Protect your WiFi from Hackers

Vasileiadis A. (CyberKid)
Vasileiadis A. (CyberKid)

.

Follow

11 min read

.

Aug 29, 2024

Listen

Share

More

Wi-Fi Hacking is much easier than most people think and the way to achieve it is

some common techniques that most hackers use. With a few simple steps, the average user can protect their home router from the five most common WiFi hacking methods

A simple user will say that they have slow internet and will call customer service thinking that the provider is to blame. An average user who is a bit more sophisticated will try to confirm whether he has slow internet or not by doing an Internet and Intranet speed measurement on the terminal and then try to find the best available channel , maybe that will fix his problem.

At this point, our freckled friend should also consider whether he has fallen victim to

password cracking,
social engineering,
WPS attacks,
remote access
rogue access points.
firmware vulnerability
Here we will see some basic attacks as well as security settings to implement to get rid once and for all of the nagging question Who is stealing my WiFi… ooooo?

Attack 1: Password Cracking
Password cracking is a proven and effective method of accessing a Wi-Fi network, based on the user's habit of choosing a bad password. In this case there are two ways a user can fall victim to this attack.

The first is to exploit a router that uses a weak type of encryption called WEP rather

than the more modern WPA2 that is the standard for most wireless networks. Using a WEP key allows even a complex password to be cracked within minutes, rendering it ineffective (... yes there are still those who use it...)

There are many tools available for cracking WEP networks, and they are able to detect and analyze WEP networks using Kali-compatible wireless network adapters .

The second method of password cracking concerns the more secure WPA2 encryption method and results in a means of attack that causes a “brutal” forced disconnection of devices.

By disconnecting the devices from the (victim) WiFi for a few seconds, a hacker

can force the devices that will reconnect to the network to exchange a sequence of packets called a handshake. This handshake is enough to try to guess a huge list of passwords during the device handshake process. Thus, by testing millions of passwords, “bad passwords” can be cracked in a few minutes or a few hours.

Some of these tools are as we saw in the related article :

airgeddon,
Besside-ng
Aircrack-ng.
These tools can be used to record and crack network passwords through eavesdropping, as we mentioned, during the handshake process.

Solution: WPA2 and Stronger Passwords! Hackers rely on some bad habits we have to succeed in an attack. Using stolen passwords collected from real user accounts is a common tactic based on the tendency of users to reuse their favorite passwords, or the tendency of users not to change the factory password, or to use passwords such as numbers phone or anything particularly obvious.

So you should use your router's WiFi passwords that are unique and not based on information or interests that you have made public or that can be easily guessed by anyone.

You can also detect if someone is hijacking your WiFi by downloading the free Fing mobile app, which allows you to

scan and see which devices are connected to your router. If a device is connected when it shouldn’t be, you have at least a suspicion that an unauthorized user is connected and can take action such as changing the password.

Attack 2: Social Engineering Attacks
Generally, a social engineering attack relies on tricking the user rather than using some technical exploit of a vulnerability, so the victim may not realize that something has happened.

There are many reasons why you should not give someone (a stranger) your WiFi password. It is important to remember some facts about Wi-Fi:

Wi-Fi allows direct communication with devices on your network, such as web

cameras, desktop computers, and other devices that may be wired rather than wireless. This means it can exploit any vulnerability in your devices and intercept anything. In short, it’s like giving your key to a thief.
Once someone connects to your WiFi, they can access your router’s admin interface and create a remote backdoor (due to a vulnerability in the router’s firmware, for example), preventing you from kicking them out of your network, even if you change the password access.
Passwords are easy to give, but once someone has access, it’s hard to remove them. A malicious user may try to reach not you directly, but someone (a neighbor?) who knows your WiFi password, to gain access to it.

Solution: Always be cautious!

Many routers on the market include the ability to create a guest network that does not allow communication with other devices on the network or sub-networks.

It is also recommended that you change your WiFi password periodically, at least once every six months and monitor who has access to it e.g. with Fing .

So just like we don’t give out the PIN from our bank account, why would we give out the password from our home WiFi to a stranger?

Attack 3: WPS PIN Attacks
WPS setup PIN attacks have been widely used since they were discovered, allowing software such as Reaver , which tests several PINs and is able to crack any router in minutes 1 .

Even with the world’s most secure secret password, a router that is vulnerable to Reaver attacks can be cracked and discovered by any hacker in our area.

Although Reaver is a fairly successful attack method, a new generation of attack was created with the development of the WPS Pixie-Dust method . This attack exploited flaws in the way many routers assigned random values to their PIN. With WPS Pixie-Dust, a vulnerable router could be compromised in minutes or even seconds.

Once an attacker has the WPS setup code, they will always be able to access your router, no matter how many times you change your WiFi password. Since many routers do not allow you to change the PIN,

this means that the router is permanently vulnerable as long as the WPS setting is enabled.

Solution: Disable WPS & verify with tests! While several routers offer the convenience of WPS, most can disable it to prevent Reaver or Pixie-Dust attacks. To do this, you'll need to log into your router's settings and look for the part of the page that says 'WPS Setup' or 'WPS Access' settings.

Once there, turn off WPS. Once this is done, reboot your router and check if the setting is still disabled (there is usually a small light on the WPS indicator).

While this may seem sufficient for some routers, some older models may say they have disabled WPS, when in fact they still

respond to WPS and Pixie-Dust attacks. If you suspect this is the case, it would be a good idea to run a tool like Wash , which will detect any nearby network that has WPS enabled. If your router appears in this list even after changing the setting, it may be time to buy a new router.

