

How to check who is using Wifi temple, your home WiFi theft

The network administrator will guide you how to see who is using Wifi Temple with Wifi management software and some tips to detect if your Wifi network connection is being stolen and to find ways to prevent the situation. that again.

Today the role of wireless networking like Wifi is undeniable. People, home use Wifi to access the network. People using laptops, tablets, smartphones, digital cameras, printers, gaming devices, smart watches and many other devices can connect to each other or connect to the Internet through Wifi connection. However, how to set up Wi-Fi for safety and strong password is enough to make users headaches.

Of course, setting up your Wifi network like WPA2 settings and strong passwords is extremely important. But this does not mean that others cannot know what your Wifi password is. Even if you change your Wifi password regularly, your password can still be revealed when your friends, neighbors or family members share Wifi information with others and even people you don't know. Can access your network connection and use. This is one of the reasons why your network connection is getting slower and slower without you even knowing it.



Although many routers are manufacturers integrating additional security measures such as MAC address filtering, but others, especially hackers can also break these configurations. Many modern routers give you a list of wired and wireless devices to access the network connection, but some other routers do not. Therefore, some people will not know who is accessing, connecting and using their Wifi 'temple'. In the following article, Network Administrator will guide you how to see who is using Wifi Temple with Wifi management software and some tips to detect if your Wifi network connection is "being stolen" or not. and to find a way to prevent it.

In addition, readers can refer to the steps of Wi-Fi security better with hiding the SSID here.

How to see who is using your Wifi

1. View Wifi users by checking signal lights on the router
2. Use the Router's web interface to see Wifi users
3. Use Wifi Wireless Network Watcher management software
4. See users who steal Wifi with SoftPerfect WiFi Guard
5. Use network management software Advanced IP Scanner
6. Check wifi users with Angry IP Scanner
7. See who is using Wifi with Who Is On My WiFi
8. View Wifi users on Android using ezNetScan
9. View Wifi users on iPhone with IP Network Scanner
10. What to do when Wifi is used?

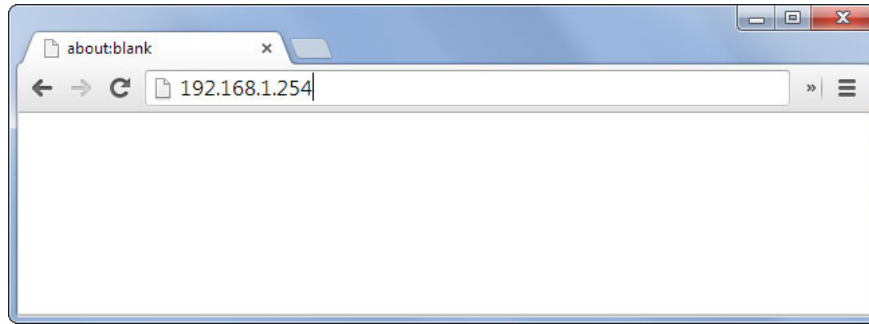
View Wifi users by checking signal lights on the router

Wifi-based routers often have signal lights to report when there is a device using a wireless network. Therefore, one way to help you check whether your Wifi is used by others "use the temple" is to turn off all your wireless devices and see if the indicator light on the router continues to blink or not. . However, this can also be annoying if you have multiple devices that are connected to Wifi, and checking this way doesn't give you too much information. Therefore, you may need the solutions below.



Use the Router's web interface to see Wifi users

Wifi transmitters have tools to help users see the list of devices that are connected to Wifi. What you need to do is access the router's web interface to find that list. First, enter the router's IP address into the address bar of the browser. On Windows, you can find the IP address of the router by accessing the **command prompt** (press the **Win + R** combination and then enter "**cmd**"), then enter **ipconfig** in the window that appears. Find the "**Default Gateway**" line and this is the **router's IP address** . On the Mac, go to **Network Preference** and the IP address of the Wifi transmitter is the address next to the "**Router**" section .



