9 Tips to Make Your Home Wireless Network More Secure

Devolutions

HOME WIRELESS NETWORKS CAN BE HIGHLY INSECURE

In a recent article on cybersecurity tips that parents should teach their kids, we highlighted how, contrary to what many people believe, home wireless networks can be highly insecure. Unfortunately, the only people who are happy about this are hackers.

Since you're definitely not interested in making hackers happy, here are 9 tips to make your home wireless network more secure (by the way, a big THANKS to community member **Scott Bowling** for giving us the idea for this article!).

1. Enable Network Encryption

The problem: All routers these days feature network encryption. That's the good news. The bad news is that it may not be configured appropriately by default. This situation may expose your users to poor and vulnerable encryption configurations that hackers can attack to compromise the wireless communication.

What to do about it: This one is really easy: make sure you choose WPA2-Personal (Wi-Fi Protected Access 2) instead of WEP (Wired Equivalent Privacy)! If you have a newer router that supports WPA3-Personal, that's even better. Here is what Wi-Fi Alliance says about this emerging standard:

"WPA3-Personal brings better protections to individual users by providing more robust password-based authentication, even when users choose passwords that fall short of typical complexity recommendations. This capability is enabled through Simultaneous Authentication of Equals (SAE), which replaces Pre-Shared Key (PSK) in WPA2-Personal. The technology is resistant to offline dictionary attacks where an adversary attempts to determine a network password by trying possible passwords without further network interaction."

The bottom line is that whether you select WPA2-Personal or WPA3-Personal, you still must use a strong password, which is called the Pre-Shared Key (PSK), to maintain a proper level of encryption security. This will be the subject of our next tip.

2. Change the Default Pre-Shared Key (PSK)

The problem: Using the default PSK is like leaving the keys in your front door — it's basically an invitation for the bad guys to come in and take what they want. Encryption security relies on it, so it's just as bad as using a weak, easy-to-guess, or duplicate password (i.e. a password that is used elsewhere, such as an email or Facebook account), especially for a WPA2-Personal enabled deployment.

What to do about it: Change your network's PSK to something that is unique and strong. Obviously, you know what unique means. But what does strong mean? According to Avast, a strong password:

- Uses at least 15 characters
- Uses a mix of numbers, letters (upper case and lower case), and symbols.
- Does not use memorable keyboard paths (e.g. qwerty)
- Does not use common substitutions (e.g. passw0rd)
- Does not use a single dictionary word
- Does not use any personally identifiable information (e.g. your spouse's name or date of birth)

As my colleague Jenny discussed a little while ago, one of the best ways to choose unique and strong passwords is to use passphrases instead of passwords. Passphrases combine uncommon words that are relatively easy to remember, but virtually impossible for hackers to guess. For example, let's say your favourite color is **blue**; a friend of yours once had a **poodle** named Blue; whenever you think of poodles you think of Paris (for some reason); to get to **Paris** you need to take an **airplane**; and when you're on a flight they always give you those little packs of **peanuts**. Put all of that in a blender and you come up with: "**bluepoodleParisairplanepeanuts**".

If remembering strong and unique passwords is difficult — and for most people it is — consider using a password manager, which will generate a suitable password and then store it for you in a secure vault. Click here for our comparison of popular password management tools.

3. Change the Router's Default Administrative Credentials

The problem: To setup your wireless router, you typically need to login to an online platform located at http://192.168.1.1 or http://192.168.0.1, and then enter a default password — usually "admin". If a hacker manages to access this portal, they can make all kinds of unauthorized changes, and even lock you out of the router.

What to do about it: Just as you selected a unique and strong password for your network SSID, do the same for your administrative credentials. Again, using a password manager is a good idea here so that you don't forget your password or feel obligated to store it in an unsafe manner (spreadsheet, document, etc.).