In Kali Linux , you can run the following command if you have a compatible wireless network adapter and after turning it into monitor mode and type the following to display the nearby vulnerable networks.

wash -i {monitor-interface}

You should see something like the following.

root@kali:~/reaver-wps-fork-t6x/src# wash -i mon0

BSSID Channel RSSI WPS Verison WPS Locked ESSID

D8:EB:97:11:BM:D9 9 00 1.0 No To-Tsampa-Pethane

Here, we can see a network called To-Tsampa-Pethane on channel 9 using WPS version 1.0. This means that the device either has the WPS setting enabled or it may not be possible to disable it for that particular router model.

Attack 4: Remote Access Attacks
While remote access can be useful , enabling this feature by default and without taking the necessary security

measures is a bad idea.

The reason this shouldn’t be enabled is because of the way these devices are discovered and shared in services like Shodan . This engine has an index for every device with ports directly exposed to the Internet, such as IP cameras, routers, and IoT devices.

Although remote management should not be enabled by default, many router devices come with this setting enabled and even with factory password settings in its Admin panel.

Remote access risk comes from two different sources, external and internal .

Once a device is registered with Shodan,

it’s only a matter of time before someone (hacker or bot) tries to connect. An external attacker will usually rely on a list of factory passwords for that particular device.

The inherent danger of this attack is that someone with temporary LAN access or the WiFi password can enable remote management and then just come back whenever they want. Whenever they want to connect remotely to the network, they can simply log in with the credentials they’ve created beforehand.

Solution: Disable Remote Access & Port Forwarding

The first step you can take to ensure that your devices are not exposing ports directly to the internet is to log into your router’s admin panel and look for a tab that

says port forwarding settings.

This is section may be under the “Advanced” tab on some devices. When you find the page, there should be no active ports , as shown in the image below.

If, however, there are any promotions that you are sure you did not add, you should disable them immediately. Since you are here, also change the password in the admin panel of your router.

Attack 5: Rogue Access Points
A rogue access point is a WiFi network designed to trick users into connecting to it. After that, it is capable of stealing passwords and spying on connected devices. Hackers using roque access points use tools like WiFi Pumpkin that run

on simple, low-cost hardware like Raspberry Pi.

A simple setup like the one in the image below can be provided as a passwordless network to lure the victim.

So the way your laptop and phone look for WiFi is usually enough to automate your connection if you use many free WiFi networks that don’t require a password. When your phone or laptop sends probe data for available recently connected networks, attackers can create a fake WiFi network with the same name as the one your device is looking for. If the network does not have a password, your device will connect without warning you.

Workaround: Spot detection of a Rogue AP

When using WiFi, you should always know which network your computer is connected to.

It’s easy to test this by turning on Personal Hotspot on your phone. In the settings of the personal hotspot you put a name of a coffee shop where you used their WiFi recently. Leave it without a password. If your computer connects automatically, it is possible that someone malicious has configured your Internet connection or you have automatically connected to a rogue access point without realizing it.

The way computers store the wireless networks they’ve joined isn’t very clever, and most computers will automatically join any WiFi network that has the same name as a network it’s previously connected to. The exception to this rule is

if the network has different security settings than the one you were previously connected to, where you suddenly see a password required.

For security reasons, it’s a good idea to find the recent (foreign) connections you’ve made to your WiFi and disable the auto-connect setting on them when they’re in range.

You should go to your computer’s Wi-Fi settings and delete any networks you no longer want to connect to.

If you don’t want your computer’s connection to be compromised, be sure to delete connections you no longer use and make sure your computer doesn’t connect to networks with the same name.

Then it’s smart to avoid connecting to unknown networks whenever possible and instead use your phone’s hotspot or a trusted network. Make sure you use a VPN whenever possible to make sure that even if the connection to that particular WiFi is not reliable, it won’t be so easy to intercept data.

Router Firmware vulnerability
Your router has a Linux operating system which of course can have software errors since it is old. A software bug could allow a hacker on the other side of the world to remotely infiltrate your network and steal your personal information.

So a software vulnerability that someone exploits with a Krack Attack leaves millions of devices exposed that will never

be patched for such vulnerabilities. If the router's operating system uses a software version for which your provider has not issued a security update, you are forever exposed to whatever passwords and security locks you add.

Solution: Frequently check for Router Firmware updates
While most commercial routers update automatically, some require you to manually activate the update process. Unfortunately, this is not a given for the routers you receive from your Internet provider. In the majority of them the providers do not deal with security updates of the routers that they give to their customers.

A phone call to customer service will make you wonder if it's time to invest in a

commercial router. Here we should note that it is worth looking at a list of routers that are compatible with the open source OpenWRT operating system which gives more possibilities to the “sophisticated” user. However, empirically speaking, most commercial routers are clearly better off than what the providers provide.

Whichever router you buy, it’s a good idea to set a reminder on your smartphone to check for available updates at least once a month.

Epilogue
So in general there are two ways to be secure when it comes to your WiFi

securing your own Wi-Fi network
and ensuring that you are careful and considerate when using any network you

do not control.
Of course you could strengthen your WiFi router even more by taking advantage of the mac filter settings and disabling the SSID Broadcast from the router's admin panel, but when we're talking about a home router, these settings can cause problems if you don't know how to handle them 2 .

Finally, it should be understood by all our unsuspecting friends that, just as the doors and bars of our house keep out unwanted people, so our router is the "door & bars" of our digital home.