Wireless Network Security at Home

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 at home.

Many judges are suspicious that home wireless networking may not be very secure – but lack the technical knowledge to configure the network security settings properly. Documentation accompanying home wireless networking equipment is often incomplete, impossible to understand, or even misleading.

The bottom line is that without proper hardware, software, configuration and use, all the information accessed through or stored on your computer is vulnerable to unauthorized access.

This article is designed to address home wireless networking security issues in a practical and plain-language manner. Taking the easy, free and common sense steps outlined below will make your home network reasonably secure against unauthorized access. Be aware, however, that even with all the recommended best practices in place, your home network will *not* be 100% secure. For that reason, all sensitive data should be encrypted during transmission and that means using a VPN or websites that use SSL encryption. (You can recognize these by a URL that begins with https://.)

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

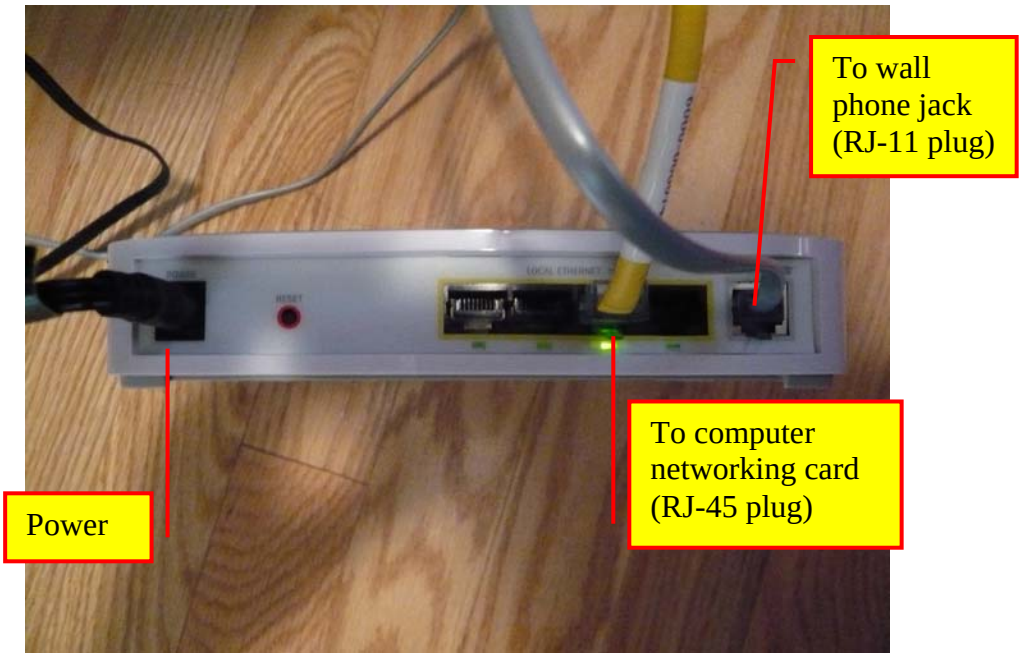
Your Home Setup

Home Internet service is accessible through the same wires (or satellite dish) that provide your land-line telephone and cable television services. For the purposes of illustration I will show you my own home wireless set-up, which is provisioned through my Bell telephone line, and show you the default out-of-the-box settings, most of which are seriously lacking in effective security protection.

Whether you access the Internet through your telephone or cable service, you need a router to connect your computer to the Internet. A router is a device that connects two networks – in this case, your home wireless network with the Internet. Depending on what equipment and system you use, your router could also be referred to as a residential gateway, a cable modem, or a DSL modem.

Bell Internet Gateway (front view)

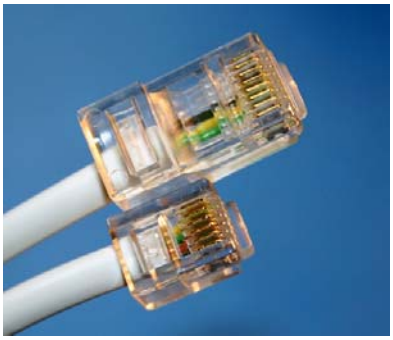
Your router is plugged into the cable or telephone wall outlet. (So in that regard it is not "wireless".) Once the router is connected to the wall outlet, you need to connect your computer to the router. There are two ways to do this: by a network cable (wired) or with a wireless connection. The only way your computer can connect wirelessly to the router is if it has built in or external wireless network card. See illustrations below:



Wireless router with four wired ports (rear view)

