Using Public Wi-Fi Safely

Public Wi-Fi networks are convenient if you're on-the-go, especially when travelling or working remotely, but these networks also pose a huge security risk. Why?

Information you send over a public Wi-Fi network can be seen by anyone on the network who knows his or her way around computers. In fact, it's actually quite easy for hackers to track your activity and steal your information if they are connected to the same network. They may even have the tools and software to remotely access your personal devices! So you need to take precautions when connected to Wi-Fi.

What hackers can do

- **Set up an evil twin.** An *evil twin* is what information security professionals call a *rogue access point*, that is, a wireless access point set up without a network administrator's consent.

  Here's how it works. Let's say you're at a hotel that has a Wi-Fi network called, "Hotel Guest." A hacker could easily set up a wireless hotspot from his or her device and give it the same name. Then, if you try to access the real Hotel Guest network, you could instead get connected to the hacker's access point or evil twin, allowing the hacker to view all of the information you send over the network.
- **Launch a man-in-the-middle attack (MITM) attack.** An MITM is another tactic used to access and steal personal information. Using a traffic sniffer to analyze all the traffic that comes through his or her evil twin, a cyber criminal can intercept the data transmitted between you and the server with which you are communicating.

  For example, if you go to Amazon.com on a hotel's Wi-Fi, a hacker deploying an MITM attack can intercept, read, and even alter information sent between you and the Amazon server. If you input your credit card number to make an Amazon purchase, the *middle man* (i.e., the hacker) can redirect your payment to a fictitious site designed to look like Amazon.com. In short, when the payment is processed, the money goes to the hacker instead of Amazon!
- **Deploy wireless traffic sniffers** such as Wireshark and Microsoft Message Analyzer. These programs capture traffic passed over a network and are often used in conjunction with evil twins and MITM attacks. Sniffers enable hackers to read any unencrypted data sent over the public Wi-Fi network, including usernames, passwords, credit card numbers, banking information, e-mails, sensitive or proprietary work-related information, and more.

Mobile devices are also at risk
The risks described above also apply to mobile devices. When you are connected to a public Wi-Fi network, cyber criminals can monitor data and information sent and received through the applications you use—even if you're not actively using an app.

For example, if your Gmail e-mail app is set to autosync with its mail server, it frequently communicates with the Gmail server to obtain new messages. Anything passed during those exchanges could be seen by a cyber criminal who is sniffing your activity, regardless of whether the app is open on your mobile device!

3 tips for using Wi-Fi safely
Despite the risks, it may not be feasible for you to avoid connecting to public Wi-Fi networks, so here are three tips for accessing these networks more safely:

1. ***Always* connect to a Wi-Fi network through a virtual private network (VPN).** This way, your communications will be sent through a secure, encrypted tunnel over the network and be safe from hackers' prying eyes. Remember, you may believe that a Wi-Fi network is secure because it is password protected, but this isn't true.
2. **Disable autoconnect for Wi-Fi so that your device won't automatically connect to it.** This will prevent you from connecting to rogue access points, which in turn will protect you from sniffer tools.
3. **Keep your operating systems, software, and apps up to date.** Outdated systems and software leave you vulnerable to hackers because savvy criminals have ways to exploit security holes. Keeping your browser current may prevent you from being redirected to fictitious phishing sites designed to look like trusted sites.

Think twice the next time you connect to public Wi-Fi. For personal devices, consider a personal VPN* for use on your computing and mobile devices to secure your data over any network.

Questions?
If you have any questions about the information shared here, please feel free to call me at **610-280-9330.**

Sincerely,
Steven M. Seide, CFP®, AIF®

The views expressed are those of the individual authors and may not reflect the views and policies of Commonwealth Financial Network® or our firm.