BROWN

Knowledgebase > Network and Connectivity > Home Wireless > Set up a Secure Wireless Network at Home

Set up a Secure Wireless Network at Home

Stephanie Obodda - 2023-06-06 - Comments (0) - Home Wireless

When setting up wireless at home, make sure to properly configure your router/access point to protect your:

- bandwidth *(don't let neighbors hog it)*
- record/reputation *(the net can be used for illegal activity)*
- identifiable information *(online banking, purchases, travel plans, etc.)*
- computing devices *(which could be compromised)*

Secure your wireless router by taking these important steps:

Initial Setup and Placement

1. Change the admin password. Your password is your first line of defense, so make it unique and strong.
2. Update your router firmware. Consider updating the drivers on your wireless card as well.
3. Enable network encryption. Use WPA or WPA3 (see Encryption Options below).
4. Disable remote management. To help prevent unauthorized changes to your router settings, make sure that no one can access your router settings from outside of your network.
5. Place the router in a central location. Keep it away from outside walls and adjust its range.

Router Configuration

1. Use MAC address filtering (specify what MAC addresses you allow onto your network and hard code those into the router’s MAC filtering list).
2. Pick a unique SSID (Service Set Identifier) and hide it (DON'T use the default; make sure you're not broadcasting the SSID).
3. Change the default network addressing (to an another private RFC1918 network).
4. Disable DHCP on the wireless network (prevents someone connecting to your wireless router from obtaining an IP address).
5. Turn off the router when away.

Use the Strongest Encryption Option

- WEP (Wired Equivalent Privacy): 40-Bit or 104-Bit key algorithm, first cracked in

2001, now can be hacked as fast as 30 seconds; it has therefore been deprecated by IEEE as no longer meeting security goals.

- WPA-TKIP: Uses 128-Bit encryption keys and dynamic session keys; made to be backwards compatible with Pre-WPA hardware, but is vulnerable to attacks.
- WPA2-AES (Wi-Fi Protected Access 2): Introduced in 2004, WPA2 remains the most popular security protocol. It uses the Advanced Encryption Standard and is an upgraded version of WPA. It is not backward compatible.
- WPA3 (Wi-Fi Protected Access 2): This wireless security protocol offers enhanced security features such as stronger encryption, protection against dictionary attacks and individualized data encryption. According to eSecurity Planet (see article below), "Announced in 2018 by the Wi-Fi Alliance, WPA3 simplifies the process of configuring devices with little to no display interface — such as IoT devices— by introducing Wi-Fi Easy Connect. This works by allowing the IoT device to present a QR code or a Near Field Communication (NFC) tag, which the user can scan with their device to establish a secure Wi-Fi connection. Despite advances like stronger encryption and more secure key exchange, WPA3 has yet to gain much traction among users."

Useful Resources

- Wireless Security: WEP, WPA, WPA2 and WPA3 Explained (eSecurity Planet)
- General Wireless Information: www.wi-fi.org
- Random Password Generation: www.grc.com/passwords.htm
- Check Your SSID Exposure: www.wigle.net