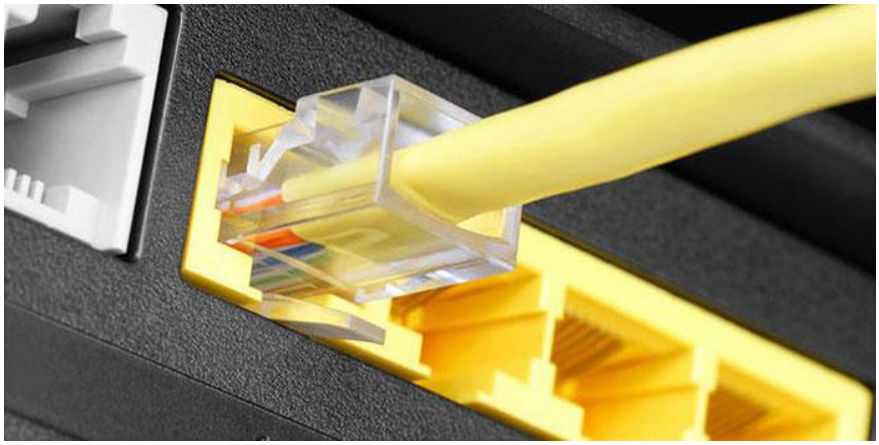
Tricks to improve wifi network security

The more developed the use of wifi network, the more problems arise, the unsafe wifi security affects the access speed. So how to improve the absolute security of home wireless network.

Currently internet usage is a daily necessity. The Internet helps to raise intellectuals and integrate into the world's technology community.

People today use the internet anytime, anywhere, especially the use of wifi, the more the use of wifi grows, the more problems arise, the wifi security. Therefore, home wireless networks may be the most insecure Internet connection. Users can be attacked from the Internet and even neighbors.

While no security measure is perfect, there are a few simple, standards-based tips that can be used to improve the security of your network. family wires and make attackers more difficult to access.



Always access the admin panel with Ethernet

Logging in to the router's admin panel is simply opening your web browser, entering the IP address (or sometimes the URL), then the router admin username and password. Everything is fine, as long as you do not do so on a wireless connection.

When logging into the admin panel over the wireless network, those credentials will be sent over the network and potentially intercepted. Signing in only when connected by Ethernet can eliminate this risk.

In fact, it is advisable to completely disable remote access and require a wired connection to adjust everything. This way, even if hackers interfere with the wireless connection and break the password, they cannot change anything.

Change network name (SSID)

This is a very simple measure, changing the default network name. An attacker knows the default name that router and ISP manufacturers use. If they can find out what kind of router the user is using just by looking at the network name, it is also much easier to attack the exact router. It saves them both time and effort.

In addition, this type of information opens the door for more sophisticated attacks, specifically attacking the router's firmware. An attacker can directly exploit the firmware and be more accessible and more discreetly if they only find out the password of the wifi owner.

Change the admin username and password

Similar to the above security method, users need to change username and password of network administrator. The attacker knows the default username and password and they will try those first.

Note, changing the admin username to something a little hard to guess. Password must be a passphrase. That means it must be a phrase that contains at least one or more words without meaning. Also use capital letters, numbers, and a few special characters.

Use strong encryption

Encryption is a must-use feature on all routers. Ignoring the use of encryption is like keeping all doors and windows in the house open. Anything said or done can be seen and heard by anyone.

If you don't use encryption for your wireless network, you make a big mistake. In fact, if you're using encryption, you can still make mistakes. Not all encryption is created equal. Make sure the user has chosen the right settings.

Seriously, it only takes about 30 seconds to enable encryption in the router settings. And when doing so, make sure to use WPA2 mode if it is available, or not then use WPA Personal. In any case, do not use WEP encryption, as it is weak and easy to crack.

Turn on the firewall

Not every router has a built-in firewall, but if the user's computer does, turn it on. Firewalls can act as the first line of defense. They are specifically designed to manage and filter traffic coming in and out of the network and can block access through unused ports.

Turn off WPS

WPS stands for Wifi Protected Setup. This is a system connected to an encrypted wifi network without entering a password. There are some differences, but all are relatively similar. Although WPS can work well in theory, it's not really that good. WPS can cause a number of security holes. It is enabled by default on most routers. If you feel you don't need WPS, you can disable it and close these security holes.