Wireless network card (to be inserted into computer)

The outlet on the right is used to connect to the phone wall outlet using a standard phone cable (without a filter). The yellow cable is a local area network "(LAN") cable connecting the router to my computer's network card. The RJ-45 plug on the end of the LAN cable looks like a telephone jack only bigger:



RJ-45 (network) plug is bigger than RJ-11 (telephone)

Since my desktop computer is plugged into the router, I am not actually using a wireless connection at my desk, even though my router is a "wireless" router. However, the router is signalling its existence through the air and I can pick up the signal anywhere in or near my house, with my wireless network devices, for example, my laptop, which has a built-in wireless network card, or my Blackberry, which also has built-in Wi-Fi capability (in addition to its facility to access the cell phone network).

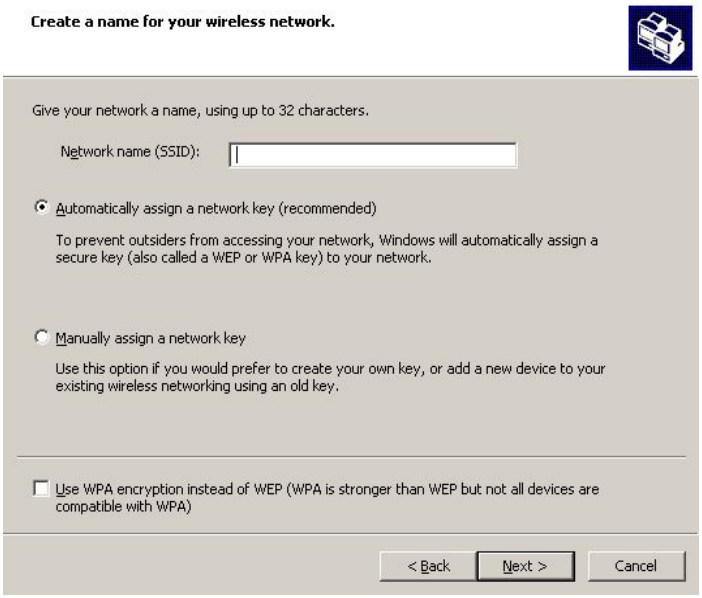
The security of home wireless networking involves protecting your signal and Internet account access against the intrusion of others. How is this accomplished? By configuring the router with software that is built into the equipment, and with networking software that is part of the operating system on each of your computers or handheld devices. We will begin by setting up a home wireless network.

Note: The following screen shots show how to set up a wireless network with a Windows XP computer, and using Bell as the Internet Service Provider (ISP). Please refer to the Appendix to find information about other options.

Setting up a wireless network

On a Windows XP computer, you can establish a home network with the Microsoft Wireless Network Setup Wizard, as illustrated above. For other operating systems, refer to the appropriate manual or obtain assistance from a qualified IT support specialist.

The first step to securing your wireless home network is to change the name of the network that is built in. That is called the default SSID, which stands for ***s**ervice **s**et **id**entifier*. Change it to something that will not identify you. For example, "Felsky" or "1500 Maple Avenue" are not secure SSIDs because they divulge personal information.



Name the network

On the screen above you also have the option of choosing "Use WPA encryption..." WPA stands for ***Wi-Fi Protected Access.*** Even if an upgrade is required (for example, you may have an older notebook with a built-in wireless networking card that does not support WPA encryption), you must choose WPA[2] and never leave the older WEP[3] setting – or even worse – no encryption at all – to remain. (For this illustration I left my network SSID as "Bell053" (the default) and I did *not* enable WPA encryption.)

My network appears first on a list of networks (below) that are available in my neighbourhood.[4] You can see that there's a fairly strong signal from "Toto." My neighbour's dog is called Toto so I'm pretty sure I know whose network that is. I also see that my neighbour has enabled WPA encryption. You can see that other neighbours who use Bell Internet – Bell666 and Bell861 have kept their default SSIDs and have not enabled WPA encryption, making them easy targets for hackers.

