By Jen Sharp, jensharp.com

Wi Fi – Why Fi? The Risk of Using Public Wireless

Jen Sharp holds a real laptop, powered on and working, as she skydives over Osage County, Kansas on Saturday, October 9, 2010. Traveling at 120 mph and at about 8,000 feet, she illustrates the concept of unfettered, no cords, wireless, coupled with risk.

Photo by Emily Reimer, SkyDive Kansas

Technological advances are moving at the speed of freefall! In just a few short years, we have propelled ourselves into an e-connected society, for both work related and social communication. Perhaps I am easily amused, but I still marvel at modern technology, despite its incessant presence in my daily life. Sitting at a sixteen-inch wide assortment of plastic, metal, lithium ion, with light emitting diodes, I am able to search the Web and find some obscure morsel of knowledge originating half way around the world. Yet consumers are insatiable, continually clamoring to be "plugged in," connected to our beloved electronics. Further still, we are now demanding the same stuff, only "unplugged," totally free, unattached. Ironically, as I write this, I am sitting in an airport in Chicago, with my laptop running on batteries, connected to the Internet via public wireless fidelity, unfettered by cords.

This freedom comes with a hitch, however. Using public wi-fi can be risky if you misunderstand its capabilities and limits. By employing a few key guidelines, you can reduce your risk and enjoy this freedom with minimal risk.

Levels of risk

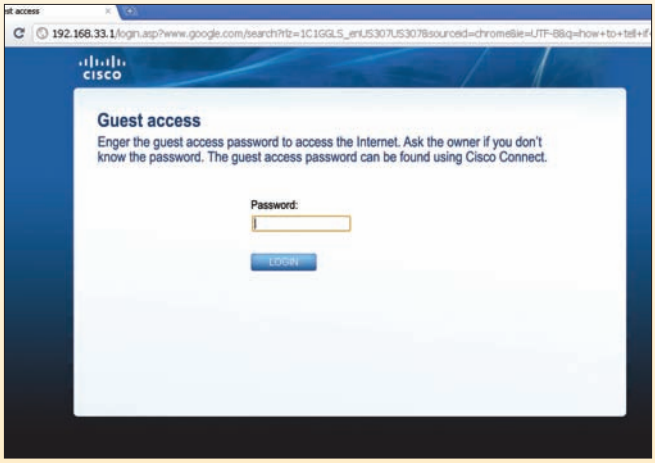
Understanding the way wi-fi works can help you choose your involvement based on the level of risk you are willing to assume. Because information sent over open public wi-fi is not secure, it is transparent, able to be seen by anyone who is logged into the same network.

So, what are our choices here?

1. Go ahead and use public wi-fi

Public, open, non-secured connections are available at wireless hotspots everywhere. Bookstores, restaurants, or other retailers often offer free wi-fi as an enticement for you to feel comfortable, and spend time and money at their establishment. While it is likely safer and more reliable if the network is supported by a chain or well-known company, information sent over these connections read like an open book. Think of it like this: if you would not write it on a postcard, do not send it over public wi-fi.

On some public wi-fi networks, you might even be prompted to enter a password. Do not be fooled into



thinking you are safe just because you do so. This password simply allows you to access the network, either free or for charge, but it does not encrypt any data you might send after you get past the login screen.

You might also see https:// in the URL and think you are safe. Again, this may not be the case. Another user could be on the network and set up a dhcp for you to connect through him; he could then use a password sniffer and capture anything you send. While it is unlikely that someone with this knowledge would target a single individual instead of a business transmitting a large amount sensitive data such as credit card information, it is possible.

In other words, keep your activity on public wi-fi confined to receiving data, not sending it. For example, you can take advantage of googling the Web, watching videos, reading the news, getting the weather… just refrain from logging into any account.

2. Use a Virtual Private Network

If you can use a connection that is entirely encrypted, any data you send over a network would be useless if it was seen. You can do this if you take advantage of a virtual private network, or VPN.

A VPN is just as the name suggests: virtual because it is not a network on its own; it piggybacks off of a public internet connection It is private because it blocks unwanted incoming queries. And of course network is the connection. There are several techniques to achieve this, but in general, you can think of it as a tunnel instead of an open highway. You can purchase and download VPN software online and use it like an application for when you connect to the internet. Nothing you transmit on public wi-fi via VPN would be decipherable.

3. Subscribe to a mobile VPN

For those continually on the go, finding free public wi-fi can be a challenge. Some take their need for e-connection a step further to ensure they are linked. A mobile VPN is a service that appends on an access point referred to as a hotspot. These are simply wireless connections like any other, only with an interface that adds security to all users. For example, T-mobile, Boingo, or AT&T offer service in the form of one time connections or monthly/annual subscriptions. Hotspots are tied to location still, so when choosing a service, it is advisable to research the locations offered to discover if their touted 150,000 locations worldwide happen to be somewhere you frequent.

