# Theory - Wifi security: next to the password protected layer

What is Wifi? Is the wireless network that we still use every day, at home, in the office, at the cafe ... And if we consider the basic theory, what is the Wifi password? Do you know other than how to set password for Wifi, are there any other security methods?

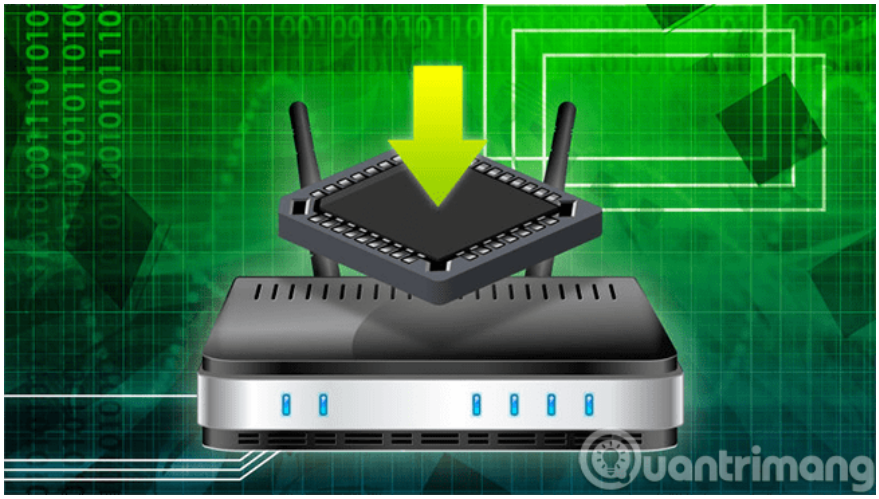
What is Wifi? Is the wireless network that we still use every day, at home, in the office, at the cafe . And if we consider the basic theory, what is the Wifi password? Do you know other than how to set password for Wifi, are there any other security methods? We often discuss the same issues in the following article of TipsMake.com.


## 1. Basic structure:

On the basic theory, you can imagine that the working principle of Wifi passwords would be like this:

1. Wifi password will have the main task of encrypting all data transmitted and transmitted through modem device, router, and prevent other devices from connecting to the network if there is no password.
2. We need to distinguish and know that: **Wi-Fi Protected Access (WPA2) mode** is the main security function along with **Personal** mode **(PSK)** only suitable for home use, small stores, and mode **Enterprise** with **802.1X** security layer is better compatible with networks in large enterprises.

## 2. Firmware update and upgrade:




When choosing to use Modem, Router, you absolutely should not skip this step. That is to check and update **Firmware** - control software to the latest stable version. The best way is to check directly on the home page of the major and reputable equipment suppliers in the world. You can refer to the link below:

1. TP-Link
2. LinkSys
3. Cisco
4. Buffalo
5. .

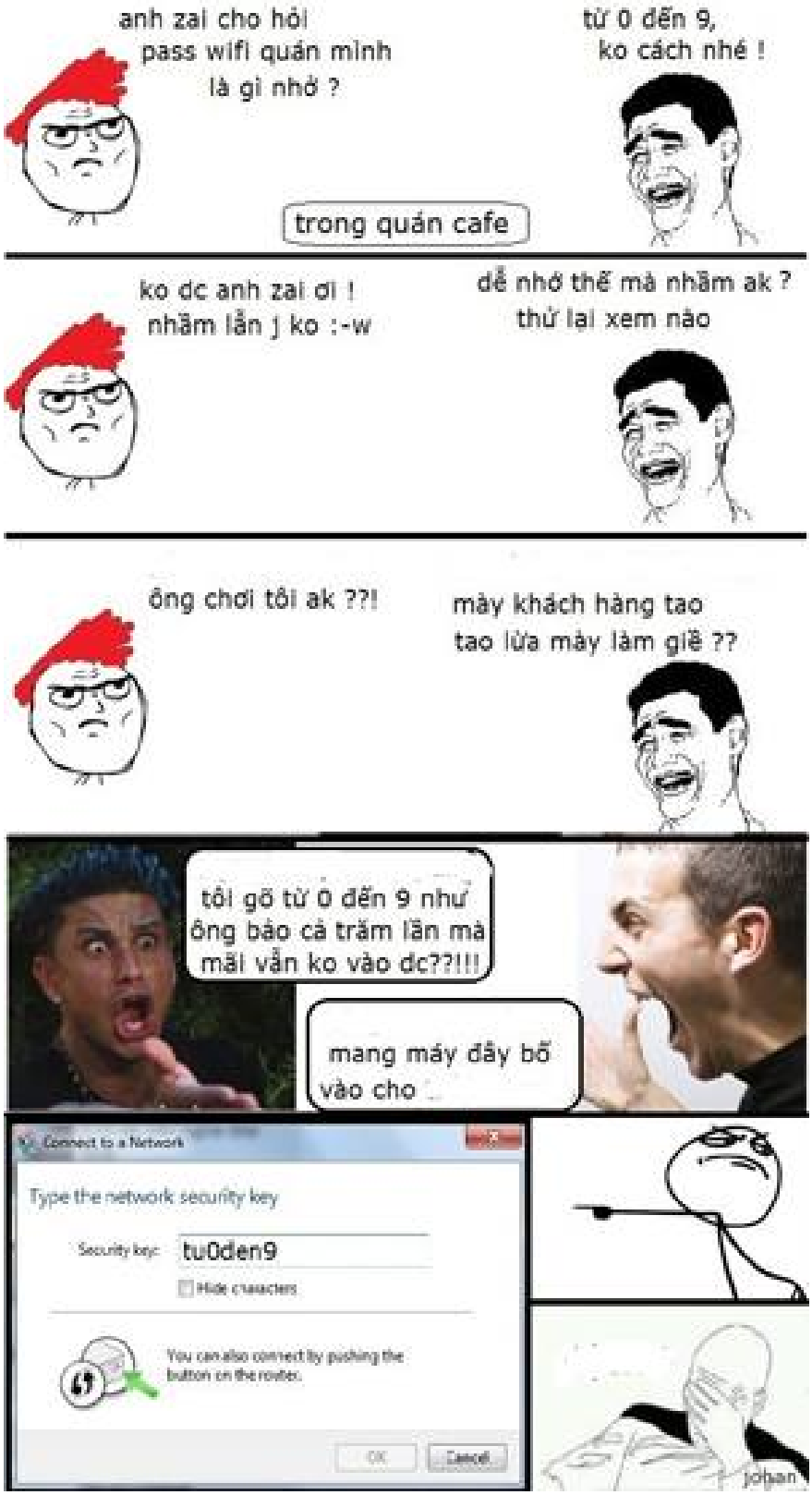
## 3. Choose a flexible Wifi name:

When setting up and configuring Wifi, make sure you change the name of Wifi - **SSID** (full **Service Set Identifier** ) by default. If you are lazy, keep the default name (usually in the form of tplink-wireless, linksys-wifi .) and set a password, it will be easier for hackers to crack the Pre-Shared Key (PSK) . Why is it easy to say here? This is because the SSID information used in the hash process to generate the key - the password, and the rainbow data sheet optimized for Brute Force Cracking is mainly applied to the default SSID.

Another problem with the default SSID, is that the wifi transceivers are virtually indistinguishable from the differences between Wifi systems with the same SSID. This will lead to the computer, the mobile phone will automatically connect to those SSIDs and lead to instability.

One more delicate reason is that the other people are familiar. If you keep 1 SSID from year to year, many people will accidentally connect to your Wi-Fi system, even if they just pass through your office, cafe . Changing SSID periodically will help limit this problem.

## 4. Change admin password and restrict access:




Similar to SSID, changing Wifi passwords is often recommended by security solution providers. Time is 1 week 1 time or 3 times in 1 month. Because changing Wifi password is also quite simple, it does not take much time that few people do too. How to set a password is easy to remember, you just need to follow the rules:

1. Avoid sensitive, easy-to-remember information like shop owner's name, phone number, birthday .
2. Instead, there are some good news, including numbers and special characters. For example: **Hoilamgi1234 @** , **Khongcospass &&** . for example

Some device vendors have additional access restrictions - **Control Access** in their products. You can set restrictions via the firewall, or turn off access to admin rights via LAN, WLAN, or directly from Wi-Fi.

1. See the instructions for blocking websites with Router TP Link

# 5. Turn off the Wi-Fi Protected Setup (WPS) feature:

This function is designed to make Wifi signal encryption process faster and easier. Users just need to select, or enter the PIN code. However, this approach contains a lot of security holes, allowing hackers to take advantage to unlock PIN, thereby gaining access and controlling all Wifi transceivers. Pretty dangerous right?

Hopefully the above information can help you better understand the process of establishing and securing the Wifi system.***Good luck!***