Murray Associates | Security Report

Wi-Fi Security
The 20-Point Checklist

by Kevin D. Murray, CPP, CISM, CFE

Wi-Fi is the worst leaker since the Titanic.

I have a saying, *"Raise your head above the crowd, and somebody will throw a brick."* Usually, this is a good thing. Seeing salvos whiz by is a sign one is achieving. The more you see, the better you are doing. In the case of the ubiquitous Wireless Local Area Network (WLAN, aka Wi-Fi), the salvos are more like silent torpedoes. You won't see them coming.

Spies, hackers, terrorists and nosey neighbors are targeting business Wi-Fi big time. And, why not? Business information is valuable, ransomeware pays, and voyeurs seek entertainment. Most Wi-Fi systems are sitting ducks, especially with employees working from home.

Wi-Fi is used by smartphones, printers, VoIP phones, security cameras, smart TVs, smart speakers and all other IoT devices. Wi-Fi is also the gateway to your network, where everything else can be remotely attacked by outsiders. Additionally, many bugging devices now use Wi-Fi as a bilge pump to move information out, without sinking the ship.

Batten down the hatches and turn on the radar. It's as easy as 1-2-3, and you don't have to do it yourself. All you have to do is make sure it gets done. Let's get started.

You may not need to (or be able to) tick off all the numbers. That's okay. Just doing as much as you can will increase your Wi-Fi security profile.

Conduct an independent technical assessment of your Wi-Fi system. Have a Technical Surveillance Countermeasures (TSCM) consultant handle this for you; at work, and at home.

The assessment should be conducted from two points of view: **security** and **legal compliance**.

In the United States, compliance laws may include Wi-Fi related provisions under:

- Sarbanes-Oxley Act – U.S. Public Companies
- HIPAA – Health Insurance Portability and Accountability Act
- GLBA – Gramm-Leach-Bliley Financial Services Modernization Act
- PCI-DSS – Payment Card Industry Data Security Standard
- FISMA – Federal Information Security Management Act
- DoD 8100.2 – Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense Global Information Grid
- ISO 27001 – Information Security Management

In Europe, these laws may include Wi-Fi related compliance requirements under:

- Basel II Accord
- EU-CRD
- Data protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Anti-terrorism, Crime and Security Act 2001
- Data Retention & Investigatory Powers Act 2014

Harden your Wi-Fi network. If you have staff IT technicians, have them run down my checklist to fix any oversights or vulnerabilities. Your TSCM consultant can also help you accomplish the task.

You don’t need to know all the technical details. Pages of explanations have been written as to why each of these items are on the following list. Just trust each item is on the list for a good reason, and double-check to make sure each task is accomplished.

Summary Checklist for Wi-Fi & Router Security

1) Change the default URL, username and administrator password.
2) Change the network security settings to WPA2, or WPA-Enterprise if you are a large organization.
3) Change the default SSID, but not to something which advertises who you are.
4) Turn off Wi-Fi Protected Setup (WPS), but if you must use it, use it with caution. ”PIN” codes have a finite number of combinations. They can be easily guessed using a hacking program; thus allowing unauthorized access.
5) Keep track of your equipment. Maintain an up-to-date list of everything you expect to see on the network, even if you do not use MAC filtering (see below).
6) Scan the network for ”UFO” MAC and IP addresses regularly. (Unidentified Fi’ing Objects)
7) Make sure the Wi-FI hardware firmware is up-to-date, and is kept up-to-date.
8) Disable remote login to the Appearance Points (APs).
9) Disable wireless administration of the router.
10) Turn off Guest networking. If you need to offer Guest access, keep it separate from your network. Have a Terms of Use, password access, log-in page.
11) Turn on the firewall if your device offers one.

12) Use anti-virus and anti-spyware software on the devices which access your wireless network.
13) Check for Wi-Fi capability when adding new equipment to your network. Printers are notorious for having Wi-Fi capability active, by default, without any security measures activated.
14) Once you've set up your router or AP, log out as administrator.

Useful tips, but they may not stop a determined hacker:

15) Disable broadcasting of the SSID.
16) Reduce the range of the wireless signal to only what is needed.
17) Filter MAC addresses to comb out unauthorized users from connecting. Tip: On larger Wi-Fi networks, adding a MAC profile matcher[1] will make this a much more effective security measure.

Additional general usage tips:

18) Turn off the wireless router when you are not using it.
19) Never assume public wireless networks are secure. Use a VPN connection.
20) Turn off the automatic Wi-Fi connection search feature on all your devices. Keep their search lists clear of old connection SSIDs for an extra measure of security.

3. Conduct re-inspections of your Wi-Fi system on a scheduled basis. In addition to establishing a history of due diligence, re-inspections identify new connections to the network which may be unauthorized, or incorrectly configured for security. Quality TSCM consultants will do this as a matter of course when conducting your regular inspections for bugging devices.

> ***"I am the master of my fate,***
> ***I am the captain of my soul."***
> William Ernest Henley 1849–1903

His words apply to many things in life. These days it includes our electronic souls.

Start the protection process, now, before it is too late.

Sail safely, my friends.

=====================================

Kevin D. Murray CPP, CISM, CFE is a technical information security consultant and TSCM specialist with over four decades of experience.

Murray Associates is an independent security consulting firm which provides eavesdropping detection and counterespionage services to business, government and at-risk individuals.

Headquartered in the New York metropolitan area, a Murray Associates team can assist you quickly, anywhere in the United States, and internationally.

Extra: If you like spy and privacy news, security tips and more, visit spybusters.blogspot.com. Be sure to sign up for the free email updates.

[1] http://greatbaysoftware.com/ (I have no relationship with them. Others may offer similar products.)