How to secure WiFi network, increase security for WiFi

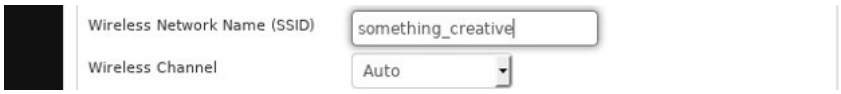
To secure WiFi there is no perfect method, you need to use a combination of tricks and tools to ensure the WiFi network is safe. Here are ways to secure WiFi that you can refer to.

Everyone uses wifi. It is a fact of modern life, but it comes with some serious security risks. The home wireless network may be the most unsafe Internet connection. You can be attacked from the Internet and even from your neighbors.

Although no security measures are perfect, there are some simple steps you can take to improve the security of your home wireless network and make it harder for attackers to access.

1. 4 steps to set up your home wireless network
2. How to know who is "using the temple" Wifi your home or not?

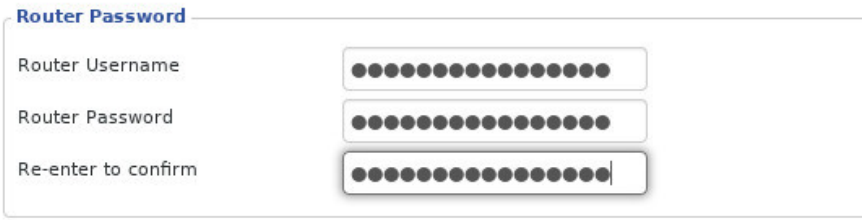
Change network name (SSID)



This is a very simple measure, changing the default network name. The attacker knows the default name that routers and ISP manufacturers use. If they can find out what type of router you are using just by looking at your network name and being able to attack the router more easily. It saves them both time and effort.

In addition, this type of information opens the door to more sophisticated attacks, attacking the router's specific firmware. An attacker can directly exploit the firmware and have more access and a more discreet way if they only find your password.

Change username and password



Similar to the above security method, you need to change the username and password of the network administrator user.

Attackers know the default name and password and they will try them first. Don't think you're smart just by changing your password or changing a character. An attacker has a tool that can quickly check thousands of ways to combine passwords and usernames.

Changing admin username to something is a little difficult to guess. Password must be a passphrase. That means it must be a phrase that contains at least one or more non-meaningful words. You should also use capital letters, numbers, and some special characters.

Use strong encryption

If you don't use encryption for your wireless network, you've made a big mistake. In fact, if you are using encryption, you can still make a mistake. Not all encryption is created the same. Make sure you have selected the correct settings.

Select **"WPA2 Personal"** for your network. It would be great if you could set up the business version, but it really wasn't easy unless you had some experience with it.

For encryption algorithms, select **AES,** do not use TKIP. AES provides stronger encryption and is difficult to exploit. TKIP is only selected as an option for backward compatibility, and if you really need TKIP, update your device.

Choose a strong password

The password you use to log into the network also needs to be strong and it needs to be different from the password for the administrator account. Choose a long password, including at least one least-used word, numbers and special characters. Your password must be at least fifteen characters long.

Change WiFi password

Even if your Wi-Fi password is extremely strong, you need to change it. Like any password, you should regularly change new phrases. That doesn't mean you need to change your password every day, but every few months is a bad idea.

Disable guest network

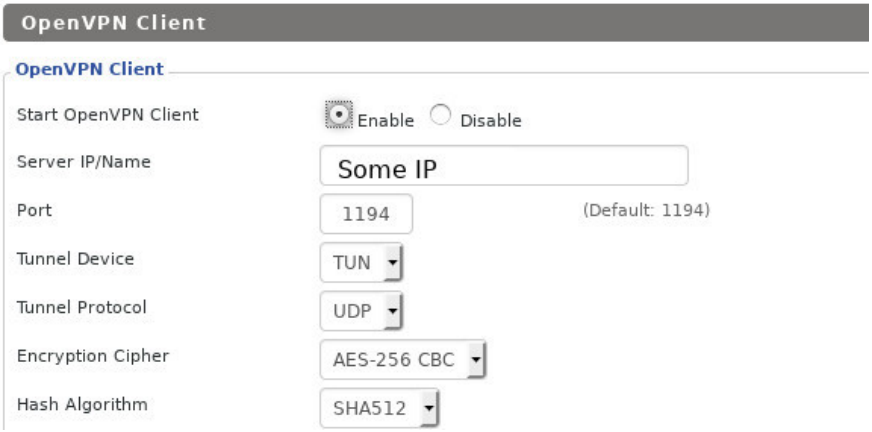
The guest network may be a double-edged sword. Make sure, your guests do not log in and access your entire network, and they do not use your password. However, if the guest network does not have a password, you are still open to anyone who wants to connect. Basically, you are giving an attacker an opportunity to access your network.

