Cybersecurity And Public Wi-Fi

Cybercrime is an incredibly popular industry in which criminals seize lucrative opportunities to safely commit their crimes. In many cases, these criminals do not have to even live in the same country as the one where the crime they are committing is taking place.

In previous articles, I've written about how cybercriminals love to target our data, specifically our sensitive information. I've written about how they expertly use social engineering attack tactics to trick us into willfully giving away our data. In this article I want to discuss where we are particularly vulnerable to a cybercriminal's attacks.

With so many places in our digital world where we are vulnerable to a cybercriminal's attacks, perhaps at the top of the list is when we are using public Wi-Fi.

What exactly is Wi-Fi? Simply put, Wi-Fi lets your digital devices communicate with each other and other internet users without a wired connection, all while in one specific area of coverage. Public Wi-Fi is a service provided by a restaurant or a coffee shop or any public place that offers its patrons internet access, often done for free.

Free internet sounds great, but as is the case with most things in the world of cybersecurity and cybercrime, free usually means not very secure. With no need to authenticate to establish a network connection, free Wi-Fi provides an easy opportunity for cybercriminals to access your sensitive information to do any number of things with it, none of which are good.

That being said, you may find yourself in a situation where your only Wi-Fi option is public and unsecured. Even still, you need to take action on a business task now. If such a situation arises, here are some tips to help you with the use of public Wi-Fi:

1. When you are in a public place, don't assume because it says "McDonald's free Wi-Fi" on your phone that you are connecting to McDonald's internet. Many criminals will choose legitimate names to fool you into thinking you are connecting to the right place. Always ask the service provider for the exact spelling of their hotspot name.

2. While using public Wi-Fi, never log into a site that accesses your sensitive information — no health care sites, no banking or financial websites and nothing that requires a password.

3. Use SSL to encrypt your communications when accessing web accounts or email. To do this, make sure the website URLs you visit say HTTPS and not just HTTP.

4. Always use a VPN. Virtual private networks provide even greater protection when accessing a corporate network.

5. Always use a secure wireless provider. They will give you a secret passphrase required to access their service.

6. Disable Wi-Fi auto-connect. Configure your Wi-Fi to connect only to hotspots you select and not automatically to whatever hotspot is available.

7. Turn off Wi-Fi when it's not in use. This will prevent unintended connections.

8. Invest in an unlimited data plan to prevent the need for having to use public Wi-Fi.

Public Wi-Fi is incredibly vulnerable to cyberattacks, as this connection mode streamlines easy access to your sensitive information. In the best interest of your colleagues, your loved ones and even yourself, when it comes to public Wi-Fi, remember the tips from this article and proceed with caution.