4. Use a trusted land line

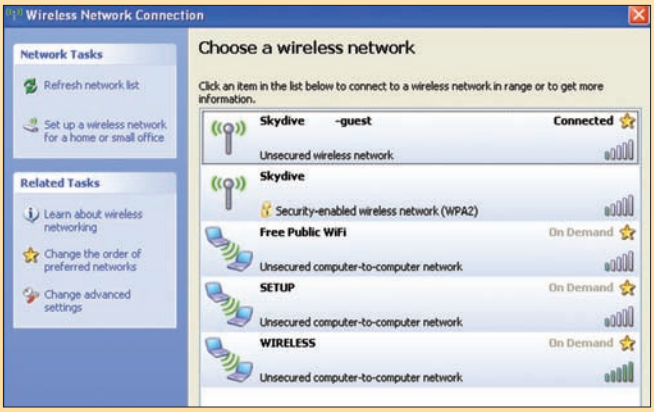
Perhaps the type of information you need to send is sensitive data, such as webmail, bank login, or payments tied to credit card accounts. In those cases, if you cannot utilize encrypted connections, it would be best to find a trusted land line and plug back in.

However, simply because the connection is wired does not make it safer necessarily. For example, if you are on an ISP that uses cable, any data that is not encrypted sent over this subnet can be visible to everyone else on that subnet. So, your neighbors might be able to freely see your information. Again, possible not probable: the users on a cable connection are probably confined geographically and small in number.

Making it secure

In many of our homes, we utilize wireless and set up a connection for multiple computers to reside on a single network. However, even these connections are subject to hacking unless you set up a firewall and use WPA2 security, all available in Windows operating systems.

You can check to see if your connection is secure. At the bottom of the task bar right next to your clock, there is a wireless icon. Right click on it and select “View Available Wireless Networks.”



Or you can also right click and select “Open Network Connections” and look for the lock key icon.

Free VPN software

http://download.cnet.com/hotspot-shield/

Editor's review

This freeware program promises to encrypt all your Internet connections, but since most public wi-fi access points in the U.S. are open, it's a bit hard to gauge Hotspot Shield's effectiveness. However, the connection itself is a bit wonky.

Once the program is installed, it creates an HTML link on your desktop. Double-clicking on it will open the application in your Web browser, and you'll be taken to a page detailing your Connection Status, IP Address, Server Address, Bytes sent and received, and the duration of the connection. Hotspot Shield is ad supported, so you'll get a big banner ad that lives at the top of every Web page, too. Closing the tab with the app's control panel doesn't disconnect the shield, though. For that, or to reload the control panel, you have to go through the green shield icon that gets loaded into your system tray. Also, there's a five GB transfer limit.

Overall, we can't give Hotspot Shield a strong recommendation, but as a last resort it might be worth trying out.

Publisher's description

Hotspot Shield protects you online and lets you access the information you need. Join seven million users in 100+ countries who use Hotspot Shield everyday to: 1) Access blocked services like Facebook, YouTube, Twitter, Skype in countries where Internet is censored; 2) Keep hackers from stealing personal information while users are browsing Internet on public locations like Starbucks; 3) Browse Internet privately. Hotspot Shield is the most stable and the only 100 percent free VPN tool in the world with no bandwidth limit and it does not slow down the Internet speed. Hotspot Shield does all of this without collecting, let alone making use of, any information on your personal identity.

Is it worth the trouble?

As with any risk assessment, you identify red flags that signal for you to pay attention to a particular aspect of the situation. Wherever possible, you reduce those red flags, such as subscribing to a mobile VPN if you want to use webmail, or on the other hand choosing not to participate at that time. In addition, assessing the likelihood of risk is important in making decisions about your participation. Even though it is possible, is it very likely that one person sitting in a coffee shop would be waiting for a single user to enter credit card information so they could steal it? Perhaps you might choose to risk it anyway, citing the example of a more attractive target: one hacker harvested a restaurant's wireless check system and grabbed hundreds of credit numbers in one instance.

Even further, despite efforts to encrypt and secure data, recently it was discovered that anyone on a WPA2 secured network can decrypt other users anyway. (Just google "Hole 196" if you want to amuse and frighten yourself.) Is it worth the trouble?

In my opinion, I would conclude yes, taking precautions ahead of time for the reward of enjoying free access is the best balance.

The bottom line

While using any public network connection, you should always assume the worst case scenario — even if it is not the reality – so you consciously accept what is possible even if unlikely. Fortunately, applying some safety measures can allow you to enjoy the freedom with greatly reduced risk. But the bottom line is, no matter what level of protection you employ, any security system designed by a human being can always be figured out or undone by another sufficiently motivated human being. On the other hand, as Helen Keller suggested, "Life is either a daring adventure, or nothing."

Since 1997, Jen Sharp (JenSharp.com) has served business and government across Kansas and the U.S. and even internationally, specializing in web development, design and programming including e-Learning, ecommerce, content management systems, and other small business solutions. Her work has earned National and International awards: krwa.net won Best Website in 2002 from the National Rural Water Association.