The only exception here is if you can create a separate password for the guest network. It's okay if your guest network has the same security level as the main network. If not, disable it and if you don't trust your guests, change the password when they leave.

Turn on the firewall

Not every router has a built-in firewall, but if your device does, turn it on. Firewalls can act as your first defense. They are specially designed to manage and filter traffic to and from your network and can block access through unused ports.

Use VPN



You will not prevent your neighbors from entering your network with VPN, but you can prevent attacks from outside the nearest area that way.

When using VPN, first connect to the VPN server, then connect to the external Internet. All traffic comes from VPN, including any information about your local computer network because VPN creates virtual local networks. While connecting to them, your computer is on both the physical intranet and the virtual network. Internet can only see virtual network.

VPN has the added benefit of anonymizing part of your traffic. A VPN will not make you completely anonymous online, but it will definitely help.

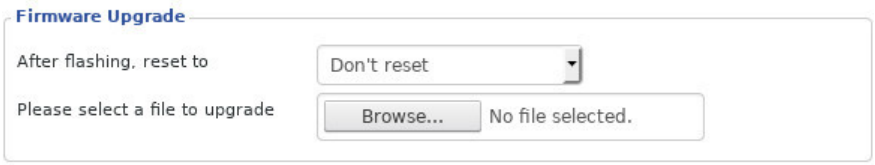
1. 11 best VPN software

Turn off WPS

WPS stands for Wifi Protected Setup. This is a system that connects to an encrypted wifi network without entering a password. There are some differences, but all are relatively similar.

Although WPS theory can work well, it is not really that good. WPS can cause some security holes. It is turned on by default on most routers. If you feel you do not need WPS, you can disable it and close these security holes.

Manage router firmware

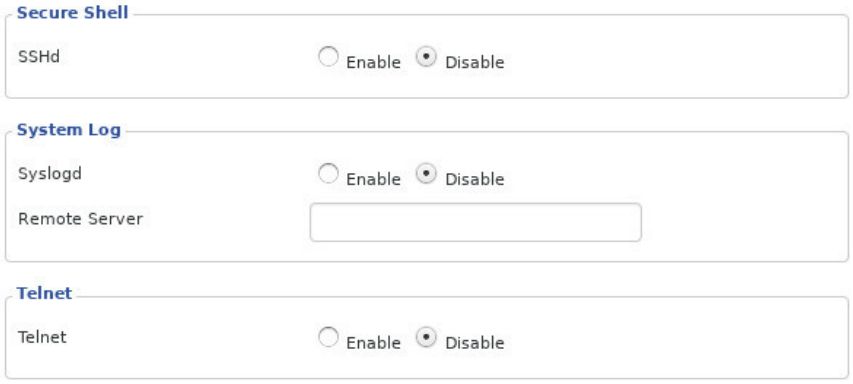


Like computers, routers have an operating system. However, it does not automatically update security updates like computers, so you need to update it yourself. Some routers may download firmware updates from the Internet. For other routers, you must download them yourself and upload the router from your computer.

As with computers, updates often include important security fixes. If you don't update, attackers will take advantage of these security flaws to attack you. You do not need to do this regularly, just check monthly updates or longer.

If you have a bit of technology knowledge, you can consider using a custom open source router firmware. There are a few really great tools that you can upload to your router and it is often updated quickly and more features. If you've never done this before, be careful because you can destroy the router.

Turn off remote management / unnecessary services



Many routers have remote management services. In some routers, these services are enabled by default. Do not confuse here. This is not the web interface that you use to manage routers from within the network, remote services allow you to manage it from the outside. That means an attacker from the open Internet can access your router management interface. There are not many practical reasons why you need to manage your router from outside the network, so you won't miss many things if you turn off this potentially dangerous service.

There are other services that the router comes with is not necessary. For example, some routers with SSH or Telnet are enabled by default. There is no reason, especially because you can use the router's web interface. Some routers even have FTP and Samba enabled by default for file sharing. Both can make network attackers easier. If you have them, turn them off.

If you are interested in security topics or you have read an article like this before, you may wonder why some things are not mentioned. A good question! Static IP addresses, MAC filtering and SSID hiding are ignored because they have been proved inactive. Sure, you can prevent some mild interventions, but for the right tools, none of these tricks are effective. You should invest your time and effort when it achieves results like strong encryption and password.

Be smart and try your best to make sure your router is protecting you.

You finished reading the article "**How to secure WiFi network, increase security for WiFi**" 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.

© 2019 TipsMake.com