8 steps to increase security for wireless routers

Most IT equipment today has plug-and-play capabilities, but there is one device that you should never use this way: a wireless router.

The router is perhaps the most important gadget in your home. It checks all incoming and outgoing traffic, acting as a sentinel to ensure that nothing dangerous happens, and that nothing sensitive gets out.

The router controls access to your home WiFi network and all phones, tablets, and laptops. etc. connect through there. Therefore, it is essential to keep the router secure.

The good news is that doing this isn't too difficult or time-consuming, but it will significantly reduce your risk.

Here are the steps to take to increase the security of your wireless router.

1. Log in to the router and change some settings

The first thing you should do when you get a new router is log in to the device's *control panel* , then change the Wi-Fi connection password, the type of security protocol the router is using and the name. identify the router.

However, most importantly, you need to change the name and login password for the device's *administrator account.*

Some routers do not allow you to change the admin account name but still allow changing the password of the account that holds administrator rights for this device. If you don't do this, bad guys can gain access to your home network, log into the control panel, and take ownership of the router by using the device's default settings.

If you don't know how to log in to the router, see the accompanying documentation, ask your Internet service provider (ISP), or try to find the user manual for the router you're using on the Internet.

2. Use long and difficult to guess passwords

You should use a password that is about 20-30 characters long, a random mix of letters, numbers, and special symbols *(if allowed)* . If you have a lot of passwords to remember, you should use a password manager to remember them.

3. Use WPA3

Security protocols for routers improve over time, which means old protocols are outdated. The latest standard, called WPA3, encrypts your WiFi connection, making it harder for cybercriminals to guess your WiFi password.

If your router and other devices do not support WPA3, you can use the previous standard called WPA2-AES. But any models that are still using WEP need to be replaced immediately. They are simply not equipped to handle today's threats.

4. Always update the router's firmware

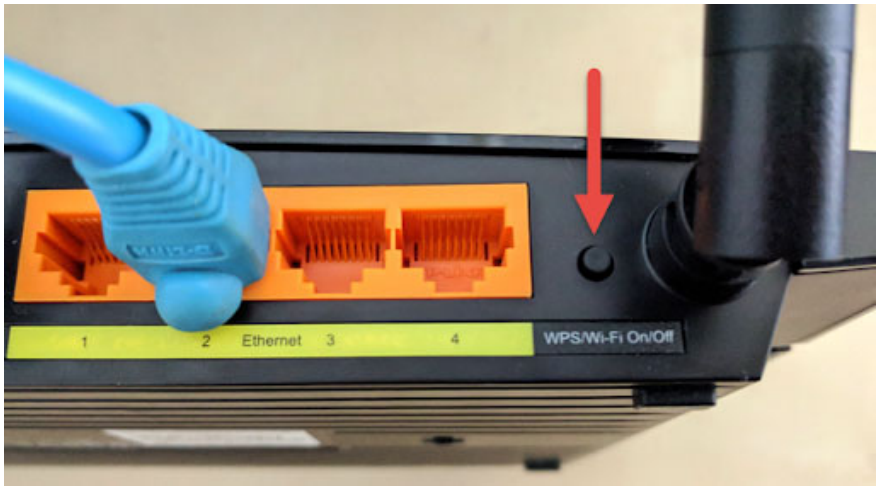
Routers run low-level software called firmware, which essentially controls everything the router does. It sets security standards for the network, defines rules about which devices can connect, etc.

Some more modern routers update themselves in the background, but no matter what model you have, it's always worth making sure the firmware is up to date. This means you've got the latest bug fixes and security patches, which can protect against any discovered exploit attacks.

The update process varies from router to router, but like password settings, the option to update router firmware is not too difficult to find in the router control panel. If you have difficulty, check your router's documentation or the official support site on the web.

If you're lucky, the process will happen automatically. You can even get notifications on your phone every time the firmware is updated (this usually happens at night). Otherwise, you may have to download the firmware from the manufacturer's website. Reference: How to upgrade Firmware for Wireless Router? For more details.

5. Disable remote access, UPnP and WPS



Many routers come with features designed to make remote access outside the home easier. But unless you need admin-level access to the router from elsewhere, you can usually disable these features safely from the router settings panel. Besides, most remote access applications can work fine without them.

Another feature to look out for is Universal Plug and Play. Designed to make it easier for devices like game consoles and smart TVs to access the web without making you go through multiple configuration steps, UPnP can also be used by malware programs to gain access Advanced access to router security settings.

If you want to be as secure as possible, disable remote access and UPnP. If some applications and devices on your network rely on them, you can re-enable the features without worrying too much.

You should also think about disabling Wi-Fi Protected Setup. WPS lets you connect new devices with the push of a button or a PIN, but it also makes it easier for unauthorized devices to gain access. Unless you specifically need it, disable this feature.

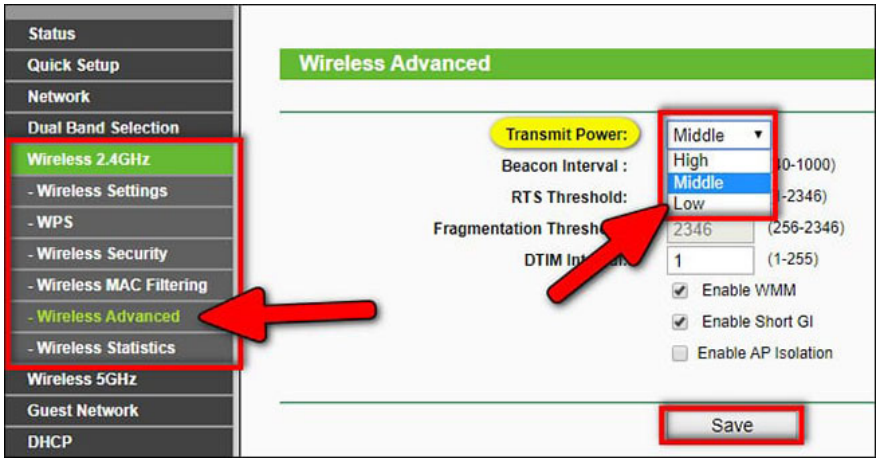
6. Reduce the power of the wireless transmitter

In many cases, people do not need the wireless router's WiFi transmitter to operate at maximum capacity.

Of course, you might have a large house and need to set up an additional access point to expand the WiFi network's range so that it covers the entire area of ??the house. But if the router is doing enough for your small apartment, try reducing the transmission power so it only goes to the places where you really need to use your wireless network.

The idea is simple - It is to make the wireless network inaccessible from outside your apartment.

If you set the transmit power to **Low** in the router settings, potential hackers will not be able to connect to your hotspot from the outside due to the weak signal.



7. Change the IP address range to Non-Default and disable DHCP server

First, you can switch to subnet **192.168.201.0** instead of continuing to use the default **192.168.0.0** or **192.168.1.0 subnet.**

Second, you can manually assign static IP addresses to all devices on the network. This will make the process of getting the correct IP address much more difficult.

8. Stop using mixed standard mode

Similarly, you may want to switch your router to the WiFi 5 or WiFi 6 standard and cut off support for previous standards.

If you want to try it out, just log in to the router configuration page and change the **'802.11a/b/g/n/ac mixed'** mode to **'802.11ax only'** or **'802.11ac only'.** On some routers, you may also find the **'802.11ac/ax' option.**

This will make your WiFi hotspot visible only to clients that support the latest generations of standards.

Why do that? The answer is simple: by adopting such measures, you will narrow the circle of devices. And the fewer devices connected, the better the performance.

You finished reading the article "**8 steps to increase security for wireless routers**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.