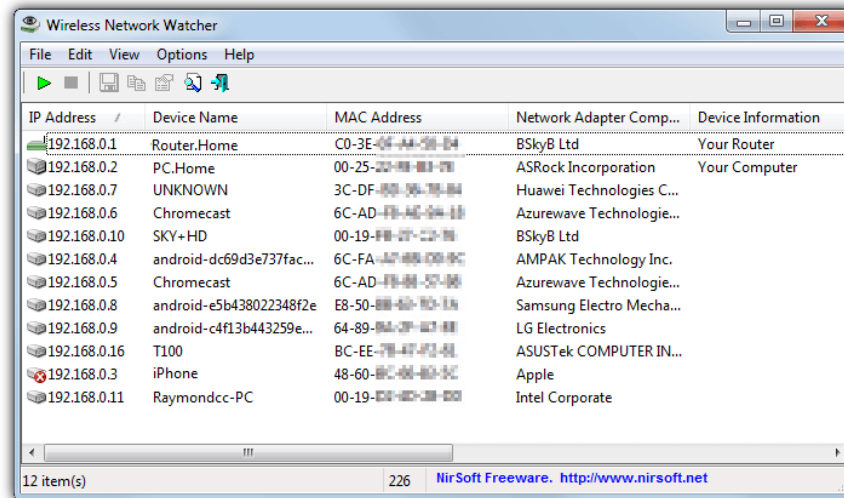
After entering, you will be prompted to login to the router account. This account is often accompanied by instructions when buying a transmitter, and usually has a username and password "**admin**". Note that if you have not changed the password of this account, you should replace it immediately if you do not want to be exploited by a hacker.

After entering the web interface, you find the items related to the list of connected devices. Here we can only say that in general because the location of this list will depend on the manufacturer's router. For example, **Netgear**'s router will be "**Attached Devices**", or some other router is called "**Device List**". Here you will be **provided with a list of IP addresses, Mac addresses, and device names** (if the router recognizes them) connecting to the Wifi network. You compare this list with your devices to see if Wifi is being used by strangers.



Note: Many people assume that the DHCP list on the router also shows the devices that are connected to Wifi, but this is not true. DHCP - the automatic configuration protocol for IP addresses, only showing DHCP clients: Devices that receive the automatic IP address provided by the router. If he encounters a slightly hefty hacker, he can access Wifi using static IP to bypass the list of DHCP.

Use Wifi Wireless Network Watcher management software



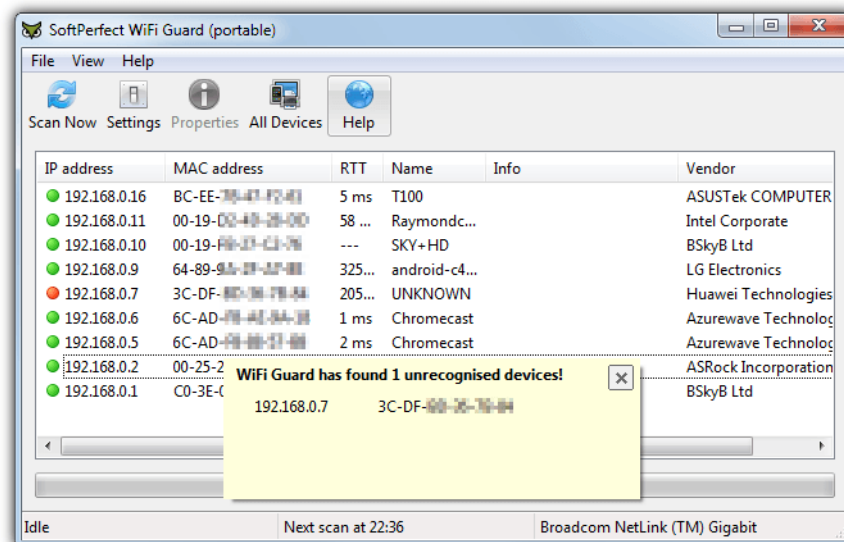
Nir Sofer's Wireless Network Watcher is one of the utilities that supports users who can detect who is connecting to their Wifi. The highlight of the utility is that it does not require setting up an IP address range and starting to scan the network connection automatically for connected devices. If you want to scan another network or range of other IP addresses, you can use the **Advanced Options** option by pressing the **F9** key.

