

Free wireless hotspots are popping up all over the place: hotels, airports, restaurants, and even downtown Greenville. Laptops, cell phones and PDA's arrive with connectivity built-in, all you do is click on an available network and you can browse the Internet, send and receive emails, check your stocks, make reservations, etc. Keep in mind though that wi-fi hotspots do not employ any personal security measures, that's right, none. Their SSID, or network ID, is plainly broadcast; there is no encryption - WEP or WPA, and no MAC filtering whatsoever. After all, how would they know who to filter? Let's go over some basic wi-fi precautions that will make your browsing experience more secure as well as some wi-fi limitations. Remember this is not an entire list, due to space limitations, but these are basic guidelines to raise your awareness of how easy it can be to pry into your personal data.

First is email – If your address includes 'Bellsouth', 'Nuvox', or 'Charter' in it, chances are you are going to be able to receive emails but not send them when not at your home base. Why? Because these Internet Service Providers do not use SMTP authentication, they rely on the fact that you are using their physical network lines, DSL or cable, for your Internet connection, thus your network address becomes a part of their internal subnet. Since you are a recognized IP address you are not prompted to login to their mail server before sending your email. ISP's such as Earthlink, Yahoo, Readyhosting, and others do offer an SMTP authorization version of their email products. But *when checking email via a public hotspot it is always much safer to use the webmail interface provided by your ISP.* This involves connecting to the Internet and then logging into the ISP mail server, whether Bellsouth, Nuvox, or Charter, and checking and leaving your mail on their mail server. You can download it to your machine when you return to your home or office. This is the most secure method, since ISPs use SSL (secure socket layer) when granting webmail access.

Evil Twins – For most of us this term conjures up images of a new Stephen King movie, but in the Information Technology world it refers to an illegitimate access point trying to pass itself off as a legitimate one. For example, in one of those rare moments of free time you might be sitting at Panera Bread Company and decide to click on "show all available wireless networks"; the results might be **panera**, **pnera**, **panera1** and **linksys**. Only one of those is the Panera wi-fi network. The others could be hackers sitting within range to get you to connect to their network by mistake so they could see what data is available for looting on your laptop. Wi-fi range is generally around 300 feet so these access points might be in the business or hotel next door, across the street or in the parking lot. *Make sure you know the name of the wi-fi network you want to use*, and change the wireless settings on your laptop to *not* connect automatically to any available wireless network. Also, *turn off 'ad-hoc' mode*, which lets other computers connect to you directly, possibly without your knowing. And for good measure, when finished on the network, just turn off your wireless antenna altogether by locating the physical on/off switch on the side or front of the laptop

File Sharing – Turn it off. There is no need to file share with strangers at the coffee shop or airport unless you just really want to, just remember to turn it back on when you get home.

Personal Firewall – Use one. Windows XP Service Pack 2 has one built in that works just fine. This is opposite of the advice from the home networking piece I wrote last month because at home (or office) you do want to see the other computers on your network, but on a public network you do not. Another reputable free firewall is Zone Alarm, which can be easily downloaded from the Internet.

VPN software – since your physical vulnerability window exists from your machine to the access point, you can also purchase personal Virtual Private Network, or VPN, software to use when connecting in public. JiWire has a good one called Spotlock.

Since many of these settings are opposite to what you are going to use at home, I recommend making a list of settings that need to be changed (for public use) and then changed back (for home use). You might consider doing this simply to be organized and methodical, otherwise it is potentially very easy to start fiddling with different settings and render the wi-fi networking inoperable on a laptop entirely. These are some of the many small steps you can take to secure your public Internet use, and lessen your risk of identity theft and data theft. For more information regarding wi-fi security please contact Carin Slader at cslader@mdserv.com or 864-297-8889.