CONNER ASH P.C.
Certified Public Accountants
and Business Consultants

12101 Woodcrest Executive Dr., Ste. 300
St. Louis, MO 63141-5047
Tel: 314-205-2510
Fax: 314-205-2505
www.connerash.com

An independent member of BKR International

WHY NOT FREE PUBLIC Wi-Fi?
By: SUE DETERS

We all use it, we all love it. Why? Because it's FREE! The problem is that it truly does come at a cost. You can be exposing yourself to "the bad guys" with a click of a button. The majority of Public Wi-Fi hotspots are not encrypted. There are a few that will require a password, but who do they give the password to? Everyone!

So what are the hackers looking for? That's the easy question, your personal data. They want your logins, passwords and more.

Hackers have plenty of methods to get your information and they don't have to be a computer genius to do so. They use Snooping or Sniffing tools to track the websites you are going to and can even capture emails and other confidential information. A hacker can setup an "Evil Twin", which is a rogue access point that is made to look like a real one. Once you have connected a hacker can listen to all your internet traffic.

So how do you protect yourself? There are two primary ways:

- First, do not set your devices to automatically connect to Public WiFi. Try to use WiFi that requires a login. This is still not safe, but it is better than being totally open. When on Public WiFi, do not visit sites that require a login that contain confidential information, such as your banking software, Facebook or other social media.
- Purchase a Personal VPN for your system. A Virtual Private Network or VPN encrypts your data and hides the location of your system. There are several good VPN services available including Express VPN and IPVanish. Read the reviews and find the one that fits your need best.

Be wise, stay alert and continue to practice safe computing!