

---

Subject: Top 10 Reasons Why Data Scientists Advice Secure Wifi Connection  
Posted by [admin](#) on Thu, 30 Jul 2026 10:52:15 GMT

[View Forum Message](#) <> [Reply to Message](#)

---

## Introduction

In this day and age, the use of wireless technology is very prevalent. If we were to take a look inside many of today's households, it is almost certain that we would find numerous gadgets that can connect to the internet through a network.

These networks can either be wired or wireless. Most households today use a wireless network at home in order to connect to the internet, we often refer to this as a Wi-Fi network.

When using a Wi-Fi network, security should be a high priority for you, this would help to minimize or eliminate the risk of having unwanted access to your network. To some people, having unauthorized access on your Wi-Fi network might seem like a small issue but this could lead to numerous problems if not properly managed.

Today I will inform you why you should have a secure network and how you can go about building one.

## My picture

### Reasons you need to have a secure Wi-Fi network

There are many reasons why you should seek to secure your Wi-Fi network. In this article, I will go over a few of them in order to help you to better understand the risk of neglecting proper security measures.

#### 1. Unwanted use of your network

One of the main reasons you'd want to have a secure Wi-Fi network is to stop the unwanted use of your network. Having unauthorized use of your network cannot only lead to potential security threats but this could also affect you in other ways such as increasing your internet bill based on additional data usage.

#### 2. Access to personal files and data

It should be known that when unauthorized access is gained to your network, it is also possible for this person to access sensitive data that might be saved and shared on this network based upon your file sharing settings.

#### 3. Ability to corrupt devices on Wi-Fi network

When someone gains unauthorized access to your network, they also have the ability to corrupt devices that are on that network by placing some kind of malicious software within shared network folders or through other methods. This could lead to serious damage or compromisation of devices connected to this network.

#### 4. Building a secure Wi-Fi network at home

In order to build a secure Wi-Fi network at home, there are many key things that you must take into consideration. Please allow me to go over a few of these things in order to ensure that you

will take proper measures to secure your network.

It is very important that you pay attention to each point as none is more important than the other. Good security includes a combination of tactics to ensure best results.

#### 5. Change your network's name (SSID)

Changing the name of your Wi-Fi network will play a big role in securing it. Change the name of your network/SSID (Service Set Identifier) so that hackers cannot see the type of router you have. The more they know about your router, the better their chances of cracking its WPA2 encryption.

As Apple support says, Some common default SSID names to avoid are linksys, netgear, dlink, wireless, 2wire, and default

Don't use a name such as, "BetYouCan'tHackMe" or "DanielsMom." The first name practically begs hackers to break into your network, while the second name gives away information that hackers could use for identity theft.

#### 6. Enable WPA2 Encryption

Log into your router's administrator console to see your encryption options and whether encryption is even turned on. Fortunately, many newer routers come with Wi-Fi Protected Access 2 (WPA2) encryption turned on.

WPA2 has stronger security and is easier to configure than the prior options. The main difference with WPA2 is that it uses the Advanced Encryption Standard (AES) instead of TKIP. AES is able to secure top-secret government information, so it's a good option for keeping a personal device or company WiFi safe.

#### 7. Keep the firmware update

Keeping the firmware of your router updated is a great practice to ensure that good security measures are in place. This process may differ from router to router but it will ensure that you will be protected from all discovered exploits as you will have all patches to provide you with adequate protection.

#### 8. Change your network's default password

Just like changing the name of the network, changing your password from the network's default password to something strong and unique, will definitely play a big role in increasing its security.

#### 8. Setup a guest network for your visitors

Instead of having guests login to your main Wi-Fi network at home, it would be a smart idea for you to set up a guest network for them to log into. Many routers today, especially those built for business, includes a guest network feature where you can set up an alternate network for your guests to log into. This would allow you to keep the password of your main network safe as you wouldn't have to give it out to every guest coming by your home.

#### 9. Change your administration credentials

It is not just important for you to change the default name and password of your network, it would also be advisable for you to change the administration credentials of your router as well.

This information is used to access your router directly, where you can change the preferences of your network. It would be very unfortunate if someone gained access to this area of your network.

10. Ensure that ALL devices connecting to the network are also secure

It is important that you ensure that all devices connecting to the network are secure. Devices such as laptops, tablets, mobile phones, smart TVs and more must also be secure to minimize the risk of an attack on your home network. If any of these devices are vulnerable and a hacker gains access to one, your network would be facing a potential risk to an attack.

These devices can be kept secure by using strong passwords, ensuring that all software programs are up to date and by using antivirus software to frequently scan for any threats.

My picture  
Final Word

I hope that you've found this article informative and that you have learned how you can better secure your Wi-Fi network at home in order to minimize unauthorized access and other unwanted threats.

---