

THE HAWK I VIEW



Hawk iSolutions Group, Inc.

What's
Inside

**Warranty
Warnings:
Should You Buy
An Extended
Warranty For
Computer
Equipment?**

**Exclusive Report:
Are You
Making
These
Security
Mistakes
When
Surfing The
Web?**

**Phishing
?
Don't Get
Caught!**

**Computer
Maintenance, and
What You Need to
Know!**

6 Simple Steps To Secure Your Computer From Malicious Attacks and Expensive Repair Bills

- 1. Keep an up-to-date anti-virus software running at all times.** We recommend Symantec Norton Anti-Virus because it removes viruses automatically, protects against multiple threats, and defends against new viruses and spyware.
- 2. Use an alternative e-mail program other than Outlook Express.** Outlook Express is notorious for security holes. If you don't have the latest security updates, hackers can send you e-mails with viruses that automatically open and install themselves without you even opening or previewing the e-mail and its attachments.
- 3. Never open suspicious looking e-mails or attachments.** This goes without saying because most viruses are replicated via e-mail. If it looks suspicious, delete it immediately!
- 4. Stop using peer to peer file sharing sites and downloading "cute" programs.** As a rule of thumb, the "cuter" the program, the more dangerous it is. Think of it like "cyber candy". Hackers use these cute and funny programs as bait to get you to download their destructive programs. These are guaranteed ways of contracting malicious viruses, spyware, and malware. Also, peer to peer file sharing sites like KaZaa are mine fields of malicious programs. NEVER access those sites or download the programs that run them.
- 5. Set up a firewall.** A firewall is simply a device that acts as a buffer between you and the big, wild world of the Internet. Many users will get a DSL or cable Internet connection and plug it directly into their computer with no firewall in between. The one thing you have to remember about the Internet is that it is a big open field. You have access to the world but on the flip side, the world has access to YOU. Hackers have programs that automatically scan the Internet for computers connected via a cable or DSL connection without a firewall. Once they find one, they access your computer, download vicious programs, and can even use YOUR computer to send viruses to your friends and other computers, all without your knowledge or consent.
- 6. Back up your files every night.** Have you ever lost an hour of work on your computer due to a crash or program error? Now imagine losing all of your precious family and vacation photos, e-mails, music files, and documents. No one really thinks about losing all of the data on their computer until it actually happens. By then, it is either too late and you have lost EVERYTHING or it will take a lot of money paid to a specialist to recover your files. I cannot stress the importance of backing up your files enough. If the files on your computer are important to you, then it is about time you got serious about protecting them by backing up every night. The back up solution you chose will depend on the amount or size of the data you need to back up. Sometimes a simple zip drive or CD burner will do the trick. If you have a lot of data to back up, you may want to consider a tape back up system. If you want to know what is best for your specific situation, call our offices and one of our technicians will be happy to discuss the best system back up plan for you.

Computer Maintenance: What You Really Need To Know About Keeping Your Network Secure and Reliable

If you're like most people, you don't think twice about performing regular maintenance on your car. You regularly change the oil, keep air in the tires, fill up your gas tank, and take it to the dealer when it needs maintenance.

Yet, if you're like most business owners, you don't even think about doing maintenance on your computer network unless it starts running slow, crashes, or stops working.

Oddly enough, computer networks require far more maintenance than a car, not only to keep them running properly, but also to protect them from an ever growing number of spyware, virus, and hacker threats.

If you want to avoid problems and the expensive repair bills that follow, here's a short list of daily, weekly, and monthly maintenance you should perform ([at a minimum](#)) to make sure your network stays secure, reliable, and running properly.



Daily Maintenance

Back Up Your Data. One of the most devastating things that can happen to you is losing files, databases, and financial information. The method you use to back up your data will be largely determined by the amount of data you need to back up, but it should be done every day. Ideally, you want to keep an off-site copy of your data in case of fire, theft, or natural disasters.

Update Your Server and Desk Top Anti-Virus. This is critical to protecting your computer network because new threats (and their patches) crop up daily. Most anti-virus software has an automatic update feature that will install updates as they become available. However, it is important to check that your anti-virus is current and functioning every day even if the automatic update feature is turned on.

Check Your Firewall. Just like anti-virus software, you must make sure your firewall is up and running 24-7 to prevent hackers from accessing your system. We recommend checking it daily.

Weekly Maintenance

Check For Operating System Security Packs and Updates. This will protect your computer network from known vulnerabilities and security "loop holes".