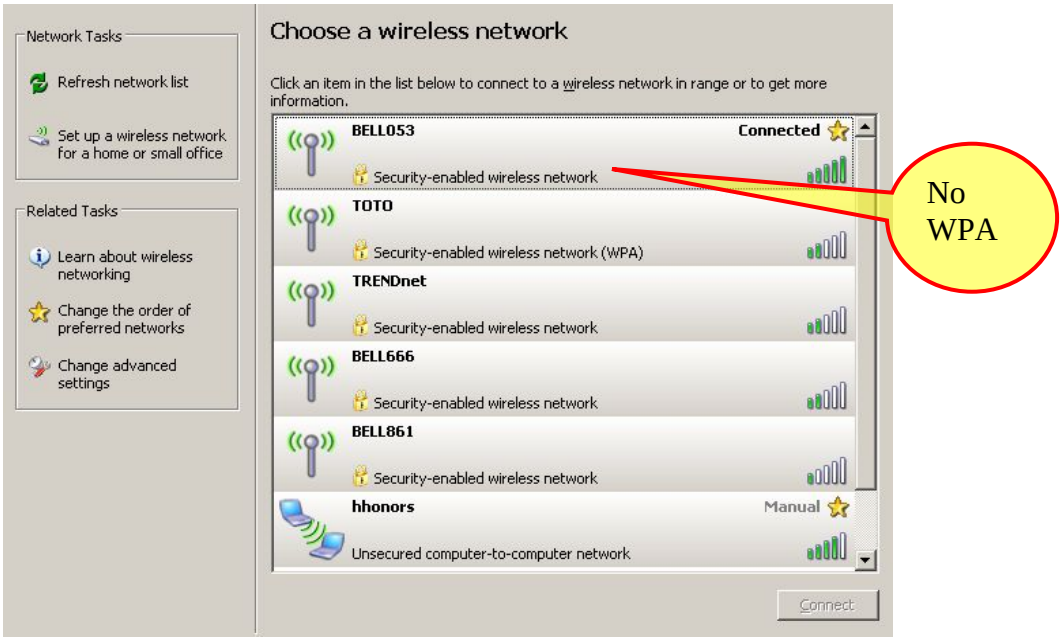
The practical result is that anyone with a wireless device or sniffer can see this list of available networks (roaming around the neighbourhood looking for unprotected signals is called "war driving") and with readily available technology can (a) use my Internet account to do their own surfing, perhaps to send spam, and (b) see whatever unencrypted text is being sent to and from my computer.

---

[2] It has recently been reported (August 2009) that WPA encryption can be cracked in one minute – but only with the most sophisticated tools. See http://tech.yahoo.com/blogs/null/147906.

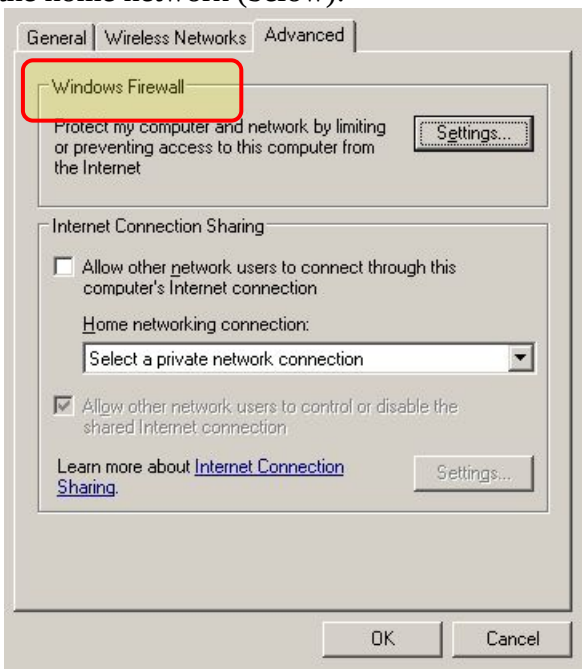
[3] WEP stands for ***Wired Equivalent Privacy***, and was intended to provide the same level of privacy as a wired network. It can be cracked easily.

[4] One aspect of security involves placement of your wireless router – if you place it near an external wall, it is easier for neighbours to gain access to a strong signal. If you are to place the router more centrally within your home, the signal will be weaker for outsiders.



