Monthly Cybersecurity Tips Newsletter
VOLUME 17, ISSUE 12 • 2022

How to Secure Your Home Network Against Cyber Threats

Computers, tablets, smartphones, TVs, thermostats, cameras, doorbells, and coffee pots. What do all these things have in common? They are all devices that connect to your home network and the internet.

Modems and routers act as the gateway between your devices and the internet. Without proper security in place, you can leave the door open for attackers to access and take over your network.

Let's review some steps you can take to keep your home network safe from potential cyber threats.

Secure Your Modem and Router

- **Use current hardware.** Technology changes quickly, and if the manufacturer no longer supports your modem and router, a security vulnerability may emerge and not receive a fix. Whether you purchase your own modem and router or lease them through your internet service provider (ISP), consider replacing them at least every five years to ensure your devices receive the support and security fixes you need to keep your home network safe.
- **Use a surge protector or uninterruptable power supply (UPS)**. Prevent potential damage to your modem and router from unexpected power surges, spikes, and lightning strikes by connecting them to a surge protector or UPS. Some models also include surge protection for phone, ethernet, and coaxial cables.
- **Disable remote management.** Some routers have the capability for you to manage your home network over the internet. While this does add convenience, it also increases the risk that an attacker will compromise your network. Disable remote management by default, and if you absolutely need it, be sure to enable multi-factor authentication (MFA) to use this feature.
- **Change your modem and router passwords from the default passwords to secure passwords.** Changing default passwords will prevent others from

accessing the configuration, changing settings, and gaining visibility into your network.

- **Enable automatic updates and install the latest firmware**. Keeping your modem and router up to date with the latest firmware helps protect them as new vulnerabilities emerge and receive fixes.
- **Enable the router's firewall.** The firewall helps prevent the devices on your network from accessing malicious sites as well as keeps outsiders on the outside of your network.
- **Enable website filtering.** Some routers have website filtering and parental controls as added features to prevent users from accessing malicious or inappropriate websites while on your network. If your router does not have these features built in, you can set up free internet Domain Name System (DNS) filtering through services such as quad9, CleanBrowsing, or OpenDNS.
- **Reboot your modem and router at least once a month.** Malicious software can infect your router without your knowledge. Periodically reboot your modem and router to clear potentially malicious software from memory, refresh your device connections, and keep your internet connection healthy and fast.

Secure Your Wi-Fi

- **Change the Wi-Fi network name (SSID).** The default wireless network name is typically the brand of the router. As such, it can provide clues to outsiders as to what type of router you are using and what vulnerabilities exist. Make sure you do not use your name, home address, or other personal information in your new SSID name. For added protection, disable broadcast of the wireless network name.
- **Enable Wi-Fi encryption.** Use Wi-Fi Protected Access 3 (WPA3) if supported by your device and choose a strong passphrase to connect devices to your network. When feasible, choose wired connections over wireless for enhanced security.
- **Enable a Wi-Fi guest network.** A security best practice is to segregate network devices. Connect your computers, mobile devices, printers, and other trusted devices on your primary wireless network. Additionally, restricting devices such as smart TVs, personal digital assistants, and your refrigerator to the guest network.

Monitor Your Network

According to Deloitte's 2022 Connectivity and Mobile Trends Survey, the average U.S. household has 22 connected devices. Do you know what devices are connecting to your network? Periodically review the devices that are connected to your network and block the ones that you don't recognize.

We rely on our home internet connections more than ever before for work, school, communication, and entertainment. By following these steps, you can greatly improve the security of your home network and protect you and your family from potential cyber threats.

Special thanks to Jason Balderama, CISO of County of Marin, CA, for providing the content for this newsletter.