4. Turn Off Remote Management

The problem: By default, some routers are set to allow remote computers and devices to access the administrative portal from the Internet. Of course, they would need the password, but it's still a risk that a potential vulnerability in the login portal might get exploited and let the bad guys in. Also, if the password does not follow rigorously the recommendations of tip #3, it may be guessed by an attacker living in a different country than yours.

What to do about it: From the router administrative portal, disable remote management. Once you do this, only computers and laptops that are connected to your network can access the router's administrative features.

5. Disable WPS

The problem: WPS (which stands for Wi-Fi Protected Setup) is designed to make your life easier by allowing you to connect devices to your wireless network. This connection happens by first pressing a button on your router, then pressing a button (or clicking a button/box) on your device. No login password is required. This is because there is a protocol between the router and the device that allows the exchange of secrets. However, this protocol might be vulnerable to brute-force techniques and expose your WPA PSK to attackers. There are also so many shady implementations and other inherent risks in using WPS that it just isn't worth the risk to your home network.

What to do about it: Disable WPS.

6. Keep Your Router's Firmware Updated

The problem: Just like all other software, the firmware that routers use may contain flaws and vulnerabilities. Once hackers identify or learn about them, they move on with the attack.

What to do about it: Regularly keep your router's firmware updated. For a step-by-step guide with screenshots on how to do this for several popular router manufacturers, check out this article at Lifewire.com.

7. Change the Default Network Name

The problem: Router manufacturers such as Netgear, D-Link, Linksys, and most others, typically set a default network name (a.k.a. SSID/Service Set Identifier). This network name is used by the encryption algorithm, along with the password, to secure communications. Password cracking dictionaries (rainbow tables) include common SSIDs. Thus, having a popular and widely used SSID can help hackers compromise the network.

What to do about it: Change the default network name to something unique, but make sure you don't include any identifying information. For example, "W2A1AC" should be fine, but "John's Network" isn't. Basically, try to be as boring as possible (save your creativity for our monthly poll questions!).

8. Turn Off Network Name Broadcasting

The problem: By default, routers typically broadcast the network name. This is designed to help people

looking for the network on their Wi-Fi enabled desktop, laptop, tablet, or smartphone. While this is useful and typically necessary for public Wi-Fi networks at libraries, coffee shops, airports, malls, and so on, it's not necessary — or safe — for a home network. After all, why put up a big sign for hackers that effectively says: "Hi there, we have a Wi-Fi network! Want to come over and visit?"

What to do about it: Turn off network name broadcasting, so that it becomes invisible to unauthorized users like hackers – and to your neighbors, who may not necessarily want to steal your data, but who might love to use your bandwidth to stream videos, play games, torrent, and so on. Also keep in mind that turning off network name broadcasting will not hide your router's activity, and it's frankly not that hard for skilled hackers to use third-party tools to detect whether a network exists or not. But it's still a good idea, especially since most people with home networks don't turn off network name broadcasting.

Important note: Make sure to remember what your network is called (or write it down on a piece of paper and then hide it somewhere in your house). This is because once you turn off network name broadcasting, you won't see it on the list of available Wi-Fi networks anymore. Instead, you will have to connect to a "Hidden Network" and enter in your network name manually.

9. Keep All Connected Devices Secure and Updated

The problem: Despite all of these security enhancements, your wireless network will still be vulnerable if a connected endpoint (e.g. Wi-Fi computer, laptop, tablet, or smartphone) has inferior security.

What to do about it: Make sure all devices that are on your network have up-to-date software and are protected by good anti-virus and anti-malware solutions.

The Bottom Line

The above tips will make your network significantly more secure, and much less likely to be attacked — especially since hackers tend to target "easy victims". Easy victims are people who haven't made any security changes since they first plugged in their router and started surfing. It's like how burglars are much more interested in breaking into homes that have weak locks or open windows vs. ones that have a super-ultra-mega-state-of-the-art security system (plus a really mean dog).

We hope you find these tips helpful, and that they keep you safe on the virtual landscape!