Wireless Network Security at Home

By Martin Felsky
Second edition, January 17, 2014

Table of Contents

Introduction

With the enormous growth in popularity of mobile connected devices, wireless access to the Internet at home is the norm. "Wireless connected devices" means a lot more than just laptops, smartphones and tablets: your Blu-ray player, camera, hard drives, gaming consoles, thermostats, lighting controls, television set, eReader, printer, and many other devices, including your car, your wristwatch and your eyeglasses, are now or soon will be connected to the Internet, all wirelessly.[1]

But judges are concerned that home wireless networking may not be secure or private enough to handle sensitive judicial information. It is easy to buy a wireless modem or router – and Internet service providers will set them up for you. But installers do not alter the default security configurations. That is left to the individual user. Documentation accompanying home wireless networking equipment is often incomplete, impossible to understand, or even misleading. If you have difficulty understanding the technical issues involved, or are confused by the jargon and documentation provided by your service provider, it may be worth investing in a home visit by a home network specialist who can set up your system as securely as possible. On the other hand if you are reasonable handy with these things, your security configuration can be done on your computer in a few minutes.

The bottom line is that without proper configuration and use, all the information accessed through or stored on your computer or mobile devices is vulnerable to unauthorized access by amateurs, even inadvertently.

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.

[1] The networking of all these devices is called "the internet of things." Google is currently developing a wireless blood sugar monitor fitted into a contact lens.

Be aware, however, that even with all the recommended best practices in place, your home network will *never* 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://) .

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. Whether you access the Internet through your telephone or cable service, you need a wireless router to connect your wireless devices 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 connection hub, or a modem.

Bell Internet Connection Hub (Sagemcom) (side view)

Your router is plugged into the cable or telephone wall outlet (or both, depending on the service provider) for access to the Internet. The only way you can connect a device wirelessly to the router is if the device has built in (or external) Wi-Fi capability.

A wireless router is signalling its availability through the air at all times. Anyone in range can pick up the signal in or near my house. The security of home wireless networking involves protecting your signal and Internet account access against the unauthorized access by 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.

When your router is set up you can usually access it by with your browser on a local IP address such as 192.168.xxx.xxx. You must then enter your username and password. The Bell hub is delivered with “admin” as both the username and password. It goes without saying that you should immediately change the defaults to your own user name and a proper password.

Once you are in the configuration screens, there are several key settings that must be adjusted.

Wireless Setting	What does it do?	How to configure
SSID	The name of the network or SSID, which stands for "service set identifier"	Change it to something that you recognize as your own but will not divulge personal information. For example, "Felsky" or "1500 Maple Avenue" are not recommended since they represent my name and my home address.
Broadcast SSID	When the SSID is broadcast, anyone with a wireless device will see your SSID on their list of available networks. This makes it easy for a guest to log in, once they are given the password.	Turning of the broadcast of the SSID does not turn off the wireless signal broadcast itself, so anyone with a slightly sophisticated sniffer will find your network anyway. Turning off SSID broadcast keeps out less sophisticated neighbours.
Obtain DNS automatically or manually	Your router can be configured to automatically assign unique IP addresses to each device on your wireless network as needed (dynamic), or you can manually assign an IP address to each device (static).	Theoretically a manual assignment makes it more difficult for a stranger to log into your wireless network, because their device will not automatically be assigned an IP address. Any sophisticated person can easily get around this restriction, though, and assigning IP addresses manually can be a chore.
Security mode WEP WPA2	WPA stands for Wi-Fi Protected Access and is a type of encryption	Choose WPA2 with AES encryption (never use the older WEP protocol, which is easily broken). Choose a long, complex and random passphrase to protect the network.
Registration mode Pushbutton (WPS)	WPS stands for "Wi-Fi protected Access." This protocol allows for wireless devices to join your	This is a convenient tool, but some experts suggest turning it off because it is vulnerable to certain kinds

