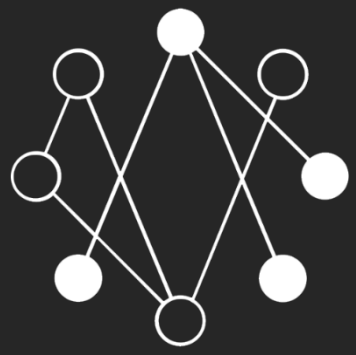
SECURE

YOUR HOME NETWORK



STEP BY STEP GUIDE

By An0n Ali

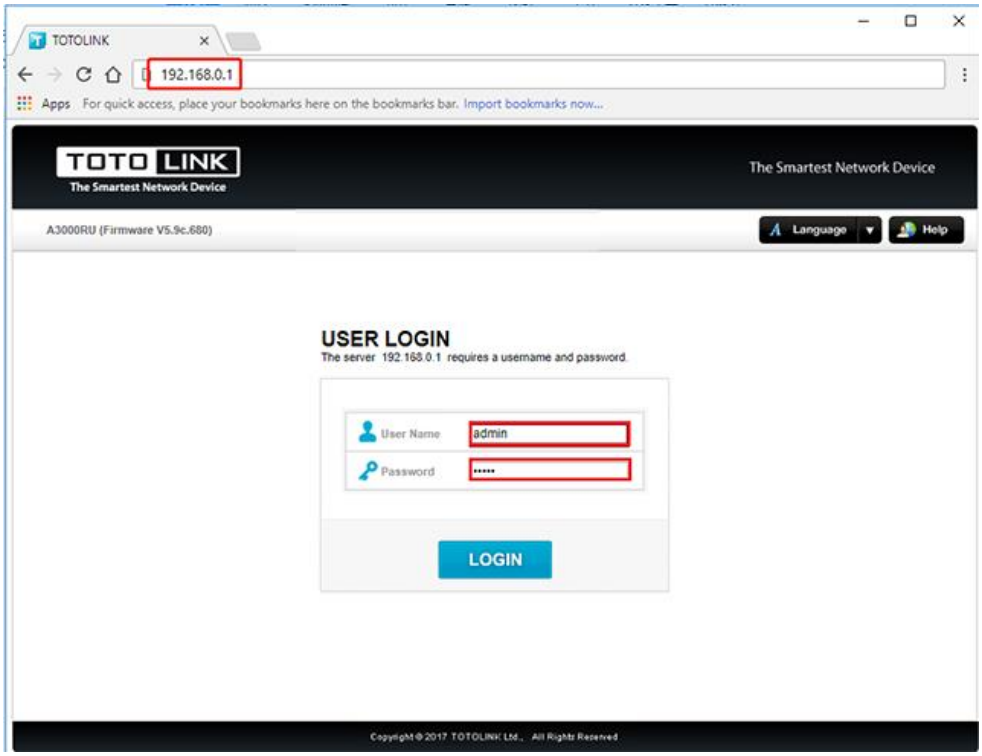
TABLE OF CONTENTS

IMPORTANT STEPS

ROUTER CONFIGURATION

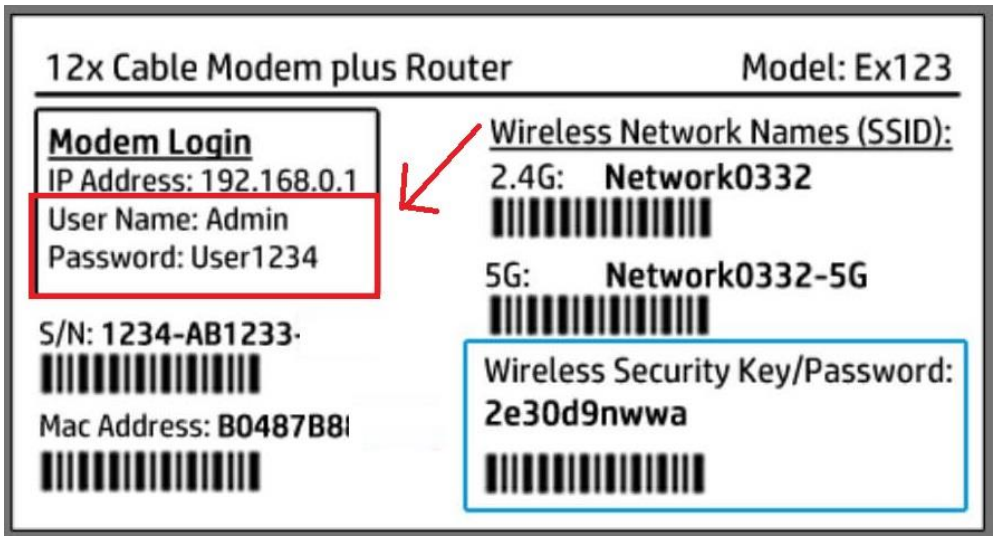
Firstly, you need to ensure that - Your home network is encrypted, all the default passwords are changed, and your router's firmware is up-to-date. For this you will need to **access your Router's Settings.**

