NJSBA PRACTICEHQ Affinity CONSULTING

WIRELESS ENCRYPTION

ROBUST AND SECURE WIFI

It's hard to believe WiFi has existed for over 20 years. We all learned the value of reliable in-home internet over the last couple of years. Perhaps you found that what satisfied the "Netflix need" didn't satisfy work-from-home. Two new technologies are here to make home WiFi better.

The first is "mesh networking." Traditionally, you had a single wireless signal from one point in your home, usually next to, or even built into, your router. The further you got from that point, the slower or less reliable your connection became until it dropped entirely. Mesh networks replace that single broadcast point with multiple points, which seamlessly blanket your house with a single WiFi network. These systems are sold in two and three packs and come with software to help you place each relay box, called a "node," at the right spot in your house.

The second feature is "WiFi 6", the sixth generation of wireless networking. WiFi 6 is up to 250% faster than your existing wireless setup, supports 50+ simultaneous device connections, which is great for small and mid-sized firms, and enables the latest wireless connection security, known as WPA3. I recently installed a mesh WiFi 6 system in my home, the eero 6 Pro (https://eero.com/shop/eero-pro-6), and have been very happy with it.

HOME OR WORK WIRELESS CONNECTIONS

If you rely on a wireless Internet connection at your office or home to work with sensitive client information, your wireless router or access point must be properly encrypted. If you set it up yourself and aren't sure, then you should immediately secure expert assistance to ensure that your security is properly configured. Sometimes, it's as easy as calling the technical support line for the manufacturer of your router. The big companies that sell wireless routers all have technical support representatives that can walk you through the process over the phone. In case you're wondering, big names in wireless routers include eero (https://eero.com), TP-Link (https://www.tp-link.com/us/), D-Link (https://us.dlink.com/en/consumer), and Synology (https://www.synology.com/en-us).

RISK OF USING PUBLIC WIFI

First of all, you need to be educated about this subject. For a quick primer, here are two short articles that will bring this issue into focus: Here's what an eavesdropper sees when you use an unsecured Wi-Fi hotspot by Eric Geier (see https://www.pcworld.com/article/2043095/heres-what-an-eavesdropper-sees-when-you-use-an-unsecured-wi-fi-hotspot.html), and What Is A Packet Sniffer? by Andy O'Donnell (see https://www.lifewire.com/what-is-a-packet-sniffer-2487312). For an interesting discussion of this in the legal arena, see the now famous California Formal Opinion No. 2010-179 which states:

> "With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, **Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall.** Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible

waiver of attorney-client privilege or work product protections, and seek her informed consent to do so."[1]

HOW TO PROTECT YOURSELF

CELLPHONE WIFI HOTSPOT

Rather than connecting to the public WiFi where ever you are, consider using a cellular hotspot or MiFi. Properly configured, these connections are a secure way to connect your notebook or tablet to the Internet via the phone hotspot.

CONSUMER VPN SERVICES

There are many services that allow you to create a Virtual Private Network connection even though you're using a public and otherwise unsecured WiFi connection. "In the simplest terms, a VPN creates a secure, encrypted connection between your computer and the VPN's server. This tunnel makes you part of the company's network as if you are physically sitting in the office, hence the name. While connected to the VPN, all your network traffic passes through this protected tunnel, and no one in between can see what you are up to. A consumer VPN service does the same thing, but extends that protection to the public."[2] Here are some options for this:

- CyberGhost: http://www.cyberghostvpn.com/en_us
- Encrypt.me: https://www.encrypt.me/
- ExpressVPN: https://www.expressvpn.com
- IPVanish: https://www.ipvanish.com/
- NordVPN: https://nordvpn.com/
- Private Internet Access: https://www.privateinternetaccess.com/
- ProtonVPN: https://protonvpn.com
- SurfShark: https://surfshark.com
- TunnelBear: https://www.tunnelbear.com

FIREWALL

WHAT IS A FIREWALL?

A firewall is a network security system designed to prevent unauthorized access to or from a private network. Firewalls can be hardware, software, or a combination of both.[3]

YOUR OBLIGATION

You need to ensure that a firewall is in place at your office and anywhere you use your computer and connect to the Internet. You can test yourself using services like ShieldsUP![4] or HackerWatch[5]. If you aren't sure if you are being protected, then you should contact a security expert to conduct a penetration test. Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.[6]

---

[1] See https://www.calbar.ca.gov/Portals/0/documents/ethics/Opinions/2010-179-Interim-No-08-0002-PAW.pdf, emphasis added.

[2] The Best VPN Services for 2016, by Max Eddy, Fahmida Rashid, 3/9/2016, PCMag - see https://www.pcmag.com/picks/the-best-vpn-services.

[3] See http://www.webopedia.com/TERM/F/firewall.html.

[4] See https://www.grc.com/x/ne.dll?bh0bkyd2.

[5] See http://www.hackerwatch.org/probe/

[6] See https://en.wikipedia.org/wiki/Penetration_test