Restore and secure Wi-Fi encryption key

Have you ever forgotten your WEP or WPA key or password for your Wi-Fi network? In this tutorial we will show you how to fix it

Network Administration **- Have you ever forgotten a WEP or WPA key or password for your Wi-Fi network? In this tutorial, I will show you how to fix if you drop the case like this, restore or reset and secure the network password** .

Want to connect to a Wi-Fi network but you forgot your password or network key? In this case you can solve the problem in several ways:

- Find the WPS or PIN button to automatically configure your security settings.
- Restore the key from another computer still connected to the wireless network.
- Reset the wireless router to the original factory settings.

Here we will look at these methods. Start by using the previous WPS or PIN button.

Use the WPS or PIN button

If the wireless router supports Wi-Fi Protected Setup (WPS), you may not need to find the encryption key to connect. The process will be like programming a remote control for a car garage door. Start by searching on the WPS or security button router, or a WPS personal identification number (PIN) printed on its label. (If your router doesn't have this button or PIN, skip this technique).

Note : Do not confuse the WPS or security button with the router's reset button, the reset button is usually located next to the ports behind the router.

For this method to work, the computer or device you want to access must also support WPS. Windows 7 supports WPS. If you are using a different version of Windows or other device type, browse to the wireless settings page to see if WPS is supported. If you have installed a certain wireless connection manager from Windows, it may support WPS.

If both routers and devices support WPS, then you are ready to test this method. If the router has a button, press it, then try connecting to the wireless network. If the router has a PIN instead of a push button, try connecting to the network; You will see a prompt asking for a PIN. In this case, the router will also transmit the network key and configure the device for you.

Restore keys with WirelessKeyView

If at least one Windows computer can connect to a Wi-Fi network, you can retrieve the key that has been stored. Obviously, it is not possible to simply open the wireless network profile to see the key, because Windows will encrypt these keys. However, you can use third-party tools, such as WirelessKeyView, to recover and decrypt your keys.

To use WirelessKeyView, visit its site and download the WirelessKeyView program. Then you need to extract the file or run the WirelessKeyView.exe program directly from the compressed folder. When running, the program will scan and show you all network keys saved to Windows. Copy the network key in hexa format and make the connection.

Restore default settings

If your device does not support WPS and even no computer can access the network, the best way you can do this is to restore the router to its original settings (factory settings). It should be noted that when you implement this method you will have to reconfigure all your custom settings, such as network name and network key.

Before performing this method, please refer to the installation instructions and installation CDs that came with the device. If you don't see them, you can download these details from the device support section on the manufacturer's website.

When ready, find the small reset button located behind the router. Some reset buttons require you to use protective pins; others you can press with a ballpoint pen. Press and hold this button for about 20 seconds. Then release and wait for a minute or two for the router to reset and restart itself. You will then be able to connect to the default network name, which is usually the name of the carrier. When the operation returns to normal, you need to reconfigure security (usually WPA2) on the router and then on your computers.

Businesses: Replace keys with Username and Password

If you are working with a network used by a business or an organization, you probably won't use password-protected encryption keys, but instead will use the Enterprise mode of WPA encryption or WPA2. In this mode, you connect to the network using the username and password.

Because network keys are securely managed in the background, this mode protects you from thieves and other malicious employees. For example, if you are using a simple Personal mode or pre-shared key (PSK) pre-shared key of WPA or WPA2, then the real encryption key will be saved on the end-user computers and devices. . If

your laptop or device is stolen or lost, the bad person or someone who picked up your device will be able to access the network key. Conversely, if you use the Enterprise mode, you only have to cancel the user account or change the password to prevent a former employee of the company from accessing your network. That method is much easier than changing the encryption key on all your computers!

One problem you might encounter when using Enterprise mode is that, it requires an external server, which is still called a RADIUS AAA server, to perform 802.1X authentication. Setting up your own server can take a lot of time and money, so you may need to consider hosting services like AuthenticateMyWiFi.

Lock protection!

Now that you finally have your encryption key and password, remember it! If you work in a home network, you might consider protecting your key or password with a text file and placing it in your personal file. Another way to do this is to write your key and password in a small piece of paper and paste it on the back of your router. This way, you will always know where to find it.