



Hawk iSolutions Group, Inc.

THE HAWK IVIEW

What's
Inside

Save your
Company
From Complete
Disaster
Page 2

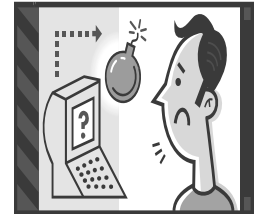
4 web sites to
visit before
you travel

Page 3

Hackers on the
Mac Attack
Page 3



10 Early Warning Signs Of Impending Computer Disasters



Computers rarely stop working overnight. In most cases, there are early warning signs that problems are brewing. Below are 10 surefire signs that you need to get a professional to investigate your network ASAP:

1. Your workstation or server starts running very slowly, freezes up, or crashes.
2. Your web browser has been changed to another strange browser you've never seen before.
3. You are getting an unusual amount of pop-up windows, even when you aren't surfing the web.
4. You don't know if every computer on your network has the most current virus definitions.
5. You don't know if you have a firewall in place or the last time it was updated.
6. You haven't attempted to restore your data from a backup tape or other storage device in awhile, and you aren't checking your backup log for errors.
7. You receive e-mails accusing you of sending spam, and/or you find e-mail messages in your "outbox" or "sent" folder that you didn't send.
8. Your computer starts making a grinding, clicking, or loud whirring sound.
9. The fan is constantly running.
10. You are getting a growing number of error messages, and you are forced to create work-arounds to complete certain work tasks.

If any of these signs are present, you should contact a pro immediately to investigate further!

The old saying of an ounce of prevention is worth a pound of cure is especially true in the world of computers and all things digital; and if you are like most businesses, your computer network is critical to the operation of your business so make sure you don't procrastinate if any of these signs are present.

Ideally, you should perform regular health checks and maintenance on your network to make sure problems don't crop up.

Here's why:

- Critical security updates need to be applied at least once a month to protect you from a constant flow of new hacker attacks.
- Firewall, virus and spyware protection need to be monitored and updated on a daily basis because new attacks are released daily.
- Your data backup system needs to be monitored and tested frequently to ensure easy data recovery in the event of loss. The rate of tape drive failure is 100%; that's why you need to frequently monitor your backups.
- Servers and workstations need regular tune-ups to keep them running fast and error free.
- Monitoring of disk space is important to avoid data loss, crashes, and storage problems.
- Server event logs need to be monitored for early alerts to network issues.

One of the biggest mistakes business

Continued on page 4 . . .



The Simple Document That Could Save Your Company From Complete Disaster!



"Go outside and play, but stay out of the sandbox. You know what that does to your cell phone."

A True Test Of Laziness...



A business owner decided that he had had it once and for all with his lazy employees.

He was sick to death of the ten of them. They wouldn't do what he asked. They sat around at their desks all day staring at their computer screens counting the minutes till they could leave. So he called a meeting at the end of the day, requesting all ten employees to come to his office.

"Ladies and gentleman," the business owner said. "I have the easiest job in the world, custom made for the laziest employee here. I just need to know which one of you that is. Will the laziest employee please step forward?"

Instantly, nine of the ten employees stepped forward.

The business owner looked at the one employee left behind and asked, "Why didn't you take a step forward with your co-workers?"

"Too much trouble," the employee answered.

—Adapted from *The Mammoth Book of Humor*, edited by Geoff Tibballs

Call HiSG for all of your
computer needs!

314-727-1174

We do care!



It's official: End users are the weakest link in the IT security chain. You can set up a firewall, encryption, anti-virus software, and password protection up to your ears, but it won't save you from the employee who posts his access information to a public web site.

Most security breaches, viruses, spyware, and other network problems are a result of human error—an end user unknowingly downloading an infected file, e-mailing confidential information, or disabling their anti-virus, to name a few.

So what is a company to do? While there is no surefire way to keep end users from making mistakes, you can dramatically reduce the number of problems by creating an acceptable use policy (AUP) and training your employees on what is and what is NOT acceptable behavior.

But if you want your employees to actually adhere to your security policies, here are a few tips:

- **Keep it simple.** A long, confusing policy that looks like a legal document is about as easy to read as the instruction manual for your digital camera. Make the policies clear and easy to read. Give examples and include screen shots where necessary.
- **Provide group training.** Many companies make the mistake of distributing their AUP by e-mail and telling employees they must read it on their own. This gives the employees the option of NOT reading and simply signing and submitting. You don't need hours of classroom training but a simple 15 or 20-minute session will force even the most reluctant users to learn a thing or two.
- **Keep employees updated.** To add to the above tip, make sure you update employees on a regular basis to keep the policies fresh in their minds and to educate them about new threats.
- **Explain the consequences of not following the policy.** This is both explaining the negative effects to the business as well as disciplinary actions that will be taken if they refuse to follow policy. Occasional violators should be warned, and habitual violators should be disciplined.
- **Monitor their behavior.** The best policy in the world won't work if it's not enforced. There are many tools on the market that can do this for you automatically.

Need Help In Creating An Acceptable Use Policy and Training Your Staff?

Not only can we help you create a customized acceptable use policy for your staff, but we can also provide training on the topic and even install network monitoring software to make sure it is enforced.

Call us at 314-727-1174 or visit us online
at www.hawkisg.com for more info!