- The easiest way to access your router settings is to **log into your router's web interface**.
- This is done by typing your **router's IP address** into your web browser.
- You can find this IP address using **your PC or your Smartphone** (search on Google to learn more).

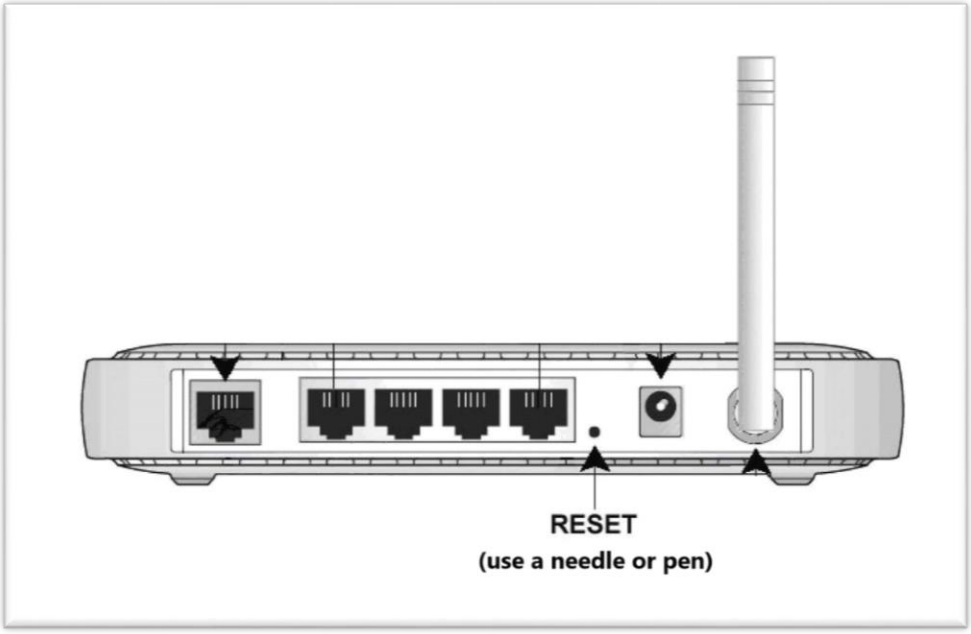


- Once you've typed in the IP address of your router, you'll be prompted for an **admin name and password.**

- Use the **default password shown on a sticker** attached to your router (usually on the back side).



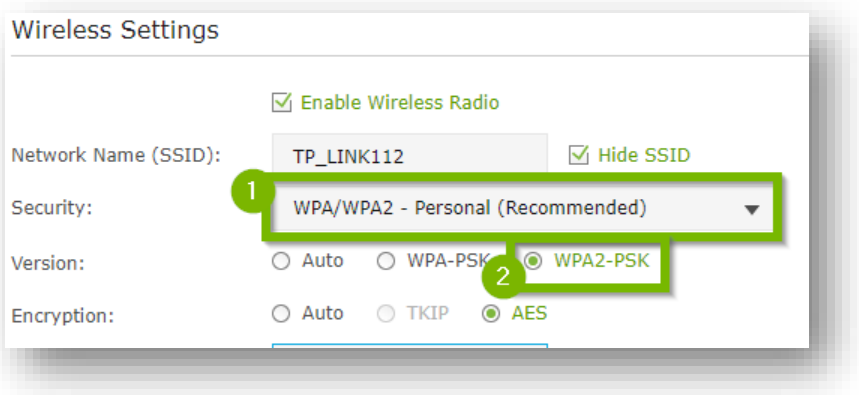
Note: If the default passwords shown on the sticker don't work, **reset your router and try again.**



Once logged in, you're ready to follow the below steps:

Note: Your Router's Interface will look different so you will need to search for settings mentioned in this guide yourself.

