Wireless Network Security When On the Road

By Martin Felsky
November, 2009

Table of Contents

Introduction

"Judicial Information" is defined in the *Blueprint*[1] (with some exceptions) as "information gathered, produced or used for judicial purposes." Judges working on draft judgments or communicating with colleagues about cases are creating and transmitting "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 will not be 100% secure. For that reason, all sensitive data should be encrypted during transmission and that means using a Virtual Private Network (VPN).

[1] See Canadian Judicial Council, *Blueprint for the Security of Judicial Information*, Third edition, 2009.

Using Wireless Internet On The Road

Many judges are suspicious 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 "hot spots" in airports, coffee shops or hotels.

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 device to the Internet - including e-mail - is transmitted in clear text and can be intercepted, read and captured.

One way to access the Internet more safely with a laptop is via cellphone-based modems such as the Rogers Rocket Stick[2] or the Bell Wireless USB Modem. The mobile phone network is reasonably secure (though not impervious to attacks) compared to Wi-Fi hotspots. However, even mobile phone security is not perfect. For example, when accessing the Internet with a wireless modem, or on a PDA device using the cellular network, there is an authentication process that takes place between your unit and the network.

According to experts, it is possible for an attacker to masquerade as a network provider. Your mobile phone-based browsing is also subject to the usual hazards of viruses and spyware. Be aware that some devices such as a Blackberry can browse the web using either the mobile phone network or a built-in Wi-Fi connection. Thus using your Blackberry or cell phone as a browser is no safer than using a laptop unless you select the appropriate network connection.

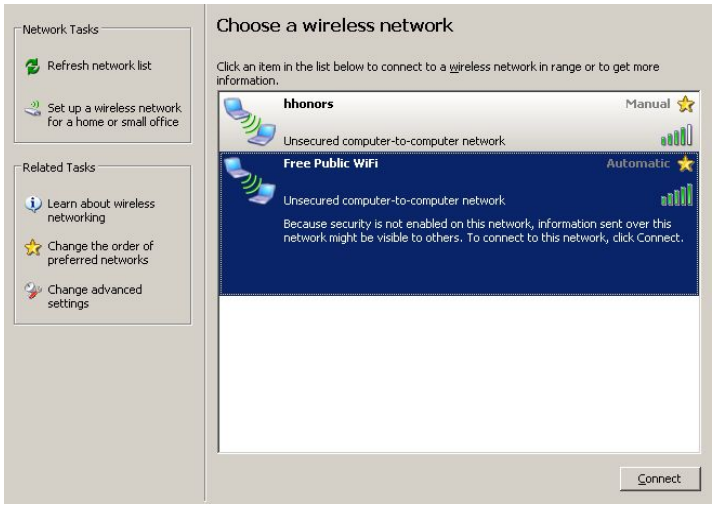
Rogers Rocket Stick

[2] All the Rogers website says about security is that the Rocket Stick has a "Secure connection so you can shop, bank and email with confidence."

There are two key issues to bear in mind when using public Wi-Fi:

1. In many public areas, your wireless-enabled device will detect several available wireless network access points - also called “Wi-Fi hot spots.” (See illustration below) The first issue: which of the networks detected are legitimate, and which are traps (or so-called “evil twins”)?
2. Assuming you <u>are</u> using a legitimate hot spot, is it properly secured?

Note: The list of available wireless networks may look different, depending on the type of computer you have. Below are two common examples using a Windows laptop and a Mac Powerbook.



Detecting Open Hot Spots (Windows)

Detecting Open Hot Spots (Mac)

Which of the networks detected are legitimate, and which are traps?

Anyone can set up a wireless network if they have an Internet connection and a wireless router. 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. When your wireless-enabled laptop or handheld device detects available networks, the signal can be strong, and it can be very tempting to connect to this strong, free, and apparently legitimate resource.

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.

In many hotels, their 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.

It is not always possible to know whether a signal is legitimate or not. I could set up a wireless network in the airport and call it "Data Valet," which is the company used in Air Canada's Maple Leaf Lounges.

According to a study in 2008 by AirTight Networks[3], 77% of the available networks at 27 airports throughout the US, Europe and Asia were not "official" hotspots.

[3] 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. 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 effectively for possible intrusion detection

The security policies and procedures of wireless hot-spot providers should be a lot more transparent. For example, there is no information whatsoever on the highly respected Data Valet website about how it protects the security of its wireless customers.

Summary of Best Practices

1. Turn off automatic connection to open networks
2. Turn off the Bluetooth "discoverable" feature, or disable Bluetooth on your device if you don't have a use for it
3. Check documentation or call the hotel front desk to determine the proper name of the legitimate wireless network
4. Use only court-provided VPN connections to access network data
5. If you are not connecting through a VPN, connect only to secure websites (e.g. https://...)
6. 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)
7. Disable sharing of services, folders and files on your laptop - this is usually enabled by default (get help)
8. Use personal firewall software
9. Keep your operating system updated with all recommended security patches

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