

THE HAWK IVIEW



Hawk iSolutions Group, Inc.

What's
Inside

Is Your Company
Getting Slandered
On Line?
Page 2

3 Easy Steps To
Get 7 Years Of
Hassle-Free
Service From
Your Printer
Story on page 3

Are You Safe To
Connect To The
Internet Via A
Wi-Fi Hot Spot?
Page 4



Information Technology for Small Business Part II

In the Hawk iView for May 2008, I began a series of articles entitled Information Technology for Small Business by introducing Small Business Server 2008, which Microsoft will be releasing in the second half of 2008. Many of the features of SBS2008 are built on and included in the predecessor product, Small Business Server 2003. The article in May was a general introduction to SBS 2008. This article will be devoted to one of the best features integrated into the Small Business Server: Remote Web Workplace (RWW).

Remote Web Workplace, whether for SBS 2003 or SBS 2008, is one of the favorite features of SBS users. The RWW website is created automatically if the RWW option is selected in the SBS200x installation wizard. RWW is available to all clients that have a valid RWW user account (properly authenticated with a correct password) and a current browser. RWW allows you to connect remotely to your SBS 200x NETWORK from any location using an internet-enabled computer; i.e., all you need is a browser and a connection to the internet.

Using RWW, a user can read their email residing on the SBS Exchange post office, access your office computer desktop, access your server computer desktop (if you are an administrator), view the Help Desk to access a current list of issues for the network, view your company's internal website, view the server usage reports and server performance reports (again, if you have an interest in this administrator responsibility), access company help information, or connect your home or laptop computer to the office network utilizing the Connection Manager.

One of the beauties of the feature is its simplicity in that there is no special software or encryption key to install to establish a Virtual Private Network (VPN) from a PC to the server. When you access RWW from a public PC, your session will end once the browser is closed. The information communicated between the browser and the server is encrypted for security and privacy. When connecting via RWW to a computer in your office, the SBS 200x server does an additional check before connecting you: If the source IP address for RDC connection is not the same as the source IP address for the RWW/SSL connection you've used to authenticate thus far, then it drops the connection - more secure than a simple VPN connection! (*see article on page four*)

To access RWW from the internet, your administrator can provide you with an IP address of your firewall. However, it would be easier to remember a registered domain name used to point to this IP address or an easy-to-remember name registered at one of the "dynamic DNS" web sites. Once presented with the RWW logon page, you simply enter your user ID and password, select your connection speed, and check/uncheck the box "I'm using a public or shared computer" as appropriate. Once your ID and password have passed authentication, you will be presented with a Remote Web Workplace page tailored for the options appropriate for your user ID. For example, if you are an "administrator", you will have the option to access the Server Desktop; if you are not a member of the Administrator group, you will not be presented with that specific option. By the way, if any of these options are not enabled by your administrator, you may not be able to gain access through the firewall.

Continued on page 3 . . .

Is Your Company Getting Slandered Online?

Do You Know What People Are Saying About You Online? New “Online Identity Managers” Are Becoming A Must For Business Owners Who Need To Keep Their Reputation Clean...

A recent front-page story in the Washington Post brought to light a fast-growing trend in today's digital world: online identity management.

According to the article, Sue Scheff, a consultant to parents of troubled teens, was getting slandered online after one of her clients turned on her, calling her “a con and a fraud,” and accusing her of taking kickbacks and destroying people's lives. Negative comments were being posted on online bulletin boards, forums, and threatening videos were posted up on YouTube for the world to see.

Even though Scheff sued for defamation and won an \$11.3 million verdict, the attacks worsened. To resolve this situation, Scheff was forced to hire ReputationDefender, a PR firm that cleaned up her reputation online.

While the costs for hiring this firm were steep (reputation management firms charge \$15,000 to \$100,000 for their services), the cost of her time, litigation and reputation make their fees seem like a drop in the bucket.

So what should you do if you are an average Joe small business with limited resources? Fortunately, an ounce of prevention is worth a pound of cure, and you can easily monitor your image online for free with a few simple steps.

First, the easiest way to check your online reputation is to Google your name or the name of your company and see what appears. Next, set up a Google Alert on your name and your company name. You'll be alerted by e-mail whenever you or your organization has been mentioned in a blog, by the media, or in an online forum.

Next, make sure your web site and your company is coming up first in search engines. If you own the top positions online, negative media may not show up on the first listing when your name is Googled.

To do this, create a profile of your expertise using social bookmarking tools and news aggregators such as del.icio.us and Newsvine. Contribute to online forums and write articles for user-generated content sites such as Squidoo. You can even create book and product reviews at Amazon.com to help establish your authority on a particular topic.

You should also create a free blog on Blogger and then link that to your main web site. Post frequently and make sure your posts are key-word relevant

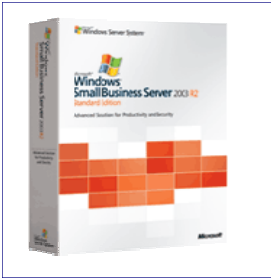
Other obvious ways to put a positive spin online about your company is to create content pages on social media sites such as YouTube, Facebook and MySpace.

Finally, be very careful about posting any incriminating evidence about you or your company online or sending e-mails with incriminating information, tasteless jokes, or messages that could easily be misconstrued out of context.