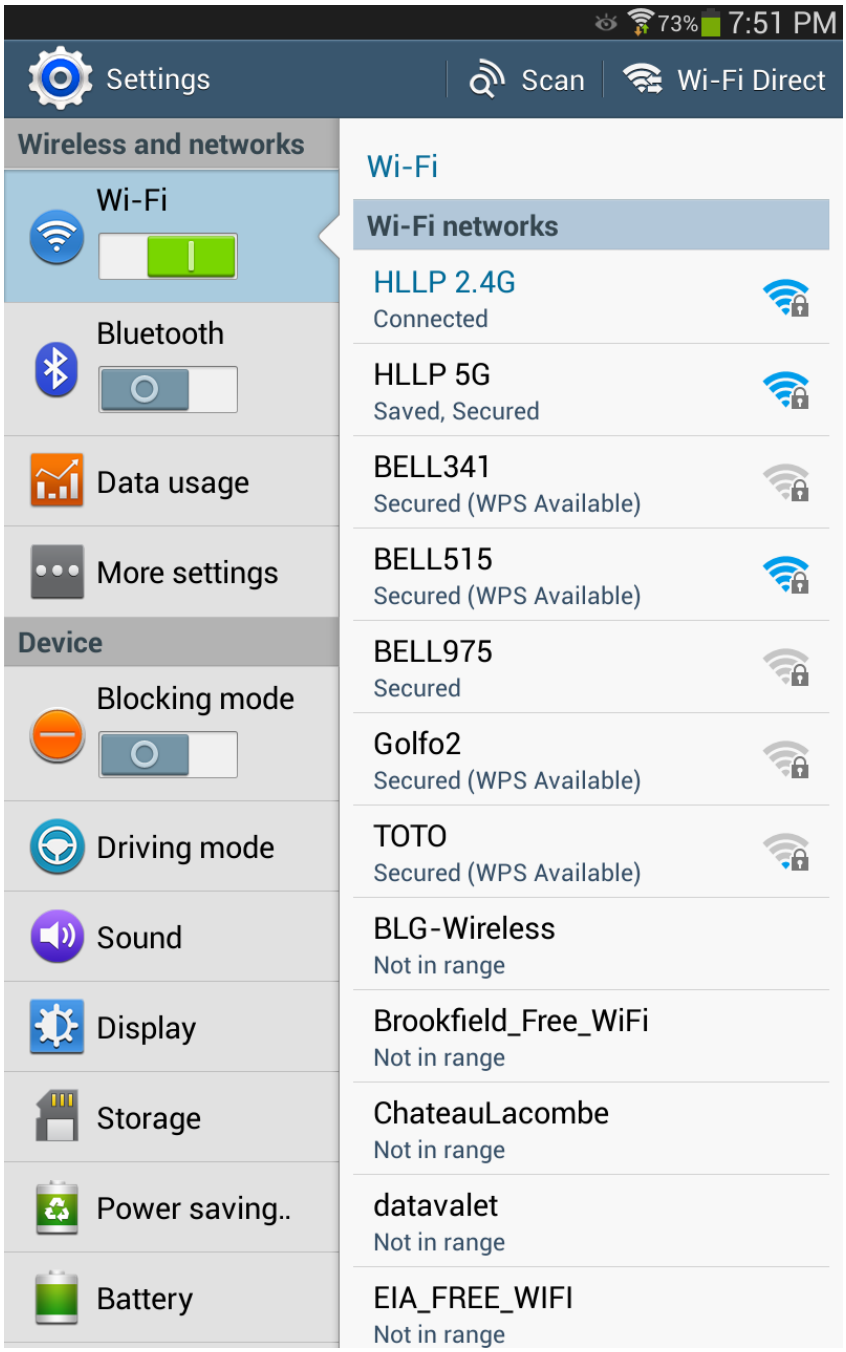
	network by pushing a button on your router rather than setting up the configuration through your browser.	of attacks.
Guest wireless settings	Some routers allow you to set up more than one wirelesss network, for example one for residents who are working from home, and one for guests.	It's good idea to provision a guest network, providing guests only with Internet access, while your own network can include shared printers and streaming media in addition to Internet access.
Guest wireless timer (Time limited or unlimited)	It is often possible to put a time limit on Internet access for guests, but especially if you have set up a limited guest network, there is not to be gained.	0 = unlimited
MAC Filtering Enable or disable	Every networkable device has a unique ID number (Media Access Control) built in as part of the hardware. This is not the same as its IP address, which is assigned and can be readily changed by the network administrator. By enabling MAC filtering you can restrict access to your network to only those devices you have specifically approved.	In theory this sounds like a good security measure, and indeed it can keep out amateurs. But it is also tedious to enter and keep the MAC address list up to date for yourself and for your guests, and anyone reasonably sophisticated in wireless networking can spoof a MAC address and gain access anyway.

My home network (HLLP2.4G) and my guest network (HLLP5G) appear first on a list of networks (below) that are available in my neighbourhood, and visible on my Samsung tablet.[2] You can see that there's a fairly strong signal from "Bell515", and there are other Bell numbered networks in the vicinity (marked "secured")

Anyone with a wireless device or sniffer can see this list of available networks and with readily available technology can (a) use my Internet account to do their own surfing,

[2] 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.

perhaps to send spam, and (b) see whatever unencrypted text is being sent to and from my computer.



Scanning for available networks – broadcast SSID

Summary of Best Practices

1. Consider central placement of your router to avoid signal leakage
2. Change the default SSID (network name) and avoid personal identifiers

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. Use only court-provided VPN connections to access files stored on court networks
5. If you are not connecting via 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, Yahoo Mail is not)
7. Implement the latest available encryption such as WPA2 (do not use WEP)
8. Set a strong administrator password for router administration
9. Consider disabling DHCP and assign static IP addresses to each computer in your home wireless network
10. Enable firewalls on all networked computers as well as the router itself
11. Unplug your router when you are away from home for an extended period
12. Consider provisioning a separate, limited services wireless network for guests
13. 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.cogeco.ca/web/resources/pdf/support/user_guides/internet/self_install_en.pdf http://www.cogeco.ca/web/resources/pdf/support/user_guides/internet/Cisco%20DPC%203825.pdf
Rogers	http://downloads.rogershelp.com/UG/RogersHomeNetworkingUG.pdf http://www.rogers.com/web/support/internet/wireless-network/128?setLanguage=en
Bell	http://internet.bell.ca/img_gallery/2701_UserGuide_2wire_EN.pdf http://support.bell.ca/Internet/Connection-help/Connection-Hub.how_to_change_existing_wireless_settings_on_my
Telus	http://www.telus.com/content/help/internet-support/wireless-home-networking.jsp
Bell Aliant	http://www.bellaliant.net/ browse to *Support* and then *Internet* and then *Use Wireless Internet*.
Shaw	https://community.shaw.ca/docs/DOC-1564