Scan and Remove Spyware. Spyware is NOT harmless. Once installed it can make your system run slow, serve up an endless stream of pop up ads, monitor your web surfing habits, steal confidential information about you, and hijack your browser.

Clear Out Old Files. This would include emptying your recycle bin, emptying your "deleted items" folder in your inbox and "sent" messages you don't need, your temporary Internet files, and any programs you are not using.

Monthly Maintenance

Run Scandisk and the Disk Defrag Utility. Scandisk will look for and repair problems on your hard drive. After running Scandisk, run the Disk Defragmenter utility. This will reorganize your hard drive so that applications and programs load and run faster and more efficiently. This should be done on the server and on the desktop machines.

Review System, Application, and Security Logs. Look for errors, problems, or other suspicious and unexpected entries.

Check Memory and Available Disk Space. Simply check to make sure your system has adequate memory installed for the current usage. Also check available disk space.

A recommended amount of free space is at least 25% of the total drive size.

Continued on back page...

Bits N Bytes

Who's Leading Who?

Every morning at about 11:30 AM, the telephone operator in a small town would receive a call from a mysterious man asking for the exact time. This went on for months until one day the operator taking his call summoned the nerve to ask him why he called every day to get the exact time. He explained, "I'm a foreman of the local sawmill. Every day I have to blow the whistle at noon to announce the lunch break. The clock in my office is unreliable and that's why I call you."

"That's really funny," replied the operator, "all this time we've been setting our clock by your whistle!"

Did You Know....

- ◆ It is possible to lead a cow upstairs, but not downstairs!
- ◆ Coca-Cola was originally GREEN!
- ◆ Every day more money is printed for the board game MONOPOLY than by the U.S. Treasury Department.
- ◆ The first couple shown in bed together on prime time television was Fred and Wilma Flintstone.
- ◆ The smartest dogs in order of intelligence are: a Scottish border collie, a Poodle, and then the Golden Retriever. The dumbest dog? An Afghan hound.
- ◆ The Hawaiian alphabet has only 12 letters.
- ◆ A strand of spider web is stronger than a strand of steel of equal diameter.

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

(314) 727-1174

michele@hawkisg.com

www.hawkisg.com

Are You Making These Security Mistakes When Surfing The Web?



Does your computer run slow, act funny, and crash unexpectedly? Do you get a ton of pop-up ads, even when you are not actively surfing the web? Has your browser been "hijacked" and replaced with another unknown browser? If so, your computer is infected with malicious spyware and viruses that can alter your computer, steal your confidential information, and disable the use of your PC.

One big misconception many computer users have about spyware and viruses is that these programs somehow invaded their computer through no action or fault of their own – this is simply not true.

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 when in reality, YOU are unknowingly giving these cyber criminals and devastating programs free access to your computer.

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.

Unfortunately, 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.



Hawk iSolutions Group, Inc.

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

Phone: (314) 727-1174
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.

Computer Maintenance Continued...

Run A Test Restore Of Backed Up Data. In addition to backing up your data every day, you want to test the reliability of your back ups by attempting to restore the data. I can't tell you how many business owners were burned because they THOUGHT they were backing up their system regularly, but later discovered their back ups were corrupt or not working when they needed it most.

Warranty Warnings: Should You Buy An Extended Warranty For Computer Equipment?

Almost every piece of hardware you purchase today comes with some type of manufacturer's warranty, and many resellers are now offering their own extended warranty plans at the check out. Is buying an extended warranty a good idea? It depends on the product you are buying; many products won't earn back the cost of the extended protection. For example, you don't need a \$50 extended warranty on a \$150 printer. But for some items, like a new laptop, the extended protection plan may make sense. Extending the warranty to three years can get you safely through until the next upgrade cycle. When purchasing an extended warranty, be cognizant of the differences between the manufacturers warranty and a 3rd party warranty. The 3rd party warranty may be cheaper, but it may not cover everything that a manufacturers warranty would. Always read the fine print before you purchase an extended warranty.

Phishing? Don't Get Hooked...



Phishing: When a deceptive e-mail arrives that tells you an account (like a bank account or PayPal account) is about to expire and requests that you visit a given web site to update and verify your personal information, pin numbers, usernames, passwords or account numbers. Obviously this is a scam designed to steal your financial information and rob you blind.

Some phishing e-mails are blatantly obvious because they are loaded with misspellings, poor grammar, and suspicious e-mail and web addresses. However, some are very cleverly done and appear to be valid notices from a credit card company or bank. Many will even use the company logo in the message and on the web site.

To make sure you don't fall victim, never respond to ANY email that is asking you to verify or give personal information. If you are unsure, call the company direct to verify the request.