The IP address scan process is quite fast and takes only a few minutes, after which you will receive information such as IP address, device name, MAC address, network card manufacturer, active status. dynamics and detection points.

Wireless Network Watcher is an open utility, this utility scans the background via an IP address range to detect new devices and disconnected devices. You can set up a notification and alert sound when the utility detects new connected devices or disconnected devices with your Wifi network.

Download Wireless Network Watcher.

See users who steal Wifi with SoftPerfect WiFi Guard



WiFi Guard is a utility based on SoftPerfect Network Scanner version - one of the utilities to detect unknown network connections or unauthorized connections. This tool will scan your network to find connected and connected devices, then scan again and display a popup notification window if any unknown network connections are detected. .

If you use and activate more than one network card, the program will display a setting window so you can select the network you want to scan. Or else you will be 'taken' to the main window, where you click the **Scan Now** option to scan all devices connected to your network connection.

For connections marked with a red check mark, the connection is allowed, double click on it and check the option ' **I know this computer or device** ', the program will ignore that device and will Do not scan the device again.

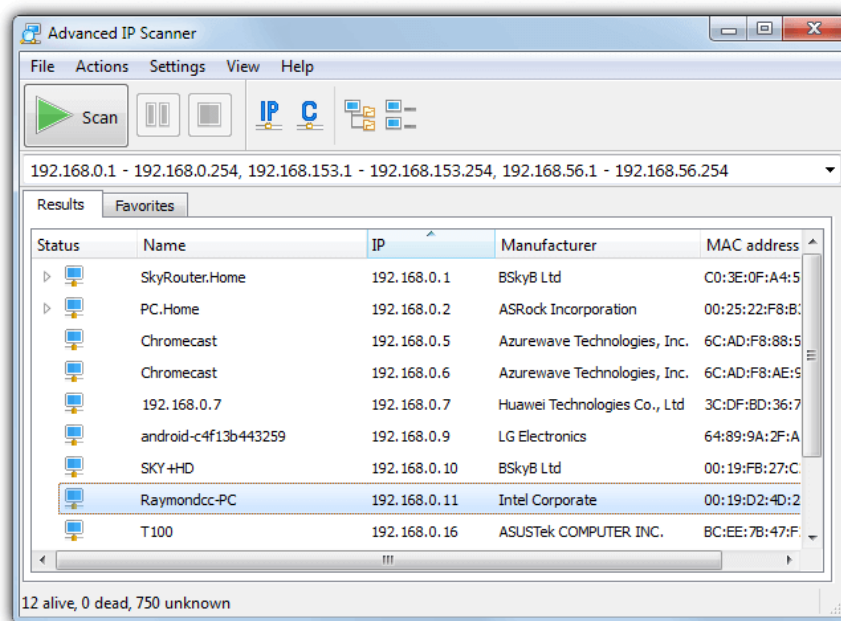
Running or minimizing WiFi Guard will scan again between 0 and 60 minutes (default is 30 minutes) and the screen will display a popup popup window if new devices of unknown origin are detected.

And as mentioned above, Softperfect Network Scanner is one of the most comprehensive utilities for scanning and Admin tools. This utility can also be used to scan and identify wireless network connections, but it will not scan devices at all intervals and give you warnings about unknown connections. origin.

Both WiFi Guard and Network Scanner have Portable versions (no installation required) and an installer version.

Download Softperfect WiFi Guard.

Use network management software Advanced IP Scanner



This is a Network Administration tool that can perform some additional tasks to scan your network connections. The tool also has a remote option to turn off and open the LAN, connect via HTTP / FTP as well as remote control with Remote Desktop and Radmin. Of course, these features are not necessary if you simply want to scan your wireless network connections.

