How Lawyers Can Connect to Public Wi-Fi Safely

by Sharon D. Nelson, Esq. and John W. Simek

Most lawyers know they are ethically bound to protect confidential data when using their smartphones, laptops, etc. when connecting to public Wi-Fi. It is time for a refresher course.

We were wrapped in a COVID cocoon for a while. Now we are traveling more often, for work or vacation. We're connecting from airports, hotels or conferences. Many lawyers have returned to previous daily patterns of working from their favorite coffee shop.

It appears we have forgotten much of what we used to know about public Wi-Fi and security. 'Public' means they're open for anyone to use – as you might expect, data being transferred isn't as secure as it would be on your home network and WAY less secure than it would be on your law firm network.

Be wary of public Wi-Fi. Don't unwittingly give login credentials, passwords, bank information and other personal data over public Wi-Fi. Be wary of accessing or transmitting confidential communications.

Why? The network itself could be insecure. Worse yet, and this happens more than you might think, a malicious hacker is on the same network and is harvesting data entered by others.

Safety steps while using public Wi-Fi:

Make sure you are connecting to a legitimate network. You might be in an airport or hotel and you see a name suggestive of where you are. "Free Airport Wi-Fi" at an airport might look legitimate but it could be a network set up by a cybercriminal. With the right tools, whoever is running that fake network can see what information is being entered, leading to the data being stolen.

Some networks will require you to set up a password to use the Wi-Fi. If so, don't use the same password you use for **any** other account – particularly if that password is tied to your email address. By doing this, even though your password is somehow compromised, it isn't one that can be used to access any of your other accounts linked to your email address. While you’re at it, if you have to use an email address, use a disposable address.

Think about what data you’re sharing on public Wi-Fi networks. You should avoid using them if you need to do anything that involves sharing sensitive information, such as usernames, passwords, banking information, etc.

Once you’re through using a network, for heaven’s sake, choose to forget the network. Say, for instance, that you connect to a coffee shop that has multiple locations. Forget the network every time. If your device allows it, configure it not to reconnect to previously used networks automatically. Automatically reconnecting to a network makes it easy to become a victim of a man-in-the-middle (MITM) attack.

Sometimes, using Wi-Fi on a public network can’t be avoided. But even if you’re certain that the network is legitimate and safe to use, there’s still an additional step you can take to help keep your information secure – use a virtual private network (VPN).

VPNs provide two key services to keep your information private and secure. First, they encrypt your data (with your own encryption key) – that’s useful on public Wi-Fi networks as they’re mostly unencrypted. By using a VPN, it makes it difficult for the network operator – or anyone who could be trying to use that network maliciously – to see what information you send and receive.

Second, they can also conceal your originating IP address, hiding where you’re geographically located – important for those who need online privacy.

Even taking precautions, connecting to a public Wi-Fi network carries at least a small risk. But there’s a much more desirable alternative to connecting to public Wi-Fi – use your smartphone.

If you’re connecting to the internet on your smartphone, it’s already encrypting the data between your device and the cellular carrier. But if you want to connect your laptop to the internet, you can turn your smartphone into a Wi-Fi hotspot. That is our choice when traveling.

If you choose to utilize a hotspot, make sure the connection is secured with a complex password. May you travel safely – and ethically!

Sharon D. Nelson *is a practicing attorney and the president of Sensei Enterprises, Inc. She is a past president of the Virginia State Bar, the Fairfax Bar Association and the Fairfax Law Foundation. She is a co-author of 18 books published by the ABA.* *snelson@senseient.com*

John W. Simek *is vice president of Sensei Enterprises, Inc. He is a Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH) and a nationally known expert in digital forensics. He and Sharon provide legal technology, cybersecurity and digital forensics services from their Fairfax, Virginia firm.* *jsimek@senseient.com.*