9 mistakes often get caught up in wireless networks

Just install once and run the broadcasting device, you will be able to easily access the network from a variety of different devices

Wireless network brings a lot of convenience for digital tech followers. Just install once and run the broadcasting device, you will be able to easily access the network from a variety of different devices .

However, the setup and installation of wireless networks is quite complicated, users often suffer from fairly basic errors. Here are 9 mistakes you should avoid when installing settings and using wireless networks at home or work.

1. Do not read the user manual

This is the mistake most people make. Wi-Fi settings depend on the router you have purchased as well as the device you will use to connect. Please use the instructions from the manufacturer to follow when installing. You will not make some mistakes below if you have read the instructions from the device provider carefully.

2. Use the default password

Users often do not care about the default password that wireless routers provide to log in to administration. To avoid being hacked, replace the default password with a more secure personal password.

3. Forgot to enable Wi-Fi relay on the device

Wi-Fi has become the current popular technology with the rise of smartphones

Mobile devices such as laptops or phones often have their own buttons or settings that allow you to turn on / off to receive wireless signals. Normally you will not be able to connect to the Wi-Fi network when the device is in 'standby' mode. Please read the instructions carefully to master the tool.

4. Select the wrong standard non-compatible devices

There are many wireless or Wi-Fi technology standards, such as 802.11a, 802.11b, 802.11g, and 802.11n. 802.11n is the latest technology that supports higher bandwidth as well as enables better signal broadcasting.

Chances are you have devices that support a variety of standards, so you don't have to be careful about these standards. However, keep in mind to avoid mistakes when selecting new, incompatible devices and supporting existing devices. Use a single standard if possible. In case a device does not support the overall technology of the system, they will cause the entire network to slow down or break.

That is why many generation routers do not support the old standards. If your laptop is not connected to the wireless network, it is likely that the router only supports 802.11g, while the connected device only "likes" the 802.11a standard.

5. Confuse coding standards

New devices often support different WPA encryption standards. Meanwhile, the old standard WEP still exists, less effective, can be compromised.

Most users choose WPA standard. If you use a device that supports only WEP, a PDA, for example, will not be able to access the network. Once again, it is necessary to confirm that reading the instructional information to understand the coding standards that the device supports.

If there is only one option, WPA, make sure that when you set up the system you have created a secure

password, such as 10 or more characters, with random words, letters and numbers. Don't skip setting up encryption. Even if WPA can be unlocked, it still takes a lot of time and effort for the thief to perform.

6. Configure poor firewall

One of the main reasons that a laptop cannot connect to the network is that the firewall has blocked the signal. To test, turn off the firewall and try again. If the firewall is the culprit causing the problem, learn how to configure the firewall accordingly to allow the device to "network".

7. Remember the wrong login information

Another common mistake is to remember the wrong login information. In case of setting up the network to connect, if there is a signal but cannot reach the network, it is possible that the WEP or WPA key you entered is incorrect. Please check again for sure.

8. Do not use any security measures

Wireless delivery data may become the target of a thief's attack. Security measures are essential. Using secure passwords, encryption, firewalls or using specialized tools to enhance security is a very practical suggestion. However, users are often quite indifferent to this. You can learn more about how to set up a secure wireless network here.

9. Don't know 'prevention is better than cure'

Some security measures you can perform include changing the default password, turning off DHCP (Dynamic Host Configuration Protocol), installing Dynamic Host Configuration Protocol (DHCP), turning off remote access, turning on the firewall. , install a dedicated firewall on your computer, hide SSID .

Meanwhile, many people enhance security by hiding devices (routers) in places where few people may be curious, accepting less signaling. This is really a fundamental mistake. Remember candles you can safely without even taking any security measures. Ideally, back up data, protect them with specialized tools that are not missing today.