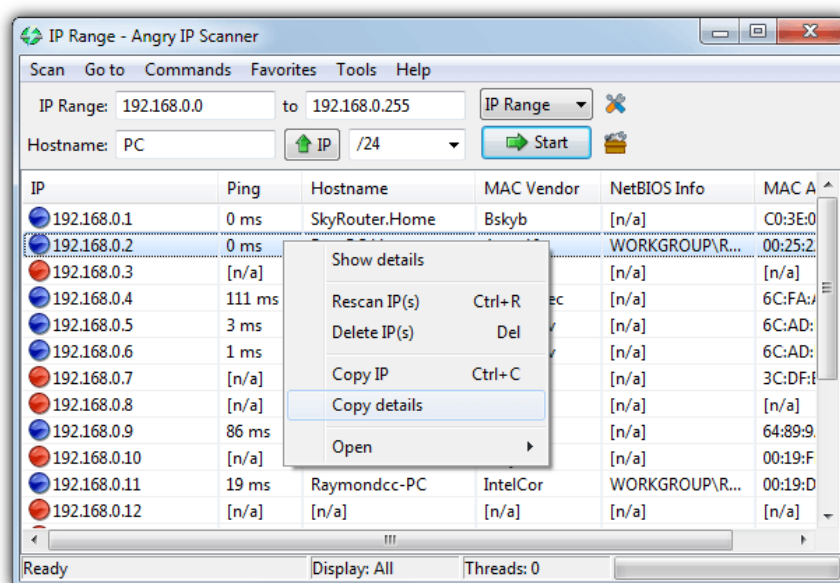
By default, Advanced IP Scanner will set the IP address range for all connections on the computer, only the range of Wifi connection is required, such as 192.168.0.1 - 192.168.0.254.

If there is only one active connection, you do not need to 'touch' the IP address range. After the scan is complete, all connections will be displayed with the names of wireless device manufacturers, MAC addresses and the name of the Advanced IP Scanner program.

Advanced IP Scanner has a Portable version, so you don't need to install the program, just run the executable file.

Download Advanced IP Scanner.

Check wifi users with Angry IP Scanner



Angry IP Scanner is a cross-platform tool that works on Mac and Linux quite well because of Java-based tools. This means that your computer must have Java Runtime Environment installed. This tool simply pings each IP address within the selected range and then displays the results along with the information you requested in the **Fetchers** window.

To select the address range to scan, you can enter these addresses manually or click the **IP** button and select your network card correctly. Then click on the dropdown menu to select the range, such as / 26 will scan to 63 (/ 26 will scan up to 63), / 24 will scan to 255 (/ 24 will scan up to 255).

You can also choose your IP address file list if you want to set up more complex.

The scanning process is quite fast because the scan program uses multiple threads. To see the results of all scanned addresses, go to **Tools => Preferences => Display** and select " **All scanned hosts** ", this will show you other devices that can connect to the network connection. of you without responding to the ping command.

Angry IP Scanner is available in both Portable version and installed version.

Download Angry IP Scanner.

See who is using Wifi with Who Is On My WiFi



This tool is different from the above tools a bit because the main task of this tool is to identify computers that are connected to your network connection and will warn you if any strange device is detected. .

However the most useful feature of the tool Who Is On My WiFi is to block unknown connections or 'fake' connections only available if you subscribe to a paid subscription, and every month you will have to pay a fee of \$ 9.95. However, the free version still allows users to find and scan devices connected to your network connection.

To use the tool, you must first configure the address range to scan, by default click the **Set** button and enter the address range you want to scan on your network, such as 192.168.0.1-254 . If you are unsure, you can access the **Diagnostic tab** on the Settings window and then click **Detect IP Ranges** to see what network connection you are using.

Then perform a scan and the connected devices on your network will be 'detected'. Select all the connections you know and set the status to **KNOWN** from the drop down menu, then select each one.

If setting Who Is On My WiFi runs in the background, the tool will display a popup window with a notification sound when any strange device is detected.

By default the tool will scan every 5 minutes although you can change this time to be between 2 and 10 minutes in the installation window. To make sure Who Is On My WiFi is turned off, you can open the system tray and check.

Download Who Is On My WiFi.

