

## Simple steps to

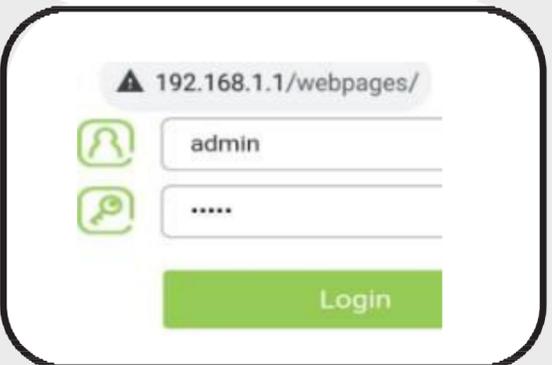
# SECURE YOUR HOME NETWORK



## USE THE DEFAULT SETTINGS TO LOGIN

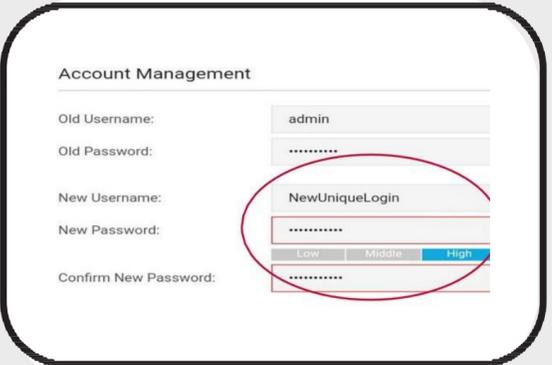
Check the bottom or side of your physical internet router for a label with similar details to the image.

- This will contain login information including your wireless network name, password and a login page for your Wi-Fi settings.



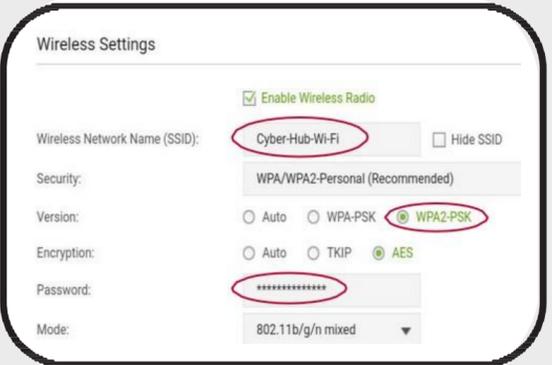
Connect to your Wi-Fi and **browse to the login page**.

Use the **default username and password** to login (in this example, username and password are both admin).



## CHANGE THE DEFAULT LOGIN

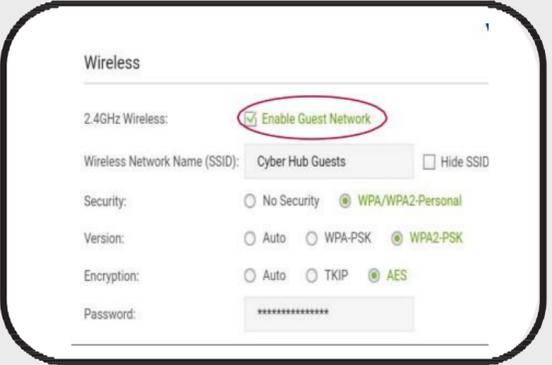
Navigate to the **administration settings** and **change this default user name and password** to a unique and long passphrase.



## ENSURE YOU ARE USING WPA3 OR WPA2

In your wireless settings, ensure you are using **WPA3 or WPA2** depending on device compatibility (if your router settings show WEP or WPA these protocols are no longer considered secure).

**Change your default wireless network password** to a strong passphrase. You may also change your network name here.



## ENABLE THE GUEST WI-FI FEATURE

**Enable the 'guest' Wi-Fi** feature for visitors so that you do not need to share your Wi-Fi password with them.

Ensure that you **perform updates** on your router.

- NOTE THAT THE WEBPAGE, DEFAULT CREDENTIALS AND ROUTER SETTINGS MAY DIFFER DEPENDING ON THE MANUFACTURER.
- DEFAULT WI-FI USERNAME AND PASSWORDS ARE READILY ACCESSIBLE ONLINE FOR AN ATTACKER TO EASILY GAIN ACCESS TO YOUR HOME NETWORK.
- FOR DETAILED INSTRUCTIONS ON HOW TO PERFORM THE ABOVE STEPS ON YOUR PARTICULAR MODEL OF ROUTER, CONSULT YOUR ROUTERS USER MANUAL WHICH CAN BE FOUND ON THE MANUFACTURERS WEBSITE.