**Public Wi-Fi – Should Lawyers Just Say No?**

Mark Bassingthwaighte, Esq.

mbass@alpsinsurance.com

 In today’s world, people frequently work outside of their offices. They may be working while visiting a coffee shop, sitting at an airport, staying at a hotel, or enjoying a city park. Public Wi-Fi networks are seemingly everywhere, but there’s a problem. While accessing public Wi-Fi can be convenient when all you want to do is buy something on Amazon, check your e-mail, or rebook a flight, there are associated risks that should never be minimized, or heaven forbid, dismissed out-of-hand. Unfortunately for lawyers, the risks are even more concerning given the sensitive nature of the information they handle.

 Public Wi-Fi networks are inherently insecure. Unlike private, encrypted networks, public Wi-Fi often lacks robust security protocols, making it a prime target for cybercriminals. To give you an idea of the seriousness of the risk. Here are a few specific threats everyone faces when connecting to unsecured networks:

* **Man-in-the-Middle Attacks:** This is one of the most common threats on public Wi-Fi networks. In this type of attack, a cybercriminal intercepts the communication between your device and the Wi-Fi network, allowing him to access sensitive information such as login credentials, emails, and the stored data on your drive.
* **Malicious Hotspots:** Cybercriminals can set up rogue Wi-Fi networks that mimic legitimate ones but are actually designed to enable a cybercriminal to capture your data. If you fall prey to this type of attack by unwittingly connecting to a rogue network, your data stream will be going directly into a cybercriminal’s hands.
* **Rogue Access Points:** A rogue access point is something well-meaning employees of various businesses sometimes set up. In short, wireless routers are added to a Wi-Fi network in order to give more customers access to the Internet. Often these routers are not configured properly, which makes them easy to hack into, even though the network itself might be secure. If you unknowingly happen to use a rogue access point to connect to the Internet, you are now vulnerable to a wide variety of cyberattacks.
* **Computer Worms and Other Malware Injections:** Computer worms self-propagate and can be programmed to do all kinds of things to include stealing documents, capturing passwords, and spreading ransomware. If you happen to be on a public Wi-Fi network and fail to have robust security in place, a worm could readily jump from another infected user currently on the network to you. And it’s not just worms you need to worry about. Public Wi-Fi can serve as a conduit for a variety of malware attacks. If a cybercriminal gains access to a shared network, she may distribute malicious software that can infect your devices potentially resulting in a data breach, ransomware attack, or unauthorized remote access.
* **Packet Sniffing**: Packet sniffing is a technique used by cybercriminals to capture and analyze data packets traveling over a network. On an unprotected public Wi-Fi network, packet sniffing tools can be used to monitor and capture sensitive information, such as passwords and financial data.

Starting to get the picture? I hope so. Again, public Wi-Fi networks are inherently insecure. That’s just the way it is. Does this mean lawyers and those who work for them should never access public Wi-Fi? In a perfect world, I might try to argue that one; but I can also acknowledge this wouldn’t be realistic. There are going to be times when it’s necessary; and truth be told, I occasionally use public Wi-Fi myself, but only for certain tasks. The better question is if you have a need to use public Wi-Fi, how can you responsibly address the associated risks? Start with the following:

* **Approach All Public Wi-Fi Networks with a Healthy Level of Distrust -** Never connect to an unknown network, particularly if the connection is offered for free or states that no password is necessary. Also, be on the lookout for network names that are similar to the name of the local venue offering a Wi-Fi connection. Just because a network connection that happens to be named Free Hilton Wi-Fi doesn’t mean it’s actually the legitimate Hilton network. If you’re not 100% certain, always ask what the proper name of the local network you are wanting to connect to is and connect to that.
* **Use a Virtual Private Network (VPN) -** A VPN encrypts internet traffic, making it unreadable to cybercriminals on public Wi-Fi. You should always connect to a trusted VPN before accessing sensitive information. If your firm provides a corporate VPN solution, use it! If not, use a personal VPN service like [NordVPN](https://nordvpn.com/), [ExpressVPN](https://www.expressvpn.com/), or [ProtonVPN](https://protonvpn.com/).
* **Enable Two-Factor Authentication (2FA) on All Accounts -** 2FA adds an extra layer of security by requiring a secondary verification method (such as a text message code or authentication app) to access accounts. Even if cybercriminals obtain login credentials, they won’t be able to access protected accounts without the second authentication factor.
* **Avoid Accessing Sensitive Data on Public Wi-Fi -** Whenever possible, avoid logging into case management systems, email accounts, or other sensitive applications while on public Wi-Fi. If urgent access is needed, a VPN should be used to secure the connection.
* **Better Yet, Use Mobile Hotspots Instead of Public Wi-Fi:** A safer alternative to public Wi-Fi is using a mobile hotspot from a smartphone or a dedicated cellular hotspot device. These connections are generally encrypted and far more secure than public networks.
* **Disable Auto Connect to Wi-Fi Networks:** When auto connect is enabled, your device can automatically connect to a malicious network. To prevent this unintentional result from ever occurring keep this setting disabled at all times.
* **Keep Software and Security Patches Updated:** Cybercriminals often exploit vulnerabilities in outdated software. Regularly update your operating systems, web browsers, and security applications to ensure you have the latest security patches. Enabling any automatic update features will help make this process as painless as possible.

 I wish I could stop here but I can’t, because almost every law firm I know of is comprised of more than one person. Anyone at a firm can naively or unwittingly fall prey to a cybercriminal when logging onto a public Wi-Fi network and this could result in very serious and unintended consequences not only for your firm, but firm clients as well. Best practices now mandate that everyone who uses a mobile device for work be subject to a written policy regarding the appropriate use of public Wi-Fi. If your firm has no such policy, now’s the time. Of course, any policy is going to be meaningless if there is no training on the risks and/or no enforcement of the provisions so keep that in mind.

 Now to my initial question. Should lawyers just say no to the use of public Wi-Fi or try to prohibit anyone in their employ from using it? I don’t necessarily go that far as long as all users have been made aware of the risks and given the appropriate tools that will help them minimize the risks.

 That said, let me share one final thought because I do get push back on this topic and can anticipate you will too. Some will disagree and say something along these lines, “the Starbucks signal is free, I’ve used it many times before and never had a problem so why all the unnecessary fuss?” My response is always the same. How do you know you were never a victim? No one is going to send you a thank you card for allowing them to steal your credit card number or place a keylogger on your laptop. We all need to understand that hacking tools are widely available to the masses. Always remember that you are never alone while using public Wi-Fi and you simply have no way of knowing what everyone else’s intentions are.

Mark Bassingthwaighte, Esq. Is the resident Risk Manager at ALPS Insurance. To learn more about how ALPS can support your solo or small firm visit: [alpsinsurance.com](https://www.alpsinsurance.com/resources/risk-management?utm_campaign=Bar%20Program%20Asset%20Tracking&utm_source=All_bar&utm_medium=referral&utm_term=q2_rm_articles_2025&utm_content=rm_resources)