Wi-Fi Network Security

This playbook describes the steps necessary to secure a wireless network. It includes actions to prevent unauthorized access and protect against various security threats.

Step 1: **Access Control**

Change the default username and password for the wireless router's administrative interface to prevent unauthorized access to the router settings.

Step 2: **Update Firmware**

Regularly check for and install firmware updates for your router to ensure you have the latest security patches and features.

Step 3: **Encrypt Traffic**

Enable WPA2 or WPA3 encryption to secure the communication between connected devices and the router.

Step 4: **Firewall Setup**

Ensure that the router's built-in firewall is enabled and properly configured to protect the network from external threats.

Step 5: **Disable WPS**

Turn off Wi-Fi Protected Setup (WPS) if it's not needed, as it can be a security vulnerability.

Step 6: **SSID Management**

Change the default Service Set Identifier (SSID) and disable SSID broadcasting to make the network less visible to outsiders.

Step 7: **MAC Filtering**

Implement MAC address filtering to restrict network access to only known devices.

Step 8: **Disable Remote Access**

Turn off any remote management features on the router to prevent access from external networks.

Step 9: **Secure Wi-Fi Guests**

Create a separate guest network with its own password and restrict access to internal network resources.

Step 10: **Physical Security**

Place the router in a secure location where it is less likely to be tampered with by unauthorized individuals.

General Notes

Regular Audits

Conduct regular security audits of the network and connected devices to identify and fix vulnerabilities.

Education

Regularly educate users connected to the network about good security practices to prevent inadvertent compromises.