Secure Wireless Network Setup

This playbook describes the steps involved in setting up a secure Wi-Fi network. It covers encryption selection, SSID settings, and the creation of a guest network for enhanced security.

Step 1: **Router Access**

Log in to the wireless router's administration interface using the default IP address, username, and password found on the router or in its manual.

Step 2: **Firmware Update**

Check for and install any firmware updates available for your router to ensure you have the latest security and performance enhancements.

Step 3: **Secure Password**

Change the router's default admin username and password to a strong, unique password to prevent unauthorized access to the network settings.

Step 4: **Encryption Setup**

Configure the Wi-Fi network's encryption settings. Select WPA3 if available or WPA2 as the encryption method to secure your network communications.

Step 5: **Network SSID**

Change the network's SSID (name) to something unique but not personally identifiable to make it less obvious to potential intruders.

Step 6: **SSID Broadcast**

Disable SSID broadcast to hide your network from appearing in the list of available networks on nearby devices.

Step 7: **Guest Network**

Set up a guest network with a separate SSID and password for visitors to use, which prevents access to the main network and connected devices.

General Notes

Regular Updates

Regularly check and update the firmware of your router to keep the network secure against vulnerabilities.

Password Management

Use a password manager to generate and store a complex router admin password securely.

SSID Concealment

Consider the implications of hiding your SSID; while it can offer security through obscurity, it may not be suitable for all users, as it requires manual network setup on each device.