# How to be safe on a wireless network

Most people enjoy the benefits of wireless technology. Wireless networks obviously bring many advantages to users, and they can be vulnerable if you don't have security.

**Most people enjoy the benefits of wireless technology. Wireless networks obviously bring a lot of advantages for users, and they can also be vulnerable if you don't have the appropriate security.**

Unfortunately, the structure of wireless networks has weaknesses outside the device and even when you enable the default security features, it is still not safe. However, with some insights into wireless technology and a few tips can help you avoid this.

**Step 1: Understand your network**

Consider how wireless networks work. In 'wired' technology, data is transferred from your computer to the web via a cable connection to physical ports, while Wireless technology uses radio waves to transmit data. The signals that carry your data are broadcast on a wide range and anyone in that coverage area can receive this signal.

**Step 2: Change your SSID and password**

This method has a significant effect. For each wireless network, from large corporate systems to small and

simple family settings, the set of identification numbers (SSIDs) is the name of your network number. To prevent your signal, you should do the following two things: First, you change the SSID and password number from the **default** to **private settings and strong** , the default SSID can help familiar hackers in each company can Setup and penetration is as easy as eating cakes. To change the SSID and network password, you must run the software for wireless hardware. You should change the SSID within the program's preference.

Overwriting the default SSID will not be better if your network name is notified to everyone. To keep your information private, you should disable the SSID broadcast. This is as simple as a mouse click in the program's preference.

**Step 3: Set up MAC filter**

Changing the SSID without changing the MAC filter is like changing the home key and forgetting the key inside. MAC (Media Access Control) filter helps you control who can access the network and who doesn't. It takes a little time to set up MAC filtering, but without it hackers can roll in and use your network.

To allow specific computers to use your network, you should add their MAC addresses. The 12-digit address is mounted on each network device (PC, laptop, router). MAC filtering is a different process for each manufacturer, but in most cases, opening software and locating security settings often takes you to the right place. Finding the MAC address for each device can also be a challenge if you don't know where it is. Click here to see instructions that will help you find inside your system.

**Step 4: Encryption**

There are two types of encryption protocols: WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access). Both block intruders by confusing the data. It seems that WPA is of great interest because of its dynamic nature, and its constant key change. However, the encryption key you did not expect is also different for each device and WPA is not as popular as WEP. On the other hand, if you don't have access to WPA code, the combination of WEP and MAC filtering is enough to prevent mediocre hackers. WPA is built into most new routers along with WEP, unless your network components support WPA, WEP will still encrypt by default.

**Step 5: Fill the gap with the software**

With all security settings, hackers can still have their hacks, all of which need extreme patience and appropriate tools. Programs that can help you like Trend Micro PC-cillin, ZoneAlarm Internet Security Suite, and McAfee Wireless Home Network Security, these programs check your network and show you when penetration occurs. An AOQ product called Active Security Monitor can diagnose your wireless security and remind you to innovate.

**Pham Van Linh** ( *According to CNet* )
**Email:** vanlinh@quantrimang.com