Wi-Fi security is better than hiding the SSID

Hiding the SSID will make your Wi-Fi network safer with the risk of unauthorized intrusion. This article will show you how to hide Wifi networks, discuss security issues when hiding this network.

Wireless networks are less secure than wired networks. It is simply due to the nature of the broadcast-based communication mode. Therefore, Wifi security is always an important issue. There are a number of ways to minimize Wi-Fi access, and one of the first things users often do is to hide the Wifi network and the router so that others cannot connect to the hidden network. This article will show you how to hide Wifi networks, discuss security issues when hiding this network.

Why should Wifi network be hidden?

According to IEEE 802.11 standard, each wireless network must have an identification number used by the device to connect to the network called a Service Set Identifier (SSID), which is easily understood as the network name.

Every 100 milliseconds, the router will broadcast the beacon frame, which is a signal transmitter containing information about the network, including the SSID, to indicate that the network exists. If the router is like a human and it will say 'I'm here, my name is Cisco04022. If you hear me, you can use that name to connect with me. ' Here's how your phone knows about all the Wi-Fi networks around. If you prevent the router from notifying other devices about the existence, it will become invisible. And the device will not know and cannot connect.

The limitations of hiding network SSID

Wireless signals are the same, they start at a source (router) and go in all directions (like a constantly expanding sphere). There is no way to capture the signal transmitted in a beam from the router to a specific device and even when you can aim it, you cannot stop this signal as soon as it transmits to the device.

Let's say your wireless network does not play SSID, no one knows its existence except you. You establish a connection with it and use the Wifi network as usual. However, when accessing the website, the router will broadcast a signal to get the website data and computer. Do you see any problems here? Wifi signals must be transmitted through open air to the computer, so anyone within its radius can block this signal.

In other words, even when you hide the SSID, hackers and other malicious users can still detect it by blocking 1) the device signal transmitted to the router and 2) the router signal transmitted to the device.

How to hide SSID or hide WiFi network

As mentioned above, hiding WiFi network cannot guarantee the security of your WiFi network. However, at present, in some parts of the world, it is not required to display WiFi name in public mode, so it is necessary to hide SSID.

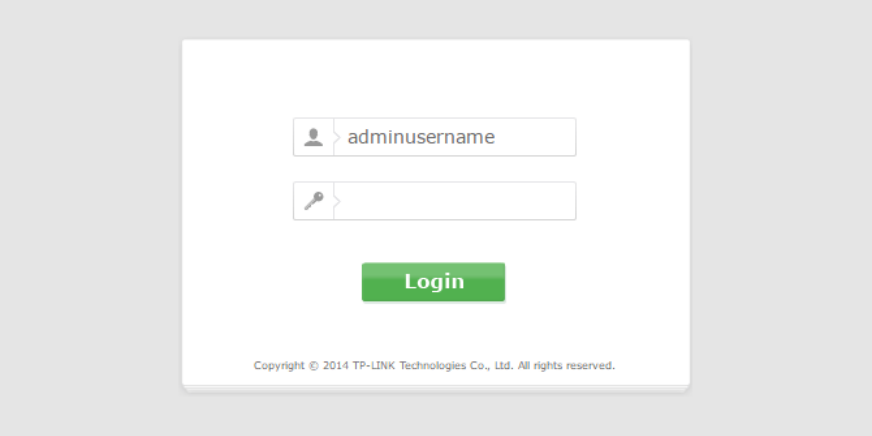
Depending on the type of router and manufacturer, hiding SSID may be different because you need to access the Router configuration page to proceed with a different IP Router address. For example, most Netgear users can access this configuration by going to routerlogin.net. Note, you need to connect the wired LAN to the router to log in to the browser.

Step 1:

In the web browser, we access the router's configuration page. Typically, the IP address will be in the form http://192.168.0.1 or http://192.168.1.1. Or more precisely, see the device for IP address.

Step 2:

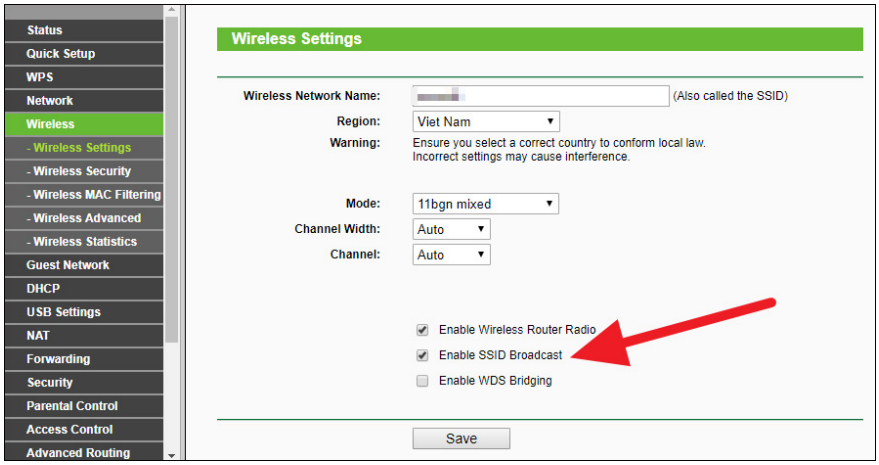
You enter your User login and password according to the information provided on the Router device or in the manual.



Step 3:

Next, look at the navigation bar of the **Wireless** section. If you have a small menu, you can find something similar to **Wireless Settings, Wireless Options, Wireless> Basic Settings** , etc.

You can adjust the SSID, channel, channel mode, channel width on this page, but here you need to find the **Enable SSID Broadcast** option and uncheck it. Depending on the router model, it has other names such as **Visibility Status, Enable Hidden Wireless** or **SSID Broadcast:**



The hidden WiFi, hidden WiFi network SSID is not a way for users to secure WiFi networks. It simply doesn't show the WiFi network name on the WiFI network list on laptop or mobile devices. Thus, we will only limit the situation of unauthorized access, access the 'pagoda' to WiFi network.

If you really want to secure your network, you need to do the following necessary tasks:

1. Change default admin information. Just a quick search on the Internet you can see the password, the default admin username of most routers. If you do not change this information, other security settings become useless. This is the first thing you need to do for any router.

2. Encryption using WPA2 and AES. As mentioned above, routers always signal in all directions, but you can encrypt them so that they are not blocked. This means that only your computer can read the signal.

3. Disable the WPS and UPnP features. These are convenient features that have many major security holes, mainly the ability to break other security features (such as firewalls), so you should turn them off as soon as possible.

Other tips for Wifi networks at home

When setting a password for the network, make sure you choose a strong password and this applies to both the administrator password and the Wifi connection password.

If you have a wireless dead zone or poor Wi-Fi signal in your home or apartment, you can solve it using either a Wifi extender or a powerline adapter.

See more:

1. Additional ways to Wifi for desktops
2. Instructions on how to retrieve saved Wi-Fi passwords on computers and laptops
3. Instructions for fixing Wifi errors with yellow exclamation

I wish you all success!