IN BRIEF

September 2015
Issue 126

OSB Professional Liability Fund

www.osbplf.org

Malpractice Prevention Education for Oregon Lawyers

Decreasing Your Vulnerability While Using Public Wi-Fi

This article was originally published on Lawyerist.com

Let's face it. We all tell ourselves a lot of lies about public wi-fi services. We have to, because using the wi-fi at the coffee shop or library or Target (really, Target!) is just too easy and far cheaper than using our cellphone's data plan, which is basically digital highway robbery. So we say things like "There is a password on this public wi-fi, so it is safe" or "I won't ever check my bank account when I'm at Starbucks, so it's all good."

Unfortunately, the truth is that public wi-fi services are shockingly unsafe. This is especially relevant to lawyers, since you may be accessing confidential data while on public wi-fi. Put simply, you are not living up to your ethical obligations to clients if you are exposing their data to public wi-fi.

For the most terrifying wi-fi hacking scenario, just take a look at Matter's recent piece, (https://medium.com/matter/heres-why-public-wifi-is-a-public-health-hazard-dd5b8dcb55e6), in which they let a hacker loose in some Amsterdam cafes. The self-styled ethical hacker is armed with a $85 box (likely the WiFi Pineapple) that can do two things: (1) redirect all Internet traffic to his devices; and (2) broadcast his own wi-fi network name that is similar enough to the real one (think "Starbucks Guest" instead of "Starbucks").

Install easily available software to that device, and the melodiously named Dutch hacker Wouter Slotboom is able to see where people vacationed, what airline they flew on last, what apps they are using, the model of their devices, what websites people are currently visiting, and, of course, usernames and passwords.

I will be honest: I initially reacted to that article with skepticism. I certainly believed that level of hacking was possible, but not in the sort of off-the-shelf way the article implied. Put another way, I figured you needed to be an elite ninja hacker to get at the sort of data the article was talking about (and also needed to buy a WiFi Pineapple). Then I sat down with Lawyerist's Sam Glover.

Sam spent about five minutes Googling things, then cut and pasted some commands into the Terminal app on his MacBook. (On a Windows machine, this might be a bit more arduous thanks to the lack of a built-in command-line utility controlling a UNIX operating system.) In just a few minutes, Sam was able to see the websites I was visiting, the packets of information being transferred, and more. Sam assures me he is not an elite ninja hacker, just a savvy Google user. He also did not have the WiFi Pineapple or any other similar device at his disposal. The most cursory search turns up entire websites devoted to "testing" networks, where "testing" means "breaking into" or "hijacking entirely."

Hopefully, you are now completely apprehensive about using public wi-fi. Since you are still going to use it next time you are at a coffee shop, what should you be doing to keep yourself safe? There are a few approaches.

One way to decrease your vulnerability on public wi-fi is to engage in piecemeal security measures. These are in no way comprehensive but are relatively easy tweaks if you are feeling lazy about security.

Check Your Wi-Fi Hotspot

First, make sure that you are connecting to your intended wi-fi hotspot. Ask your barista what the network name is. In Settings, turn off the feature on your smartphone or computer that connects it automatically to known networks. This allows you to reconnect manually each time so that you aren't connecting to a spoofed wi-fi hotspot automatically. This helps thwart the man-in-the-middle attacks deployed via WiFi Pineapple or other similar tools.

Almost all wi-fi devices – your phone, tablet, PC, whatever – broadcast a signal looking for previously accessed networks (SSIDs in network speak). With a positive response, a "Yes, I'm the network you're looking for," the requesting client automatically connects. Of course, this auto-connection only works if (a) the network is open with no password, or (b) your device has previously saved the correct network password. But for public hotspots like "Denver-Airport," "Roadside-Inn," or "Tech-Conference-2014" that you've previously used, a rogue "yes man" . . . is happy to reply with whatever network name you're looking for, sharing you into its man-in-the-middle attack. The PC or smartphone appears to be connected to the familiar airport, motel, or café wi-fi, but in actuality, the connection routes through an impersonator collecting all your data before routing traffic onto your intended destination.

Use Secure Websites

Next, whenever possible, use SSL-encrypted sites. You can tell if a site is SSL-encrypted because it will have the https prefix rather than the unsecure http prefix. Most browsers will also show a lock or shield icon by the URL of SSL-encrypted websites.

Mercifully, services like Gmail, Facebook, your bank, shopping sites, and even Lawyerist are already using https encryption. Google has actually called for web-wide https encryption, and the Electronic Frontier Foundation has created a handy browser extension that will force sites to use https on many occasions.

Use Appropriate Network Permissions

If you are running a Windows machine, use the built-in network location tools and always treat anything that is not your home or work network as an unsecure public network. Doing so will turn off network discovery and deny access to your HomeGroup. There is no built-in equivalent on Mac, but Lifehacker recommends Control Plane for performing similar tasks.

Use Virtual Private Networks

Instead of adopting the piecemeal approach of turning your network discovery on and off, reflexively checking your menu bar to make sure you are using https, and being annoyed that you have now set your devices to forget all wireless networks, you could just use a virtual private network (VPN).

Using a VPN creates a secure private network that requires your computer to exchange encrypted and authenticated information with a known and trusted network before you hop on that coffee shop wi-fi. Once you do that, the VPN helpfully scrambles your data while you are on that public connection. A number of great tools exist to make using a VPN seamless.

Cloak. If you are fully invested in the Mac ecosystem, you cannot do better than Cloak. Cloak runs on Macs, iPads, and iPhones, and will sync your data across all your devices. Cloak automatically figures out if you are on an unsecure connection and secures it. It takes about five minutes per device to set up, and once you are set up, one click secures any network. You can also tell Cloak which networks are secure (like your home or work network) so that it always treats that network as trusted.

You can try Cloak for free for 30 days. I highly recommend doing so, particularly as they just let you sign up for 30 days rather than collecting credit card info that you later need to remember to cancel. If you decide you want to keep it, there is a mini plan that will secure 5GB of traffic per month for $2.99, which should be plenty for your coffee shop surfing. If you go full road warrior and want unlimited data security (or decide you want to run a full-time VPN at home via Cloak), it will cost $9.99 per month.

TunnelBear. If you are using Windows or a combination of iDevices and other operating systems, there are a number of choices. TunnelBear is highly recommended and is actually cheaper than Cloak (and has an always-free option with a small amount of data per month if you only do minimal public network surfing). Whereas Cloak markets itself primarily as a security solution, TunnelBear advertises itself as a way to overcome access restrictions. Many Internet destinations are blocked to users of certain countries, and a VPN like TunnelBear allows you to overcome that problem.

PrivateInternetAccess. Forbes recommends PrivateInternetAccess, which is so committed to privacy that you can pay anonymously with a number of gift cards instead of a credit card or PayPal.

Whichever provider you choose (and there are many), the VPN option is both more seamless and more secure than the piecemeal approach – but it does cost money. However, if you want functionally to automate security for your client data when you are out and about, it is a relatively small price to pay.

Lisa Needham
Editor-in-Chief of Bitter Lawyer and Bitter Empire

Reprinted with permission.