Is Public Wi-Fi Safe?

By Russ McGuire - russ.mcguire@gmail.com

I've just returned from a family vacation on a cruise ship. I've got to confess that being relatively disconnected for an extended period of time was quite unsettling. The ship had Wi-Fi service but it was expensive and slow, when I could even connect to it. So, instead, I resorted to using Public Wi-Fi during our shore excursions – typically at the restaurant where we had lunch.

This experience was eye opening from many perspectives. For starters, it forced me to consider my reliance on 24x7 connectivity – is that a good thing or a bad thing? My second realization was just how ubiquitous Wi-Fi has become.

For example, one of our stops was on the island of Sark. Cars are not allowed on the island. Your transportation options are to walk, bike, take a horse drawn carriage, or ride a tractor. The Sark tourism home page currently includes this quote "The biggest event in Sark's summer calendar took place recently when hundreds of locals and visitors enjoyed the Sheep Racing weekend." Sark is a charming and beautiful place, but I would never represent it as being on the cutting edge of technology. And yet, standing in the middle of Sark's one block long "Avenue", my tablet picked up at least a half dozen Wi-Fi hotspots. Based on the naming of the SSIDs, we chose a restaurant for lunch and asked if we could use their Wi-Fi. They provided the password and I was good to go.

What is Public Wi-Fi?

Although I doubt it with this audience, perhaps I'm being presumptuous in assuming everyone here knows what I mean by "Public Wi-Fi." Just to be sure we're all on the same page; let me take two steps back.

Wi-Fi is a brand that has been established to market products that allow wireless network connectivity using the 802.11 family of standards. There are entire books written about the different flavors of Wi-Fi, but the most common are 802.11b (the version that launched the initial popularity of the standard, providing up to 11Mbps using the 2.4GHz frequency bands), 802.11g (which increased the bandwidth to 54Mbps), and 802.11n (providing up to 450Mbps using both the 2.4GHz and 5GHz bands). Most products are backward compatible, so if you have a mix of devices, 802.11b, 802.11g, and 802.11n, they will generally work together without any concerns.

Wi-Fi was initially intended for use to replace wired LANs in homes and businesses. The expectation was that all users on the network would be trusted. As the Internet revolution kicked in during the second half of the 1990s, and Wi-Fi began to be commonly available, either built into laptops or using a separate card or USB dongle, entrepreneurs saw the opportunity to use Wi-Fi to provide connectivity to the Internet. Thus was born the Public Wi-Fi hotspot.

There are many different models for Public Wi-Fi. Some are free, while some charge by the session, the day, the minute, or the megabyte. Some are open to the public and don't even require a password, while some are just for customers of an establishment (hotel, restaurant, coffee shop, church). Some merely require connecting to the hotspot, while some also require opening your browser to agree to terms of service (and perhaps provide payment information). Whatever the case, connecting is relatively easy and you can be synchronizing e-mail and browsing the web within minutes.

How Does Public Wi-Fi Bring Power to the Kingdom?

The great thing about the widespread availability of Public Wi-Fi hotspots is that you can stay connected most places that you go. One online directory (JiWire) currently lists 580,153 public hotspots in 143 countries (and they don't even show any on the island of Sark). As the Internet has become integral to so much of ministry, this ubiquitous connectivity option can help us use networking technologies to serve the Kingdom anywhere/anytime.

What are the Dangers of Public Wi-Fi?

Of course, Wi-Fi is not without its dangers. A recent story in the news reported on an 18 year sentence handed down to a Minnesota man who had terrorized a neighboring family by hacking into their home Wi-Fi network and gaining access to their e-mail and online accounts. There also have been numerous reports of people being arrested for criminal acts performed by others who accessed the Internet through their unsecured home Wi-Fi networks. Obviously, securing your home, ministry, or business Wi-Fi networks is absolutely critical.

However, the dangers change when we're dealing with Public Wi-Fi hotspots. In this case, we have no control over the security of the wireless network, in fact, the very reality that we can connect to it means that it isn't very secure. Even if you have to provide a password to connect to the hotspot, that doesn't mean that your information is secure as you use these services.

I'd like to call out three specific types of threats.

The first is called a "Man in the Middle" attack. In this case, another user on the wireless network launches a hacking tool to insert their self into the data stream between your computer and the wireless access point. Once they do that, they can see everything you're typing – including your user ids and passwords, and everything that gets sent to your computer, including e-mails and files. This is fairly easy to implement.

The second is called an "Evil Twin" attack. The evil twin is a rogue Wi-Fi access point that is configured to trick users into connecting to it. The users connect to the hotspot thinking they are connecting to a legitimate trusted service, but instead, the hacker can intercept all of their traffic in the same way as the Man in the Middle attack. For example, Joe's Coffee Shop may have a Wi-Fi hotspot with the SSID of "guest." A hacker may establish a rogue hotspot with the SSID "JoesCoffee." Joe's customers connect to the rogue hotspot thinking that it's the one provided by Joe.

In both cases, the simplest advice is to avoid sending any sensitive information while connected to a public hotspot. Whenever possible, use encrypted connections (e.g. the https version of web services such as Gmail and Facebook) so that any hackers intercepting your messages can't easily read your information (including user ids and passwords).

The third type of threat is the potential of getting viruses from public Wi-Fi networks. Hopefully, all Christian Computing readers are already running virus and spyware protection software to protect against these types of attacks, but it's worth thinking about your increased risk of viruses while connected to public networks.

It is my hope and prayer that these articles on the power and danger of technology will encourage you in your daily walk with Christ. Whether it is the printing press, radio, television, personal computers, the Internet, mobility, or Wi-Fi, new technologies continue to advance our ability to know God and to serve Him, wherever we go.

Russ McGuire is an executive for a Fortune 100 company and the founder/co-founder of three technology start-ups. His latest entrepreneurial venture is Hschooler.net (http://hschooler.net), a social network for Christian families (especially homeschoolers) which is being built and run by three homeschooled students under Russ' direction.