Wireless Network Security When On the Road

By Martin Felsky

Second edition, January 17, 2014

Table of Contents

Introduction

Judges working on draft judgments or communicating with colleagues about cases are creating and transmitting sensitive judicial information and in all cases, the same safeguards that would apply to protect that information in the hands of court administration should apply when traveling.

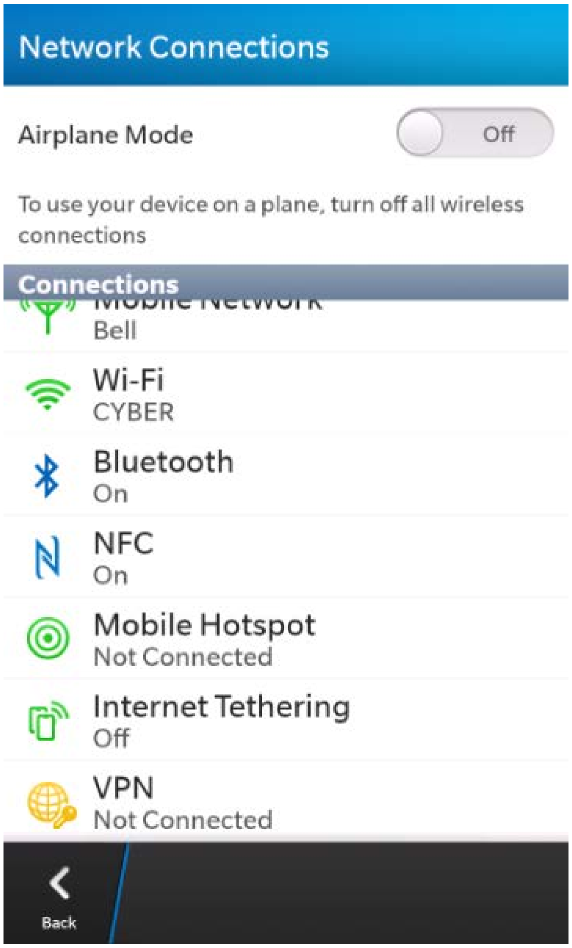
This article is designed to address wireless networking security issues in a practical and plain-language manner. Taking the easy, free and common sense steps outlined below will make your mobile communications reasonably secure against unauthorized access. Be aware that even with all the recommended best practices in place, your web browsing activities and e-mail content cannot be 100% secure. For that reason, all sensitive data should be encrypted during transmission, using either a Virtual Private Network (VPN) or SSL encryption.

Using Wireless Internet On The Road

Many judges are concerned that wireless networking may not be very secure – but lack the technical knowledge to make a proper determination. There is often little or no security documentation accompanying Wi-Fi “hotspots” or access points in airports, coffee shops, hotels or conference centres.

Any unencrypted network connection can be “tapped” with the appropriate tools even if security is configured in a reasonably safe way. Most of the content of transmissions from your mobile device to the Internet - including e-mail - is transmitted in clear text and can be intercepted, read and captured. Moreover, you might inadvertently set up your mobile device itself as a hotspot, to which strangers can then connect.

One way to access the Internet more safely is to avoid Wi-Fi altogether and use a cellular modem or tether your laptop to a cellular device (via Bluetooth) through the device's network settings. The screen below shows Blackberry settings including "mobile Hotspot", which allows you to create your own hotspot for multiple devices, and "Internet Tethering", which allows you to connect one device (such as a laptop) to the Blackberry for internet access. Turning on either of these services must be done with care to prevent unauthorized access, and when you are done they should be turned off.



Network Connections

Airplane Mode: Off

To use your device on a plane, turn off all wireless connections

Connections

Mobile Network
Bell

Wi-Fi
CYBER

Bluetooth
On

NFC
On

Mobile Hotspot
Not Connected

Internet Tethering
Off

VPN
Not Connected

The mobile phone network is more secure compared to free Wi-Fi hotspots, though not impervious to attacks.

Your mobile phone-based browsing is also subject to the usual hazards of viruses and spyware. Be aware that many smartphones and tablets can browse the web using either the mobile phone network or a built-in Wi-Fi connection. Thus, using your device as a browser is no safer than using a laptop unless you select the appropriate network connection.

There are two key issues to bear in mind when using a public Wi-Fi hotspot, especially free ones:

1. Which available Wi-Fi hotspots are legitimate, and which are traps (or so-called “evil twins”)?
2. Assuming you are using a legitimate hot spot, is it properly secured?

Which available Wi-Fi hotspots are legitimate, and which are traps?

Anyone can set up a Wi-Fi hotspot if they have an Internet connection and a mobile device (see above). They can name the network anything they want – for example “Free Public Wi-Fi” or “Marriott Hotel Internet.” By way of analogy, imagine you posted a draft judgment in a red mailbox on your street corner marked “Canada Post,” but it turned out the mailbox was a fake and the owner simply opened all the mail. Or a courier in FedEx uniform showed up at the courthouse, collected all your urgent packages, and it turned out he was an imposter. These network traps can be set up without any security at all, which means that you can connect to them very easily, and for free. In fact if your mobile device is set to automatically connect to available networks, you could be connected to an “evil twin” without even realizing it.

The problem is that if this convenient wireless network has been established by a criminal, all your Internet traffic - including passwords, e-mail messages, browsing history - passes through their hands in readable form, unless you are using a VPN in which all data is encrypted.

For many hotels and conference centers, the official Internet Service Provider will not have the same name as the hotel. There may be multiple signals available in your room. Always check the documentation in your room, or if there is none, call the front desk to find out precisely what the network name is (SSID) of the legitimate provider.

According to a study in 2008 by AirTight Networks[1], 77% of the available networks at 27 airports throughout the US, Europe and Asia were not “official” hotspots.

[1] As reported by Fox news, “Wireless Cybercriminals Target Clueless Vacationers,” Sunday, July 12, 2008 by Steven Kotler.

Assuming you are using a legitimate hot spot, is it properly secured?

According to the AirTight Networks study, 97% of users were logged into wireless networks that were unsecured. Of the *secured* Wi-Fi networks, 80% were secured by the weak WEP protocol (back in 2008). That means even when you are connected to a legitimate commercial or public system, its security depends on the hardware, software, configuration and policies and procedures of the provider. Perhaps the provider:

- Is not using the most recent encryption available
- Has not upgraded hardware to the most hardened type
- Does not do background security checks on employees who have access to customer data
- Does not monitor their system effectively for possible intrusion detection

Summary of Best Practices

1. Consider using the cellular network built into your device and turning off Wi-Fi in the absence of a secure hotspot
2. On your mobile device settings, turn off automatic connections to open networks when travelling
3. Turn off the Bluetooth “discoverable” feature, or disable Bluetooth on your device if you are not using it for a keyboard, headset or internet tethering
4. Check documentation or call your hotel front desk or conference centre to determine the proper name of the legitimately provisioned wireless network
5. Use only court-provided VPN connections to access network data
6. If you are not connecting through a VPN, connect only to secure websites (e.g. https://...) (many websites can be accessed both ways)
7. If you are not connecting through a VPN, make sure any services you use are secured (for example, JUDICOM is secured, while Yahoo Mail is not)
8. Disable sharing of services, folders and files on your laptop - this is usually enabled by default (get help)
9. Use and configure personal firewall software (you may need help with this)
10. Keep your operating system updated with all recommended security patches

For an informative video, see http://www.youtube.com/watch?v=6uR0VkWUXrI