Going On A Trip? Here Are 4 Web Sites You Must Know About



If traveling is part of your work life, you might want to check out information on the following web sites to keep abreast of safety issues.

- **The U.S. Department of Transportation** (www.dot.gov) offers airline, highway and rail safety information. For example, you can look up crash-safety reports on cars or find out how the weather is affecting air travel and road conditions.
- **The Transportation Security Administration** (www.tsa.gov) has advice on safe travel by air, land and sea. For example, they post tips on dealing with airline security checks, traveling with kids, and warnings on prohibited items. Click on "Travelers and Consumers."
- **The U.S. State Department** (www.state.gov/travel) provides information on what to do before, during and when you return from a trip overseas. You can also get warnings on locations to avoid and what to do in an overseas emergency.
- **The Centers for Disease Control and Prevention** (www.cdc.gov/travel) Don't come home sick! This site offers health-related travel information. You can research vaccination requirements, find information on how to avoid illnesses caused by food and water, and review inspection scores on specific cruise ships.



Hackers Are Now Targeting Macs

Until recently, Macintosh computer users have long enjoyed relative freedom from hacker attacks; however, researchers at Symantec Corporation say online criminals are now setting their sites on Mac users.

Online porn hunters are the latest target. Visitors to certain web sites are led to believe they can download a free video player when in fact they are installing malicious code onto their Macs.

Once the users authorize the transaction, the hackers can redirect the users future browsing to fraudulent web sites and possibly steal the user's information or passwords. Sometimes they simply send ads for other pornographic web sites. This results in thousands of dollars in income for the criminals.

While you may think that Macs are essentially more secure than PCs because they are built better, security experts would argue differently. They believe that the Mac is actually no more secure than a PC. In fact, they note that the relatively low number of viruses, exploits and other cyber attacks directed at Mac users is due to Apple's relatively small share of the computer market.

"I don't think that the Mac OS is more secure than Windows – I think it is safer than Windows because there are less people trying to attack it. There is a big difference," Natalie Lambert, a senior analyst at Forrester Research recently shared with MacNewsWorld.

With that said, the fact remains that for every single attack on a Mac, there are at least 100 attacks on Windows-based systems.

So what should you do if you own a Mac? Use the same safe online surfing practices as PC users, keep your anti-virus software up-to-date, never open strange e-mails from unknown sources, and only verify user names and passwords by phone with your bank or other financial institutions.

Windows Server 2003 R2

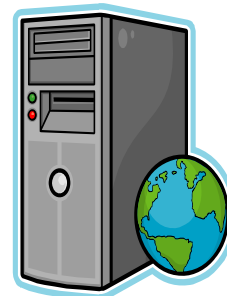
Improve Security and Data protection with Windows Server 2003 R2

The recommended server for supporting mission-critical applications for your midsize business.

Windows Server 2003 R2 helps keep your information technology (IT) systems reliable, manageable, and secure. Built on Windows Server 2003 Service Pack 1 (SP1), Windows Server 2003 R2 easily supports the business processes of your company, no matter what they are. In addition, Windows Server 2003 R2 easily scales to keep you IT infrastructure consistent with your business goals. These additions can be made without causing or scheduling downtime that can interrupt service.

Windows Server 2003 R2 features include:

- Centralized user authentication and increased security management.
- Automatic distribution and installation of updates on desktops and servers.
- Simplified end-user policy management and administrator tasks.
- Streamlined access to external domains.
- Automatic management of network infrastructure.
- Branch office management from a single location.
- Call HiSG for more information—(314) 727-1174





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

IT Solutions...helping build your business!

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.

Continued from page 1 . . .

owners make is taking a reactive approach to network support and maintenance rather than a proactive one.

In other words, they wait until something stops working and THEN they call in the professionals to fix it. This approach not only costs more in the long run, but it also leaves you vulnerable to more devastating crashes such as data corruption and loss, virus attacks, and extended downtime. Even NEW computers and equipment need regular maintenance because new threats are constantly evolving.

Fortunately, there is an inexpensive and easy way for you to completely avoid - even anticipate and prevent - these problems while making your network far more secure, reliable, and problem free.

Hawk iLAN is designed specifically for the small to medium business owner that doesn't have the time, expertise, or staff to perform this regular network maintenance.

Thanks to advancements in support technology, we can now monitor your network 24/7/365 days a year and provide all the maintenance your network needs for a fraction of the time and cost.

For a flat, monthly fee, you'll get 24/7 remote monitoring of your network to not only ensure that it is running at peak performance, but also to guarantee that your data is being backed up and secured, that your virus definitions are up-to-date, that your firewall is configured properly, that your server is optimized, as well as keep an eye on over 100 system processes and alerts that could spell problems brewing.

If you hired a technician - even a junior one - to perform these basic network tasks, it could easily cost you \$40,000 in salary, insurance, and hiring costs. If you were to outsource this type of service, it would easily run you \$800 to \$1,000 a month in hourly, on-site fees. However, thanks to our **Hawk iLAN** service, we can deliver all of these services to you for a fraction of the costs.

To take advantage of this service, contact me, John, at (314) 727-1174 or e-mail me at john.0803@hawkisg.com.



I'd Love To Hear From YOU!

Is there an article or a feature you would like me to include in this newsletter? Do you just want to sound off about something or share your opinion with my other subscribers?

Let me know!

Michele Antone-Gooch
michele.0803@hawkisg.com
314-727-1174