

# Medical Office Systems, LLC

## April 2010 Newsletter

---

### WiFi Safety at Home and Away

I get a lot of questions about WiFi safety, especially when using a public WiFi hotspot – the local coffeeshop, library, or your hotel. Below are a few guidelines that will help keep you as secure as possible.

Missed or lost a newsletter? You can always get back issues in Adobe PDF format online at my website - [www.MedOfficeSystems.com/newsletter\\_tips.htm](http://www.MedOfficeSystems.com/newsletter_tips.htm). If you have any questions about WiFi safety or networking, please call me at 630-852-1736 or 630-373-7429.

---

### WiFi Safety at Home and Away

Is it safe to surf the internet at a public WiFi hotspot? Millions use public WiFi hotspots daily, so it must be OK, right? The short answer is “Not unless you are careful”. In fact, if you use your laptop in any public area, even if not connected to a hotspot, you may still be vulnerable!

I’ll start by laying out the groundwork of what we are up against, then Page 2 are guidelines on how to safely browse the internet if you use a public hotspot.

#### **Problem #1: Radio Waves**

WiFi is really “Internet over Radio Waves” – in the most basic definition, WiFi substitutes a wired cable for a tiny, short-range radio broadcaster (the hotspot) and receiver (your laptop). Like the original wireless phones in the 400Mhz and 900Mhz band, anyone with a radio capable of tuning those frequencies could listen in to your conversation... same holds true for computers and internet traffic, your data can be intercepted and read.

#### **Problem #2: Control**

Your laptop moves from a home environment (which is controllable) to a public environment over which you have no control. In your home network, you may also have shared folders and printers on your laptop with other computers on your home network.

#### **Problem #3: Unencrypted Data**

Very few people encrypt their sensitive files. Encryption “scrambles” your data by using an “encryption key” (password) to scramble data into random characters. When you later need to use the file, it is unscrambled with the same key, and your data is back to readable form. Encryption is fairly common in corporate environments, but much less so elsewhere. There is one big downside to encryption: if you lose your key, your data is lost, so use with caution.

#### **Problem #4: Unsecured Websites**

Hard to believe, but some websites that should be secure are not, or have weak security. This is not a big deal for just reading the news online, or other non-sensitive recreational surfing activity. But reading your email or any banking or financial transactions must be done in a secure manner. Even recreational surfing isn’t entirely problem-free, if you are concerned about privacy.

OK, now that we have the scope of the potential problems defined, let’s solve them one-by-one...

[continued]

---

Reprint permission granted, provided the following appears on each page:  
Copyright © 2009, Medical Office Systems, L.L.C. - [www.medofficesystems.com](http://www.medofficesystems.com)

Phone: 630-852-1736

[john@medofficesystems.com](mailto:john@medofficesystems.com)

Fax: 630-214-4565

## WiFi Hotspot Guidelines

### At Home:

- Make sure your home WiFi signal has secure WPA or WPA-2 encryption.
  - If your router or laptop can only support WEP, it's time to upgrade your equipment.
  - By default, routers will use the "TKIP" encryption type, it is OK to use, but...
  - If your router and laptop can support the "AES" encryption method, use that instead.
- Make the password (passphrase) complicated
  - ([See February 2010 Issue](#) for Password Tips)
- Be certain that when you connect to a WiFi signal you are connected to is YOUR signal, not your neighbor or someone else's signal.

### At a Public Hotspot:

- Get the hotspot's name from the owner of the hotspot site, and make sure you connect to that signal.
- Keep your WiFi receiver OFF if you're not surfing:
  - Most laptops have a switch or button to turn off the receiver on the side or front.
  - Other laptops have a Function Key sequence such as [Fn]+[F4] that switches the radio on/off.
  - When it's "ON", you are vulnerable if you don't also do the next steps...
- Turn ON your computer's firewall:
  - Many people have firewalls off while at home, but then you're not in Kansas anymore, Toto!
  - Even if the hotspot has a firewall (most don't) you need to protect your PC from everyone else using the same hotspot.
- Turn OFF file and printer sharing:
  - At home you may be sharing your files, but you don't want to share with Mr. or Ms. Hacker down at the coffee shop.
- Encrypt your private data, just in case. [Sophos offers a free encryption tool here](#)
  - Note: encrypt only data files.
  - Make sure you remember the encryption key - or your data is lost.
  - If you do lose your encryption key, you can retrieve your files from your backup copy of data at home... [see October, 2009 newsletter...](#)
- If you need to log in to get email, or absolutely have to do shopping or banking:
  - Make certain that the login page address starts with "[https://](#)"
  - Make certain that the status bar has a padlock icon visible. [Click here for an example.](#)
  - These two items together ensure that at least while you are on the website, your data is encrypted, and while not 100% safe (nothing ever is) it is far safer than non-encrypted websites.
  - If you use Outlook or other email, make sure your email server uses SSL to transmit data.
- If you have a company-issued key card, always use it; your traffic will be encased in a "VPN Tunnel", the safest way to use the Internet.
- Even if you are just browsing for fun, realize that whatever you type may be monitored.
- Use the hotspot sparingly, don't "camp out" all day!

Questions or comments? Call or email me, I'll be happy to discuss questions or provide more details.