The router is not as safe as you think

It all depends on whether your router is secure. Here are 10 ways that your router may be exploited by hackers and other intruders.

You are happy to browse the web, visit the website, make a few transactions via online banking and maybe some games. Everything is perfect, with a computer protected by a firewall and anti-virus software or maybe a VPN.

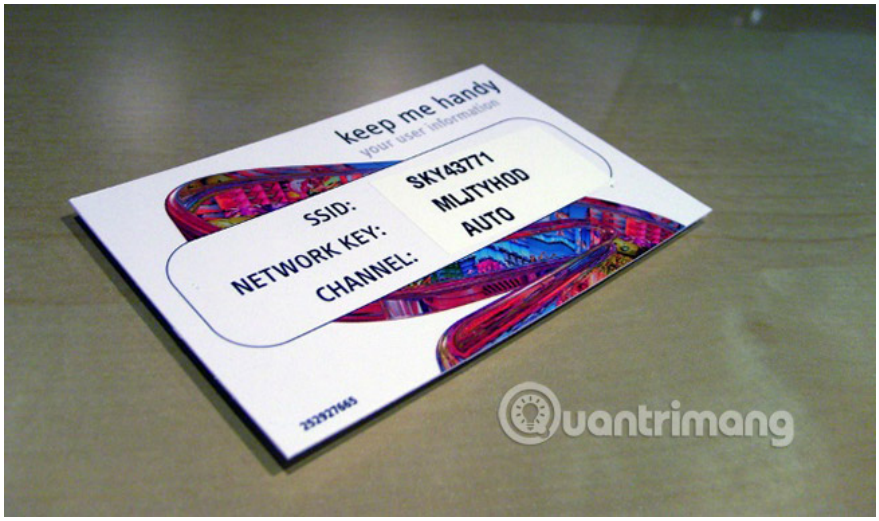
You think no hacker can ruin your beautiful day, right?

It all depends on whether your router is secure. Here are 10 ways that your router may be exploited by hackers and other intruders.

The router is not as safe as you think

1. Admin password and default SSID

Millions of routers are sold every year, all with a pre-configured admin password and printed on the side of the device. It is easy to recognize that every password is not unique. Thus, it is possible to use a relatively small number of passwords to access routers from a single manufacturer.



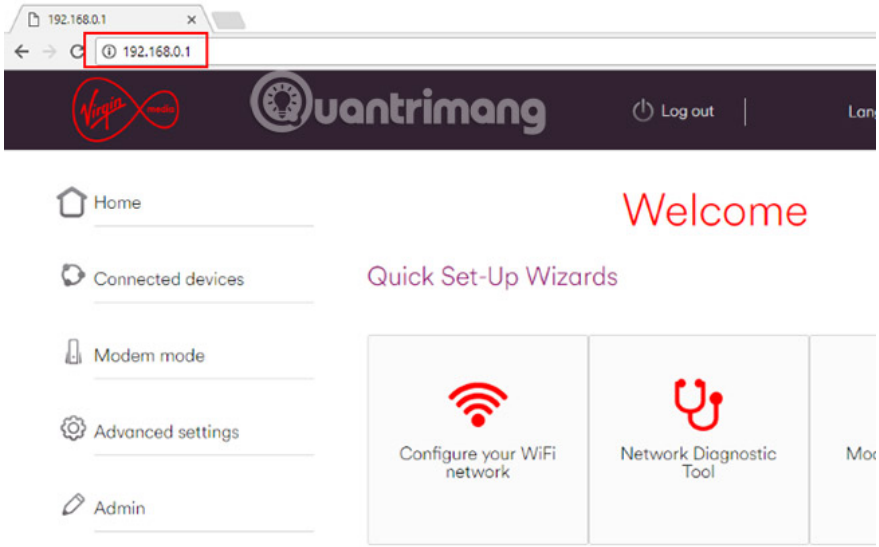
Although changing the default password for the router is very simple, but that is not what most people do. Password reset does not occur automatically. Basically, you need to log in to the admin panel on the router to do that. Most router owners often do not access this control panel, and if you belong to this group, you risk very high attacks.

Checking the router documentation to login and changing the router password is a very important operation.

When you are there, learn how to change the SSID router. In particular, care about the routers provided by your ISP. These addresses often use addresses or phone numbers to create SSID names - things that help hackers' drivers (also known as' wardriver ') determine your attributes. You certainly don't want that to happen.

2. Address admin interface clearly

Another problem with routers is that they all can be accessed in the same way. With a default password, SSID and an IP address are easy to guess, the router can be hacked.



For example, the default IP address for the router's admin interface is 192.168.1.1 or 192.168.0.1. This is not a secret - anyone can find out this information by searching online or using network tools. That means anyone can log in to the control panel for the router's admin, and access your home network.

Again, changing the default IP address is what you can do in the admin screen, accessed via the web browser. Just like the password and SSID, this is one of the first things you should change after setting up your router.

