

THE HAWK I VIEW



Hawk iSolutions Group, Inc.

What's
Inside

A Warning To Anyone Working Remotely:

Keylogger Viruses
May Be Stealing
Your Financial
Data, Passwords,
and Other Sensitive
Information!

Do You Make These Mistakes With One Of Your Company's Most Valuable Assets?

Find out on
page 4...

Security Myths

Page 3

Is Your Website Annoying This Particular Group of Visitors?

While Microsoft's Internet Explorer (IE) is still the #1 browser used to navigate the Internet, about 7% of all web surfers currently use Mozilla Firefox. While 7% may not seem like a lot of people, that translates into over 140 million people and growing. As a Microsoft Partner, HiSG does not recommend Firefox, but we do realize it is in use and acknowledge these users.

So why should you be concerned?

Since most websites are designed for IE users, interactive site functions such as shopping carts, calculator tools, surveys, and registration forms may not function properly, and graphics and text may appear scattered or disheveled.

Obviously, error messages, timeouts, and poorly displayed graphics can leave a bad first impression to a prospective customer, and may even prevent them from doing business with you.

Why Firefox is Gaining In Popularity

Mozilla claims that Firefox is far more secure and less susceptible to viruses and spyware. Firefox also has fewer critical flaws, and the flaws that are found are fixed much faster than Internet Explorer.

According to the security firm Secunia*,

a website that monitors vulnerabilities in over 9,500 products, "Microsoft



Internet Explorer 6.x with all vendor patches installed and all vendor workarounds applied, is currently affected by one or more Secunia advisories rated highly critical." *Source www.secunia.com

Should You Redesign Your Website?

If you sell products online, or if you are spending money to promote your website, it is a good idea to make sure your website is both IE and Firefox friendly so you don't prevent Firefox users from making purchases or otherwise interacting with you online.

If you are selling products and services to a highly technical audience, this goes double. According to a recent blog on PC World (www.pcworld.com) almost 20% of their visitors use Firefox.

WARNING: DANGERS OF REMOTE ACCESS YOU MUST KNOW ABOUT!

According to the 2005 American Interactive Consumer Survey conducted by Dieringer Research Group, millions of Americans are fleeing the office to work at home or other remote locations:

- ♦ 45.1 million are working from home.
- ♦ 24.3 million worked at a client's office.
- ♦ 20.6 million worked in their car.
- ♦ 16.3 million connected to the office while on vacation.
- ♦ 15.1 million at a park or outdoor location.
- ♦ 7.8 million while on a train or airplane.

If you are one of the millions remotely accessing your business network, here is a security threat you need to be aware of.

While most remote-access applications such as pcAnywhere and GoToMyPC are relatively secure, the computers hosting those applications may not be.

Cyber criminals are installing *keylogger* viruses on publicly used computers found at schools, libraries, and other business locations to steal passwords, credit card numbers, bank accounts and other personal information.

Keylogger viruses record keystrokes, ICQ/AIM chats, websites visited, and keystrokes entered by the user, and transmit this information to another remote location. This information is then used to steal money, make

unauthorized purchases under your name, and many other illegal and devastating practices.

For example, a man named JuJu Jiang was arrested last year for hijacking the accounts of several GoToMyPC customers by installing a keylogger virus onto a Kinko's computer terminal.

The victim who first noticed this exploit was sitting in front of his home computer and realized it was being controlled remotely. Without touching the keyboard or mouse, he watched as an online account was created using his personal credit card. The victim later recalled using a terminal at the Kinko's where Jiang had installed the keystroke logger.

The only sure way to protect yourself and your company is to give up the convenience of using public PCs for remote access. It is highly recommended that you carry your own laptop when traveling and only use public terminals to access information you don't mind others seeing. Never use them to access your bank account, to make purchases, to log onto a secure company website, or to access personal accounts of any kind.

If you would like more information on how to set up a secure virtual office, contact us at 314-727-1174 or send us an e-mail to michele@hawkisg.com



Notable Quotes...

"Most of the important things in the world have been accomplished by people who have kept on trying when there seemed to be no hope at all."

- Dale Carnegie

"My experience in business has shown me that people who are exceptionally good in business aren't so because of what they know, but because of their insatiable need to know more."

- Michael Gerber

"Expect trouble as an inevitable part of life. When it comes, hold your head high. Look it squarely in the eye and say, 'I will be bigger than you. You cannot defeat me.'"

- Ann Landers

"Everything that is worthwhile in life is scary. Choosing a school, choosing a career, getting married, having kids - all those things are scary. If it is not fearful, it is not worthwhile." - Paul Tornier

"As long as you're going to be thinking anyway. THINK BIG."

- Donald Trump

"Humility does not mean you think less of yourself. It means that you think of yourself less."