You don't want a search on your name to bring up pictures of you in compromising situations or sexist, racist, or off-color jokes you thought were only being sent to your friends. If you wouldn't want it posted to a billboard, don't post it or send it via e-mail.

Continued from page one . . .

In addition to these applications integrated into SBS 200x, you can also add your own applications to the list in the Remote Web Workplace. For all of those small businesses who need to survive or even flourish by being nimble, mobile, or provide work flexibility, Small Business Server 2003 and 2008 provide outstanding options. Your communications is easy to install, easy to manage, and protected. Stay tuned for more Information Technology for YOUR Small Business!!



**If Small Business Server 2008 has your attention:
Call John Antone at (314)727-1174 and he will bring out a
new USB Mass Storage Drive -yours free- just for talking
about this exciting new product!
We look forward to hearing from you!!
You can also drop an e-mail to:
John.sbs@hawkisg.com to set up an appointment!**

3 Easy Steps To Get 7 Years Of Hassle-Free Service Out Of Your Laser Printer

Printers - the necessary evil of every office. From paper jams and error messages, to problems like smearing, misfeeds, and ghosting, printers can really make your blood pressure rise.

Plus, it's easy to sink thousands of dollars into maintenance and repairs. If you want to avoid common printer problems AND save yourself a small fortune on replacements and repairs, follow these 3 easy steps:

Keep It Clean

There is no faster way to gunk up a laser printer and cause printing problems than by letting it get dirty.

On a monthly basis, use compressed air to blow out the inside of the printer. Remove the toner cartridge for better access, and don't forget to do the back if it is accessible. It also helps to take a vacuum to the outside. If you print labels or use any other type of specialty media like transparencies, use rubbing alcohol to clean the rollers inside the printer.

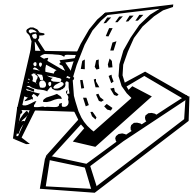
Do Your Maintenance

You can almost infinitely extend your printers lifespan by doing the regular maintenance suggested by the

manufacturer.

This includes replacing rollers, filters, and occasionally replacing

the fuser (the printer's internal furnace.) Here's a little money-saving secret: you only need to do this type of maintenance at 1.5 to 2 times the manufacturer's usage recommendation. In other words, if your printer's manufacturer says to replace rollers every 100,000 pages, you really only need to do so every 150,000 to 200,000 pages.



Use a Surge Protector

Nothing will send your printer to the bone yard faster than an electrical surge caused by lightning or other issues on the power grid.

When internal components are fried, it is often cheaper to buy a new printer than it is to fix the existing one. It is easy to protect yourself with a \$25 surge protector. DO NOT plug a laser printer into a UPS or other battery backup system. The printer's power draw is too much for a battery to handle.



Hawk iSolutions Group, Inc.

Call HiSG for all of your
computer needs!
314-727-1174 * * * We do care!



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

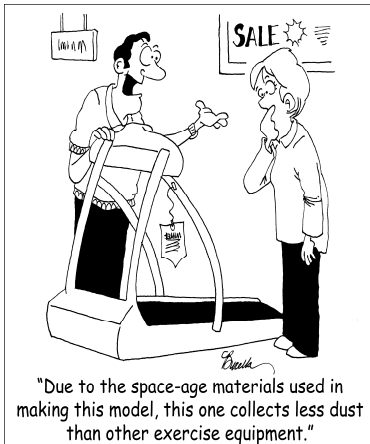
IT Solutions...helping build your business!

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.



You can't beat the convenience of checking e-mail and hopping on the Internet at (Wi-Fi) hotspots found in airports, coffee shops, bookstores, and even in some major parks. For the uninitiated, Wi-Fi hotspots are areas where you can use your wireless laptop to surf the Web and check e-mail.

But the question you have to ask yourself is, just how safe is it to connect? With the proliferation of hackers, viruses and identity theft at an all time high, you are smart to be concerned. Wi-Fi spots are very attractive to hackers because they can use what's called an "evil twin" connection to access your laptop.

An evil twin is a wireless hotspot set up by a hacker to lure people from a nearby, legitimate hotspot. For example, when you log in at your favorite coffee shop, you might actually be logging onto the evil twin Internet connection set up by the innocent-looking person

How To Keep Your Laptop Secure At Wi-Fi Hotspots

working on a laptop at the next table.

The most dangerous evil twins remain invisible and allow you to do business as usual. But in the background, they record everything you are typing. Buy something online and they are recording your credit card information. Log on to your bank account, and they can grab your password. Some hotspots may even feed you a fake Web page after you log on asking you to update your billing information. This is the same tactic used in phishing scams.

So what can you do to make sure you are not giving an evil twin access to your laptop?

First, know the name of the hotspot you're going to use by asking someone who works

there. Some businesses will give you printed instructions that include the hotspot name. Again, be careful. Hackers will try to name their evil twin network by a very similar name as the

real hotspot, and may even show up as a stronger signal.

The best protection you can have is connecting via your company's VPN (virtual private network). A VPN will protect your online information by encrypting your data and activity even if you're connected through an evil twin...Better yet, use SBS 200x! (see article on page one)

If you don't have a company VPN, you should assume that someone is looking over your shoulder and recording everything you type in. Therefore, the BEST protection without a VPN is to never type in information such as credit cards, passwords, or social security numbers when connected to a public Wi-Fi hotspot.

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.0806@hawkisg