1. **Checking for Encryption:**

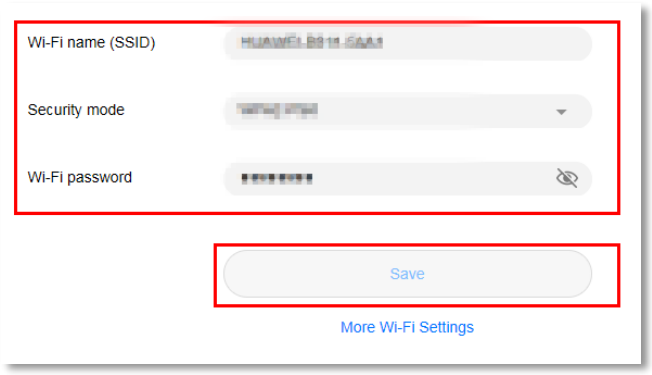


   a. **Locate security settings,** typically found under headings such as *'Wireless Security' 'Wi-Fi Settings'* and *'Connectivity.'*

   b. Select the **strongest encryption** available:

      - **1st Priority: WPA2/WPA3 (Strongest)**
      - **2nd Priority: WPA/WPA2 (Strong)**
      - **Weakest: WEP (Not Recommended, Buy a New Router Today!)**

2. **Changing Default Passwords and SSID:** Encryption only works with a strong Password and Non-Identifiable SSID.



a. **Wi-Fi Password:** Change your Wi-Fi Password to something unique, creative and more than 10 characters. (containing numbers and special characters)

b. **Wi-Fi SSID:**
Service Set Identifier or 'SSID' is your Wi-Fi network's name.
It is used to identify and differentiate one wireless network from another in a specific geographical area.

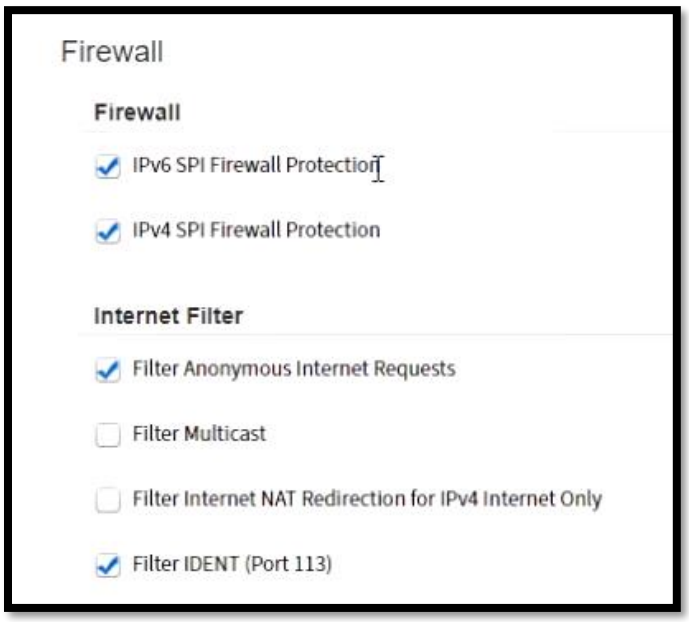
Modify your SSID:
Change it to something that doesn't reveal it's model, firmware or manufacturer.

Don't keep your house number, dog's name or any personal identifiable information.

c. **Web Interface Login:** Change the default username and password for your Router's web interface login page as well.

3. Checking for Firmware Update: If you haven't updated your router since you bought it, now is the good time to do so. You can find this under the 'System Tools' or 'Advanced' settings.

4. (OPTIONAL) Enable Firewall: Check if your router supports a Firewall and enable it.



A firewall in a router acts as a security barrier between your local network and the internet. Its primary function is to monitor and control incoming and outgoing network traffic based on predetermined security rules.