List of available networks

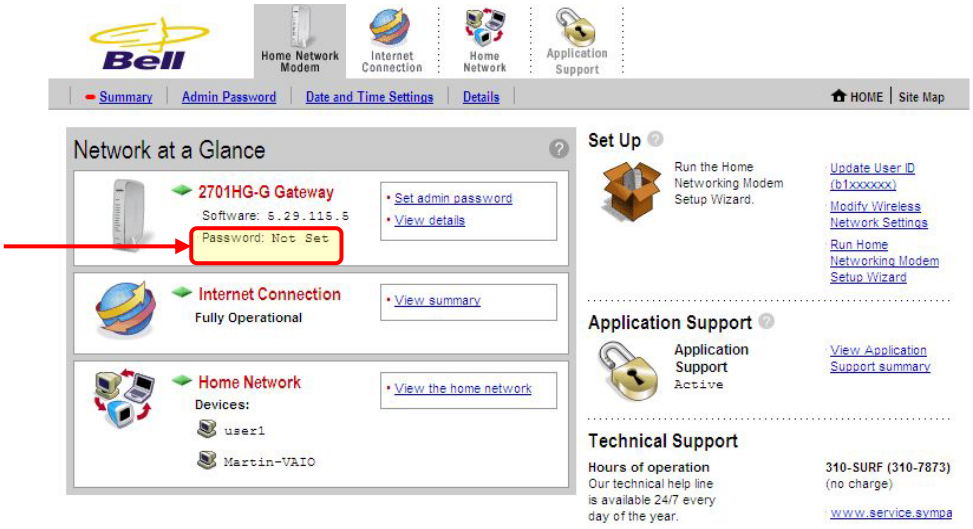
There are settings in the operating system to help prevent unauthorized access to your computer by outsiders through your wireless connection. For example, Windows has firewall software built in that can be configured and connection sharing can be disabled for each computer on the home network (below):



Firewall settings

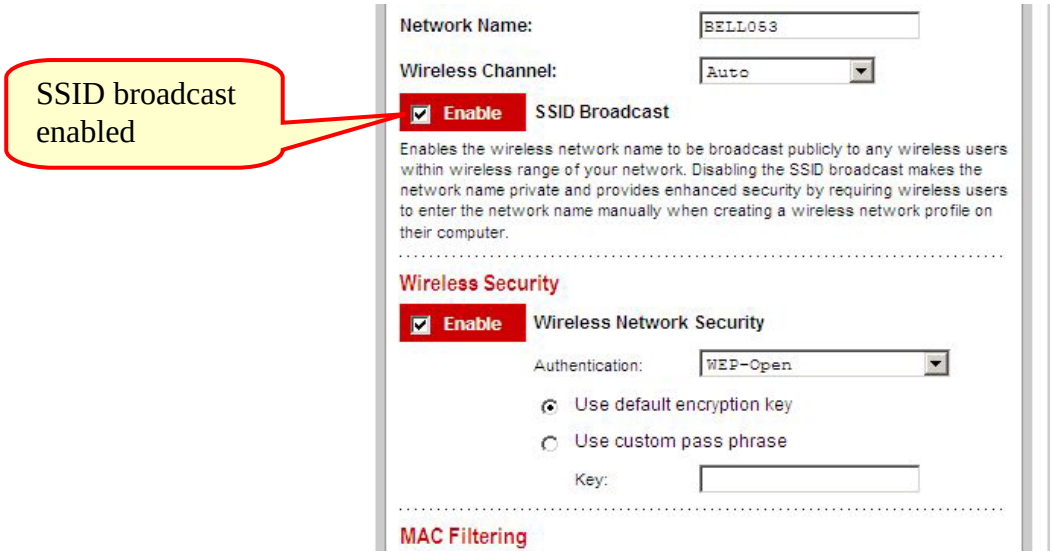
When you plug in your router and your Internet connection has been set up, you have the ability to use software that comes with the router to perform security operations as well and to establish a firewall on the router. Below is the home screen of my wireless router. You can see for the purposes of this illustration that there is no administrator password,

which means that someone gaining access to my network could readily change all the settings on my router and lock me out. *Always set a strong Administrator password for your network settings*.



BAD PRACTICE: Administrator Password Not Set

On the following screen you can see that "SSID broadcast" is enabled. When SSID broadcast is enabled, neighbours can see your network name on the list of available networks. This increases the likelihood of being hacked. If SSID broadcast is not enabled, then your network SSID does not appear:

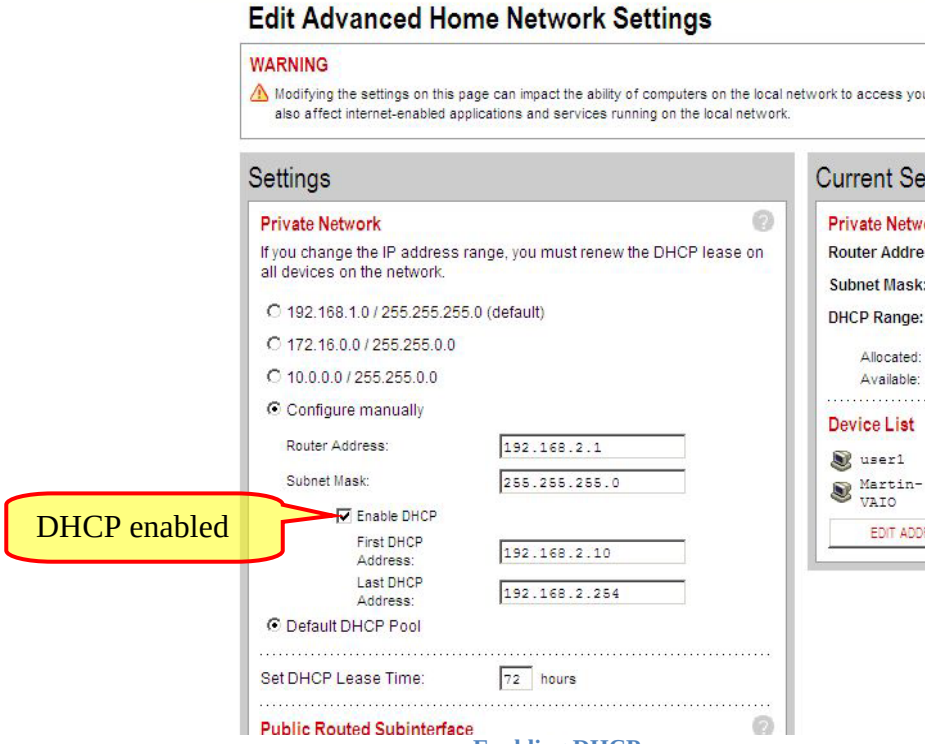


Enabling SSID

Dynamic IP Addresses

In order to share network resources (such as the router, or a printer, or shared files on a computer), each computer on your home network needs to have a unique IP address, or ***I**nternet **P**rotocol* identifier, just like a website. Your router has a unique web IP address, and all the devices on your home network can be assigned IP addresses automatically. This is done through a process called DHCP, which stands for ***D**ynamic **H**ost **C**onfiguration **P**rotocol*, and it is very convenient.

Any time a computer wants to access your home network, DHCP assigns it an IP address automatically. This makes it easy for unwanted outsiders to obtain a valid IP address for your network. It is a better practice to manually assign IP addresses to each computer on your network. In the illustration below, DHCP is enabled by default.



Enabling DHCP

Summary of Best Practices

1. Consider central placement of your router to avoid signal leakage
2. Change the default SSID (network name)
3. Disable SSID broadcast so casual observers will not see your network (more committed individuals can sniff a network even if the name is not broadcast)
4. Choose a network name that cannot be linked to you, your family or your home
5. Use only court-provided VPN connections to access files stored on court networks
6. If you are not connecting via VPN, connect only to secure websites (e.g. https://...)
7. If you are not connecting through a VPN, make sure any services you use are secured (for example, JUDICOM is secured, Yahoo Mail is not)
8. Implement the latest available encryption (do not use WEP)
9. Set a strong administrator password for the router administrator
10. Turn off DHCP and assign static IP addresses to each computer in your home wireless network
11. Enable firewalls on all networked computers as well as the router itself
12. Unplug your router when you are away from home for an extended period
13. Disable sharing of services, folders and files on your laptop - this is usually enabled by default (get help)
14. Keep your operating system updated with all recommended security patches

For an informative video, see http://www.youtube.com/watch?v=A88XB7_Jz7s .

Appendix: Wireless Home Networking User Guides

Though the general concepts are the same for most wireless internet connections, the appearance may change depending on your location and Internet Service Provider (ISP). To ensure your connection is secure, contact your ISP customer support center.

This list of available User Guides may help as you set up your home wireless network.

Cogeco	http://www.broadbandreports.com/faq/wifisecurity
Rogers	http://downloads.rogershelp.com/UG/RogersHomeNetworkingUG.pdf
Bell	http://internet.bell.ca/img_gallery/2701_UserGuide_2wire_EN.pdf
Telus	http://www.telus.com/portalWeb/inlineLink/CP_SCS/Help/Internet_Help/High_Speed/Step_by_Step_Description/Wireless_Networking_Installation_additional/Windows_2000/?_region=AB
Bell Aliant	http://nsegainkc1.aliant.net/knowledge/Docs/Internet/Conn/6520/EnableWireless/EnableWireless.htm
Shaw	http://start.shaw.ca/Start/enCA/Customer+Service+Centre/Internet+Safety/SecuringWireless.htm