View Wifi users on Android using ezNetScan

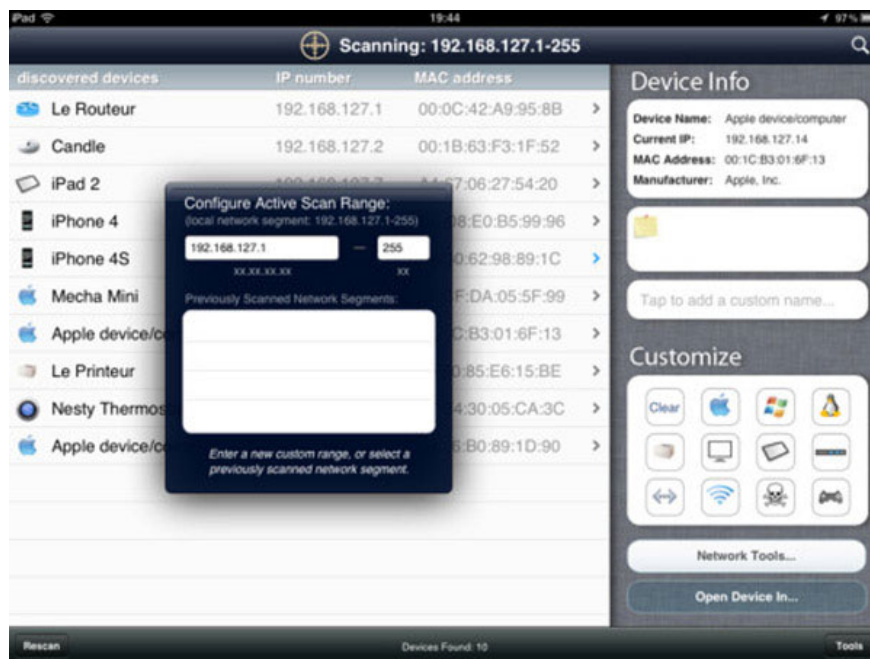
This is a free application that can scan all devices using your Wi-Fi network, then list in a full list of detailed information. The list will display the names and icons of those devices, you can easily identify a strange phone or laptop using your Wi-Fi network. Besides, the application also provides full IP address, time and usage of those devices.



Download ezNetScan for Android.

View Wifi users on iPhone with IP Network Scanner

This is also a free application, allowing you to detect strange devices using your Wi-Fi network. Although the features are not diverse and the list shows incomplete information about the device like the ezNetScan application, but this is still a useful application, works quite effectively and accurately.



Download IP Network Scanner Lite for iOS.

What to do when Wifi is used?

1. Change password

In case of finding out who is using Wifi Temple, **you need to change the router's password immediately** , and note the application of high-end security standard **WPA2-AES** . At this point, the WiFi thief will be "kicked" out of the network and unless he gets a new password (or a way to hack Wifi), it is impossible to penetrate the Wifi network.

2. Tracing the culprit

Many people believe that tracing the culprit in this case will be very difficult. IP addresses and Mac addresses may not be enough to help you do this. However, with the help of **MoocherHunter** application, this is entirely feasible. This is a very useful tool and is used by law enforcement agencies in Asia to track down Wi-Fi steals. As described, this software can identify the culprit's location through the traffic that they send over the network. The difference, the error of position is only . 2m.

The software requires you to burn the CD, then you will use it to boot the device. In this way, you can insert the disc into your laptop, take advantage of the WiFi card's orientation antenna to go around and determine the culprit's location. However, if you "act" alone, you should not rely on the software results to conclude the culprit, which can lead to unnecessary conflicts. It is like a way to help you determine who he is.

Refer to some of the following articles:

1. Wifi on Windows 10 does not connect after starting from Sleep mode
1. This is how to reset network settings on Windows 10 with just one click
1. This is a way to prevent hackers from stealing your data when using public Wifi
2. When detecting someone using Wifi temple, do the following to prevent

Good luck!

You finished reading the article "**How to check who is using Wifi temple, your home WiFi theft**" 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.