3. Manage cloud-based routers

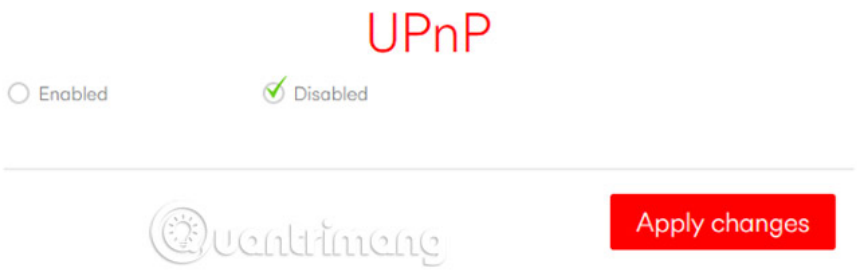
In the past few years, a ridiculous new tool has been provided by router manufacturers: Cloud-based management. This is a cloud-based service layer that provides the interface that comes with your router.

Yes, you can only access the cloud-based management tool, if the supported router is connected to the Internet. It sounds great, but it doesn't. Then, there are mesh router systems, such as Google Wi-Fi, that are completely cloud-based and can only be accessed from mobile apps. Mesh routers have the advantage of updating the firmware, but you should only consider those devices if they also provide local administrative access.

After all, do you really want to give router administrator rights to an unknown third party? How do you feel about an 'additional reliable class' between you and your router? The fact that many "reliable" services have been hacked over the years has proven to be cloud-free.

4. UPnP is enabled by default

Browse the admin panel on the router, you will see that Universal Plug and Play (UPnP) is turned on by default. This network protocol, enabled on Internet ports, makes you the target of external attacks, because it is designed for local area networks (LANs), not the Internet. As a result, it has no security.



Therefore, activating UPnP is a big risk. Your router is basically a 'magnet' that attracts malware on the Internet and you don't want to 'open the door' for data labeled "UPnP". Take a few minutes to read the documentation that came with the router or find online help on how to disable UPnP.

Although you expect UPnP to be disabled by default, that's not always the case, especially on older router models.

5. Error managing HNAP

You may not be familiar with HNAP. The Home Network Administration Protocol (HNAP) is designed to allow ISPs to manage routers sold to customers. Although accessible by end users, it is especially useful for ISPs.

Unfortunately, it has a big flaw.

With HNAP, your router's device name and other information is revealed in plain text, without any form of encryption. This reason alone is enough for you to disable HNAP. The problem is, even if you set it up, it is usually not disabled. The only solution is to buy a new modem, or at least contact your ISP and show dissatisfaction. Hopefully, they will provide an alternative.

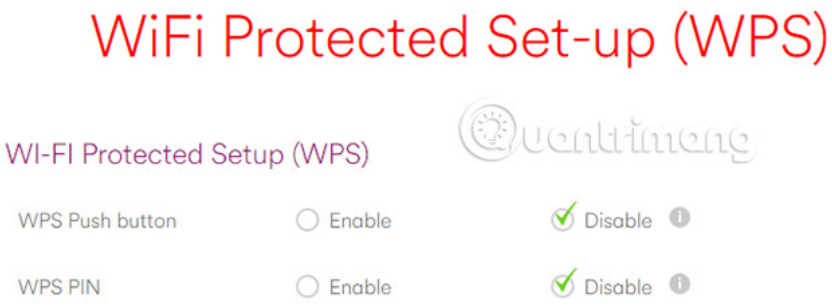
To check the HNAP vulnerability on your router, visit this URL: **http:/// [IP address of your home router] / HNAP1**

If you can get positive feedback from the router, you have a problem.

6. WPS is a security nightmare

1. How to hack WiFi passwords with holes on WPA / WPA2

Can easily allow visitors to your network without Wi-Fi password. All they need is the Wi-Fi Protected Setup (WPS) code, printed on your router.



This is an 8-digit PIN code that will retain the router's name and password. However, it is also a security risk.

First, the code remains the same (unless you force changes in the admin panel), so your visitors can access the network not just once. There is no basis to force guest users to authenticate every time they visit your home. That's not good.

Secondly, and perhaps more worrisome, is the PIN code. Although it seems to be an 8-digit PIN, but not. Instead, the first seven numbers are divided into two groups, one consisting of the first 4 digits and one group of 3 digits remaining. They are confirmed as sequential, while the 8th number acts as a checksum, so that the router can be accessed. But while usually an 8-digit group has 10 million combinations, this type of PIN has only 11,000 combinations. WPS will make a Wi-Fi network easily hacked.

1. How to hack Wifi passwords using Wifiphisher

That's a predictable code - a brute force attack will definitely do this very easily. The solution here is to turn off WPS from the router's web control panel.

7. Firmware is not stable

Updates downloaded from your router manufacturer or ISP will enhance device security. Your network will then become more secure. But sometimes that doesn't happen. For example, after updating the firmware, your previous changes to the router configuration (such as your admin password and your SSID, etc.) may be overwritten. Typically, the router is updated, but returns to the original installation and requires you to reconfigure it. This usually happens with updates from the ISP and is a good reason to use any of the profile storage facilities provided on the router's administration screen.

