Wireless Network Security Assessment

Environment: Home Lab

Author: Lakpa Sherpa

Date: November 2025

1. Objective

Evaluate the security of a home Wi-Fi network, compare it to public networks, identify vulnerabilities, and apply security improvements based on industry best practices.

2. Scope

This assessment includes:

- Home wireless network security review
- Public Wi-Fi comparison
- Router configuration analysis
- Authentication, encryption, and access control evaluation
- Remediation actions and validation

3. Network Discovery Summary

Network	Type	Security	Notes
Home Network	Private	WPA2 (initially)	Default SSID, WPS on, default admin password
Queens Library	Public	Open	No encryption
Starbucks	Public	Open	No encryption

4. Security Findings

Issue	Security Impact
WPA2 instead of WPA3	Weaker encryption than the modern standard
WPS enabled	Can be attacked by repeatedly guessing the PIN
Default admin password	Increased risk of unauthorized access
Default SSID	Reveals vendor/ target information

5. Remediation Actions

Action	Purpose
Disabled WPS	Stop attackers from guessing the PIN to join the Wi-Fi
Changed admin password	Prevent unauthorized access to router settings
Renamed SSID	Avoid revealing device type or owner information
Enabled WPA3 (supported devices)	Improve Wi-Fi encryption and security

6. Results

The home network was successfully hardened by disabling insecure services, improving authentication strength, and applying modern encryption standards. These changes reduced the attack surface and improved the overall wireless security posture.

7. Evidence Appendix

A separate appendix contains screenshots verifying:

- Router login
- WPS disabled
- SSID renamed
- WPA3 enabled
- Firmware version check
- Connected device inventory
- Public Wi-Fi security observations

8. Conclusion

This assessment demonstrated practical wireless security hardening techniques and validated improvements through configuration review and screenshots. The home network now follows recommended security practices and is significantly more resilient against common wireless attacks.

Sensitive information (device names, MAC addresses, SSID, IPs) has been redacted for privacy.