T2025_29 Secure Your Home and Work Wi-Fi Networks (October 10th , 2025)

Unsecured wireless networks are a common entry point for cyberattacks, allowing unauthorized users to intercept sensitive data, launch on-path attacks, or gain access to connected devices. Many routers ship with default credentials and outdated firmware containing known vulnerabilities, making them easy targets for attackers. Once compromised, a router can be used to redirect traffic to malicious sites, monitor online activities, or serve as a launching point for further attacks within the network. Wi-Fi eavesdropping and unauthorized access can expose personal information, financial data, and business communications to cybercriminals. To secure your wireless network, immediately change the default administrator username and password on your router, enable WPA3 encryption (or WPA2 if WPA3 is unavailable), and create a strong, unique Wi-Fi password. Disable WPS (Wi-Fi Protected Setup) due to its vulnerabilities and change your network's default SSID to something that doesn't reveal the router model or personal details. Keep firmware updated regularly or enable automatic updates, disable remote management unless necessary, and create a separate guest network to isolate visitors from your main network and connected devices.

References

- CISA. (n.d.). Securing wireless networks. Cybersecurity and Infrastructure Security Agency. Retrieved September 29, 2025, from https://www.cisa.gov/secure-our-world/use-strong-passwords

- FTC. (2022, December 2). How To Secure Your Home Wi-Fi Network. Federal Trade Commission Consumer Advice. Retrieved September 29, 2025, from https://consumer.ftc.gov/articles/how-secure-your-home-wi-fi-network