Other problems may occur. Unstable firmware installation may occur if the data is applied incorrectly or the updated image is deployed for incompatible devices. However, an unstable or reset firmware on the router can open the door for hackers to attack.

You can't do much about this. When it comes to ISPs, they will launch firmware without notice. Some manufacturers will tell you, but not all. The DD-WRT firmware flash on the router may be a good way, but it is not compatible with all devices.

The best way is to regularly log in to the admin panel and check the status of the router.

8. USB port

More and more routers integrate USB ports that users can access. This feature is increasingly popular and easy to understand why. With USB port, you can connect USB flash drive and hard drive to your router. This basically converts your router into a NAS box, a central data store. As a result, data on the drive can be accessed from anywhere on your home network.

In many ways, this is extremely convenient. But if your router is not secure, data on the USB drive may be accessed by intruders. Worse, the USB port may be targeted by an intruder with a physical attack.

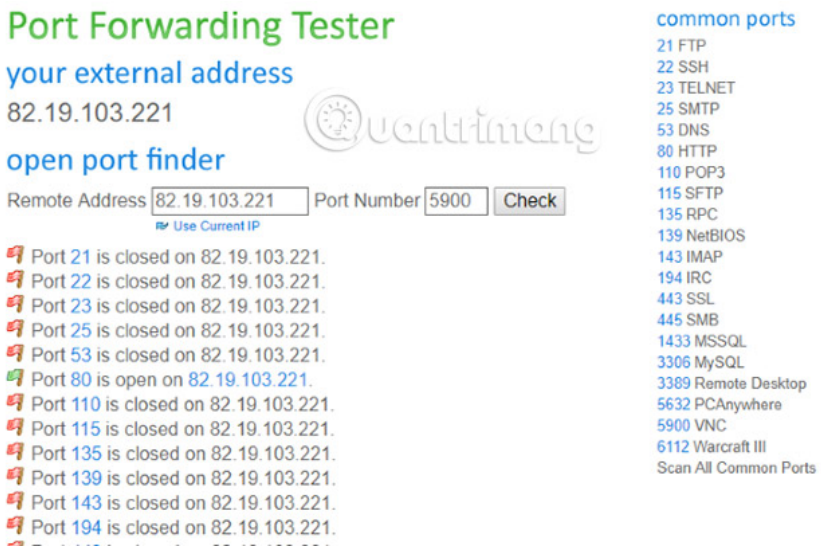
Everything will happen as follows: Someone posing as a salesperson, or even a friend knows, plugs a compact USB drive into the back of the router. Malware saved to the drive is designed to take control of your router.

Your router is now part of the botnet.

To prevent this from happening, disable the USB ports. If you prefer to use the router as a NAS box before, perhaps it's time to buy a new one. If you feel the cost is too great, you can use your Raspberry Pi as a NAS.

9. Other open ports

In addition to the ports mentioned earlier, it's easy to see that your router has other ports open. Some of them are necessary, such as HTTP, and most other ports do not. Unless you are running some dedicated device or project at home, you may not need open POP3 (110) port or VNC (5900).



To check if your router has opened a port number that you think should be closed, you will need a port test tool. Some tools are available online. For example, **https://www.yougetsignal.com/tools/open-ports/.**

Use these results to configure the router. If you do not use a specific service or protocol, there is no need to open the corresponding port.

10. Be careful with Misfortune Cookie

Misfortune Cookie that is said to be funny is like something from a Chinese restaurant, but can't be eaten, because it can make you indigestion.

This is a specific software vulnerability in about 12 million routers, until discovered, Misfortune Cookie is named so because of an error in managing HTTP cookies from affected devices. This error allows an attacker to take advantage of an HTTP cookie to exploit the vulnerability, damage the router and change the status of the device. For example, this may involve attachments to a botnet. Surely an attacker will use it to remotely access the router and other devices on your network.

Furthermore, routers can become targets in man-in-the-middle attacks, and disable the device's hardware firewall. Any computer, tablet, phone, entertainment system or IoT device on your network can be affected.

What can you do with this? Let's start by checking if you are affected. If so, the router's web control panel will not be accessible by normal login information.

To fix the problem, check with your router manufacturer. This error should be fixed in the update. If not, find a new router or see if your device is compatible with DD-WRT.

Hopefully now you have taken steps to fix problems with your router. You are required to do so, to prevent hackers from accessing the network or bots will hijack your router or PC control.

Because routers are so different, you will need to take some time to read the documentation that came with the device. All of these problems can be overcome - simply find the right place in the admin screen on your browser.

Have you encountered any security issues with your router? Are there any holes above that need fixing? Let us know in the comment section below!

See more:

1. Why should you restart the router regularly?
2. Restart the router and modem properly?
3. How to detect VPNFilter malware before it destroys the router