someone else to support your computer or network for two reasons:

Either he doesn't know enough to make this recommendation, which is a sure sign he or she is horribly inexperienced

OR

They recognize that they are *profiting* from your computer problems and don't want to recommend steps towards preventing you from needing their help on an on-going basis.

#4: The firewall and security tools provided in the Microsoft Operating System are all the maintenance and protection I need.

Again, this is a terrible misconception. Microsoft does NOT include ALL of the security features to protect your data from viruses, hackers, and data loss or your PC from running sluggish.

As a matter of fact, there is no one single vendor that provides ALL of the system security features you need to keep your computer and files safe from harm.

Continued next month, Hawk iSolutions Group, Inc. will give you 7 Simple Steps To Secure Your Computer From Malicious Attacks and Expensive Repair Bills.