



## **Wi-Fi ups and downs.**

**By Gery L. Deer**

**Technology Consultant – Deer Computer Consulting, Ltd.**

Free public wireless internet access, or “Wi-Fi,” is cropping up in retail shops all over the country. Coffee shops, bookstores, movie theatres, and even some local governments now offer free wireless internet connections, or ‘hotspots.’ Hotspots make it convenient to check email and surf the web while taking in your favorite cup of mocha-chocallatta-java.

As with most conveniences, there are also risks involved. Wi-Fi hotspots present a unique kind of set of security issues. Many unknown computers are sharing the same local network. Unlike home or office networks, most public hotspots in hotels and cafes have no ‘log-in’ requirements or address filtering in place to weed out fake access points.

It is relatively easy for someone other than the Wi-Fi host to set up a ‘fake’ access point. It’s important that the user makes certain that the network to which they are connecting is legitimate. So, how can you tell if you’re on a legitimate network?

The easiest way is to look for a sign or other marker that says something like “free Wi-Fi.” When you connect to the hotspot your computer will show the names of which networks are available. If it’s not already posted, an employee for the name of the access point so you know you’re on the proper connection.

Most hotspots require no log in of any kind, but others have a log in screen that requires some type of sign-in procedure. At public libraries and government hotspots, this is done to safeguard users and get data for funding purposes. Retailers, however, may have figured out ways to market to you once you’ve used their ‘free’ wireless.

When you ‘agree to the terms of use’ at the sign on screen of a retailer’s Wi-Fi system, it might be a good idea to read the fine print. If your computer is not well protected, the host computer could be mining information from your documents and other data. If that’s not bad enough, chances are that you are agreeing to let them. Of course if you don’t, then you don’t get to use their service. Here are 10 ways you can secure your computer on Wi-Fi.

1. Make sure you're connected to a legitimate access point.
2. Encrypt files before transferring or emailing them.
3. Use a virtual private network (VPN).
4. Use a personal firewall.
5. Use anti-virus software.
6. Update your operating system regularly.
7. Use Web-based email that employs secure http (https).
8. Turn off file sharing.
9. Password-protect your computer and important files.
10. Check the Internet for known security issues at your favorite spot.

For detailed information or a system review contact Deer Computer Consulting, Ltd. online at [www.deercomputerconsulting.com](http://www.deercomputerconsulting.com) or call (937) 902-4857.