- Ken Blanchard

"Argue for your limitations and sure enough they're yours." -

Richard Bach

Dispelling 4 Security Myths

A security guide provides information and resources to secure the operating system and networks with details about the latest vulnerabilities and fixes, articles and technical support. There is a lot at stake in security configuration guidance. In some environments, doing so it is not even an option. A system must be configured in accordance with some security configuration or hardening guide to be compliant with security policy. In other environments, security configuration guidance is strongly encouraged. Before you start making security tweaks, however, we feel that it is very important that you understand some of the fundamental problems with them. These are what we call the myths.

WARNING: Do not lose sight of the message we are trying to get across: These are myths. If you are careful to avoid falling into the trap of believing them, you will be able to focus your efforts on the things that make a real difference instead of being lured like so many others into staring at a single tree and failing to see the security forest.

MYTH 1: *Security Guides Make Your System Secure*

There is nothing that will put you into a “state of security.” Unfortunately, many people (surely none of you readers, though) seem to believe that simply applying some hardening guide to a system will make it secure.

A security guide does not make your system secure. At best it provides an additional bit of security over the other things you have already done, or will already do to the system. At worst it will compromise your security. For instance, a guide may very well compromise the availability portion of the Confidentiality-Integrity-Availability triad by destabilizing the system.

Myth 2: *If We Hide It the Bad Guys Won't Find It*

Generally speaking, renaming or hiding things is much more likely to break applications than it is to actually stop an attack. Competent attackers know that administrators rename things, and go look for the real name first. Poorly written applications assume that the Program Files directory, for instance, is in a particular place, that the Administrator account has a particular name depending on region, and so on. Those applications will now break. Arguably, they were already broken, but the result is that they no longer function.

Myth 3: *The More Tweaks the Better*

Security guides contain a lot of settings, and why not, there are a lot to choose from. Windows Server 2003 contains 140 security settings in the Group Policy interface, and that does not count access control lists (ACL), service configuration, Encrypting File System (EFS) policies, IPsec policies, and so on. The “best” configuration for these environments is nebulous at best. Therefore, a number of people take the approach that if you make more changes you will be more secure.

Myth 4: *Tweaks Are Necessary*

Some people claim that you cannot have a secure (read “protected”) system without making a bunch of tweaks. This is an oversimplification. Tweaks block things you cannot block elsewhere. For instance, if you have two systems on a home network behind a firewall or you have a corporate system that has IPsec policies that only allow it to request and receive information from a few well-managed servers, those systems will probably be safe without making any additional tweaks.

Proper understanding of the threats and realistic mitigation of those threats through a solid network architecture is much more important than most of the security tweaks we turn on in the name of security.





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.

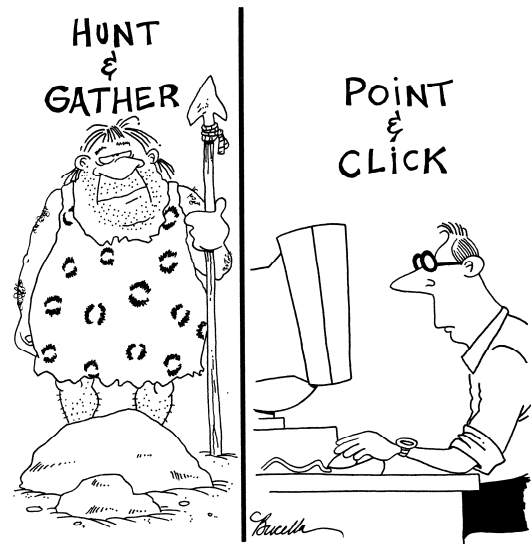
Do You Make These Mistakes With One Of Your Company's Most Valuable Assets?

If you are a small business owner with 5 or more PCs that is concerned about keeping your computer network and data safe from an ever-growing number of threats such as viruses, hackers, spam, spyware, system crashes, hardware failure, data loss, and even employee sabotage - then it's extremely important that you get and read our new special report:

**"What Every Small Business Owner
Must Know About Protecting and Preserving Their
Company's Critical Data and Computer Systems"**

This report will outline in plain, non-technical English common mistakes that many small business owners make with their computer network that cost them thousands in lost sales, productivity, and computer repair bills, as well as an easy, proven way to reduce or completely eliminate the financial expense and frustration of these problems.

This report will also discuss a new service that is helping thousands of small business owners get more speed, better performance, and more life out of their existing technology investments while dramatically lowering the number of frustrations most businesses experience with their computer network. For a limited time, copies of this exclusive report will be made available for FREE on our web site: www.hawkisg.com



The Evolution Of Man

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

Hawk iSolutions Group, Inc.

6439 Plymouth Ave Suite 112 St. Louis, MO 63133

314-727-1174

Michele@hawkisg.com