

IT Managers Connection

HOME EMAIL ABOUT RSS 2.0 ATOM 1.0

Recent Posts

[Interview] Part4: Barb Bowman - Top Five Tips in Wireless and Devices

[Interview] Part3: Barb Bowman - Top 6 Challenges with Wireless Technology

[Guest Blogger] Riding to the "Surface"

[Interview] Part2: Barb Bowman - Wireless Best Practices

[Interview] Part6: Barb Bowman - Critical Issues for Organizations; IT Pros Making a Difference

Tags

Adam Cole Barnaby Jeans BizTalk Blaine Bey Career Tips **CC Blogged Down** CIPS Collaboration Community David Carbi DJ Dinkley Don Spencer **Downloads** Energize IT **Events** Graham Jones Guest **Bloggers** Industry Perspectives **Interviews** IT Alignment **IT Manager** Interviews IT Manager Podcast Series Jacqueline Hutchinson Jing Chen Use Services Mich Tulloch **MS News** Newsware Partners Podcasts Ruth Morton Sea O'Driscoll Security **Stephen Ibaraki** Tools & Utilities **Training** Val Matson Wireless Technology

News

The postings are provided "AS IS" with no warranties, and confer no rights. You assume all risk for your use.

» Blogs that link here

Technorati

Do you want to receive this blog via email?

10 email readers
BY FEEDBLITZ



Windows Live

Resident Bloggers
Stephen Ibaraki Industry Analyst
FCIPS, I.S.P., DFAPA, CMP, MVP



Ruth Morton IT Pro Advisor
Microsoft Canada

[Interview] Part 2: Barb Bowman - Wireless Best Practices

This is the next blog in the [continuing series](#) of interviews with leading professionals. In this series of blogs, I have an exclusive interview with Barb Bowman. Barb is an internationally acknowledged home networking and device authority; Microsoft Most Valuable Professional (MVP) - Windows Networking and Windows XP Media Center.

Enjoy!

Stephen Ibaraki, [FCIPS](#), [I.S.P.](#), [MVP](#)



Stephen: You have a history with wireless. What best practices would you like to share?

Barb: More and more people are running secure wireless networks at home but totally neglect the very real risks when they travel (or even visit a local Starbucks) and use wireless networks. I'd like to share some recommendations on bolstering security in these environments. If you travel with a laptop and connect wirelessly, you need to take extra precautions. Most public wireless providers and hot spots use no security at all. Everything you send and receive is sent in the clear with no encryption.

- If you use a VPN connection to your office, you will have the protection of an encrypted tunnel. If you can't use a VPN tunnel to your office, consider using a Remote Desktop connection to a computer you've left running at home. You can use Vista Ultimate or Business (32 or 64 bit), Windows XP Professional, Media Center Edition or Tablet PC Edition as a Remote Desktop host machine but not Vista Home Premium or Basic and Windows XP Home. Vista Home Premium, Vista Basic, and Windows XP Home, however, can be used as the remote client.
- If you are going to do this, you really want to use a router/gateway (and honestly, you don't ever want to connect a computer directly to a broadband modem). You'll need to forward port 3389 to this computer (see the router docs). To make this easy to do, get yourself a free domain on www.dyndns.com and get a router that has easy transparent support for DYNDNS.

For details on using dyndns, see:

<http://www.dyndns.com/services/dns/dyndns/howto.html> and <http://www.dyndns.com/services/dns/dyndns/>

- When connecting to a new public network (hotels, municipal, etc.) be sure to specify Public when prompted on any version of Windows Vista.
- Configure the Vista or Windows XP SP2 Firewall to be on with no exceptions. Vista users should also turn off all file and print sharing in the Network and Sharing Center window. If you are using Windows XP Home edition, turn off file and print sharing on your laptop when you travel. If you are using any other version of Windows XP, [turn off Simple File Sharing](#).
- Don't visit any website or use any program that lets you send passwords, account numbers or other sensitive information in the clear. Use SSL connections for email. If you don't know how to configure Outlook Express or other email client for SSL or if your ISP does not support this, it is probably your ISP has a secure SSL based webmail application that you can use. If in doubt and there is a choice for secure or encrypted versus normal or non secure, always select the secure version. SSL sites normally have URL's that begin with <https://>
- Use online banking with care. Most banks offer SSL online access. Read the fine print carefully.
- Only use online merchants who provide a secure SSL site. Internet Explorer and most other browsers will display a padlock icon on the bottom status bar when accessing a SSL secured site.

Look for more with Barb in the next blog.

I encourage you to share your thoughts here on these interviews or send me an e-mail at sibaraki@cips.ca.

Posted: Tuesday, June 19, 2007 8:00 AM by [ednitmgr](#)

Filed under: [Stephen Ibaraki](#), [Interviews](#)

Comments



John Osley Director Community Evangelism
Microsoft Canada



Archives

- June 2007 (12)
- May 2007 (24)
- April 2007 (20)
- March 2007 (14)
- February 2007 (21)
- January 2007 (18)
- December 2006 (4)
- November 2006 (18)
- October 2006 (16)
- September 2006 (23)
- August 2006 (26)
- July 2006 (26)
- June 2006 (36)
- May 2006 (28)
- April 2006 (30)
- March 2006 (38)
- February 2006 (41)
- January 2006 (28)
- December 2005 (28)
- November 2005 (8)
- October 2005 (8)
- September 2005 (2)
- August 2005 (7)

No Comments

Leave a Comment

Title *(required)*

re: [Interview] Part 2: Barb Bowman - Wireless Best Practices

Name *(required)*

Your URL *(optional)*

Comments *(required)*

Remember Me?

Submit

Comment Notification

If you would like to receive an email when updates are made to this post, please register [here](#)

Subscribe to this post's comments using [RSS](#)

