



IT Consultant
Combined 65 years in the IT Business
Private & Federal Sector
IT Security is Your Business Too!

Router security involves protecting your home network by changing default passwords, using strong encryption like WPA3, keeping firmware updated, disabling features like WPS and remote management, and creating a separate guest network, all to prevent unauthorized access and data theft.

Essential Security Measures

- **Change Default Passwords:** Immediately change the default admin login and Wi-Fi password to strong, unique phrases.
- **Update Firmware:** Regularly check for and install firmware updates to patch security vulnerabilities, or enable automatic updates if available.
- **Use Strong Encryption:** Set your Wi-Fi to WPA3 Personal or WPA2-AES for strong data encryption.
- **Disable WPS (Wi-Fi Protected Setup):** Turn off this convenient but vulnerable feature, which can be brute-forced, as noted by the Canadian Centre for Cyber Security.
- **Turn Off Remote Management:** Prevent access to your router's settings from the internet.
- **Create a Guest Network:** Isolate visitors' devices from your main network.
- **Change SSID:** Change the default network name (SSID) to something non-identifiable.

Advanced Steps

- **Enable Router Firewall:** Ensure the built-in firewall is active.
- **Disable UPnP:** Turn off Universal Plug and Play to reduce risks.
- **Physically Secure Router:** Place the router in a secure, less accessible location.
- **Monitor Network:** Periodically check connected devices

TR Stockwood