// Educate Yourself

If you're unfamiliar with what an IP address, MAC address, Port, or router really is, and how all the devices in your home are connected to the router (or how the router is connected to the internet), watch the video below.

Link: youtu.be/9rABOh8oT24?si=jPxjPiBsJvwBc5ny

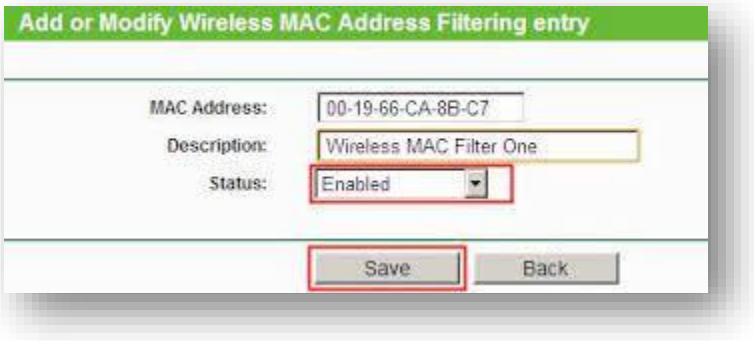
Educating yourself with these terminologies and understanding how all of the magic happens in detail will equip you with better securing your network.

ADDITIONAL MEASURES

Completing all the steps mentioned above will already secure you from 90% of threats. However, if you want to go full hacker mode, you can take these measures as well!!

1. MAC ADDRESS FILTERING

MAC Address Filtering is a setting that allows you to allow or block specific devices from connecting to your Wi-Fi based on their MAC addresses.



You can navigate to the 'MAC address filtering' or 'Access Control' section to find this setting.

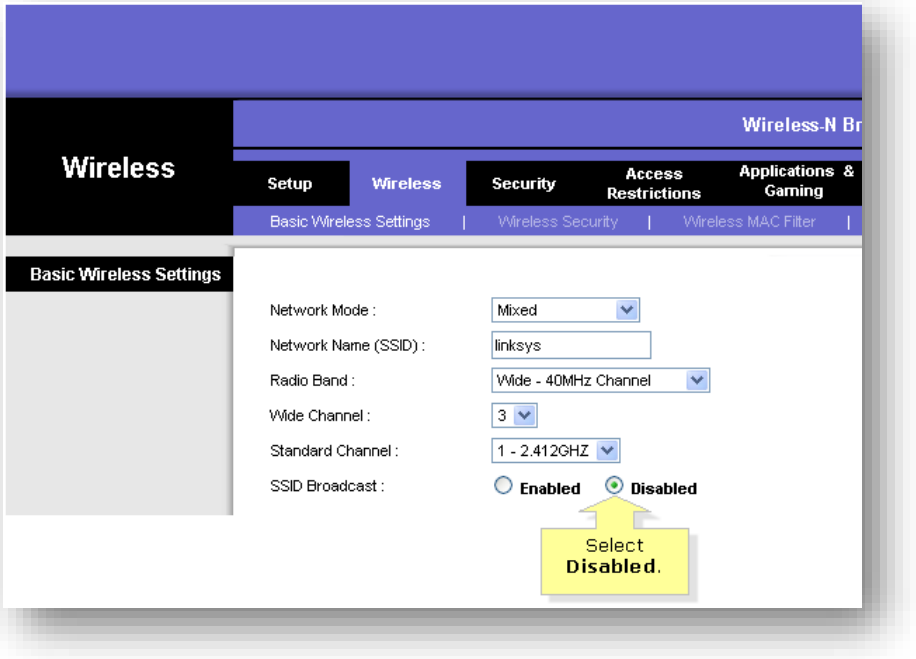
The best way to do this is by first connecting all the devices in your home to your Wi-Fi and then allowing them from the Router's Settings.

Notes: After saving changes, new devices won't be able to join your network even if they know your Wi-Fi Password.

Hackers can still find MAC addresses of connected devices and fake the MAC address of their own device to gain access.

2. SHOULD YOU HIDE YOUR SSID?

While browsing through these various settings, you might have come across the option to hide your SSID. This feature allows you to hide your Wi-Fi's name from being broadcasted to nearby devices.



I've seen many people recommend this option for network security.

However, **I don't believe this is necessary** because hiding the Wi-Fi connection doesn't render it invisible to network analysis tools and Hackers can still easily discover these networks.

Enabling this option also increases unnecessary inconvenience for new devices to connect to your Wi-Fi network and increases battery consumption of connected devices

3. EDUCATE FAMILY MEMBERS

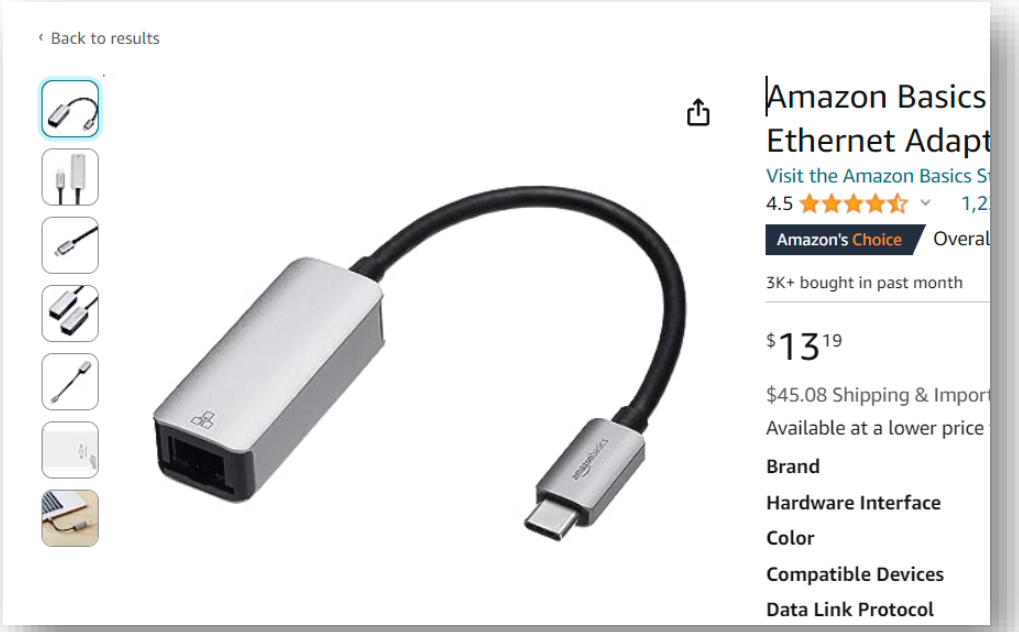
Ensure that all family members are aware of good security practices, such as not sharing passwords and being cautious about clicking on suspicious links.

"SECURITY IS LIKE GROUP IMMUNITY; THE MORE PEOPLE AROUND YOU ARE SECURE, THE LOWER YOUR CHANCES ARE OF GETTING HACKED."

4. SNOWDEN MODE

You can ditch Wi-Fi and go full Edward Snowden mode by using Ethernet cables.

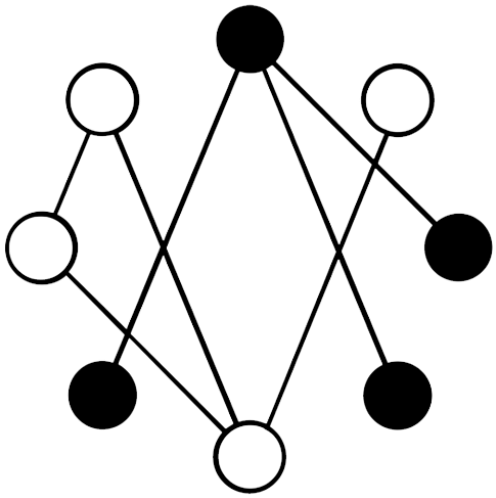
Ethernet Adapter for a smartphone on Amazon. ($15 - $30)



5. SNEAKY WAYS HACKERS HACK WI-FI

Finally, I would highly recommend watching the below video to learn the top 4 Ways Hackers Hack Wi-Fi Networks and gain insight from their perspective to stay vigilant.

Link: youtu.be/L8Qf25l9Mjk?si=5nCG263bW7W3f



AN0N ALI

// youtube.com/@an0n_ali

// instagram.com/an0n.ali