

Securing Your Home Network

Original release date: December 15, 2015 | Last revised: December 16, 2015

A router comes configured with many vendor default settings. Many of these settings are public knowledge and make your router susceptible to attacks. Remember to change your router default log-in password during your initial setup.

How are routers used in your home network?

Home routers have become an integral part of our global communications footprint as use of the Internet has grown to include home-based businesses, telework, schoolwork, social networking, entertainment, and personal financial management. Routers facilitate this broadened connectivity. Most of these devices are preconfigured at the factory and are Internet-ready for immediate use. After installing routers, users often connect immediately to the Internet without performing any additional configuration. Users may be unwilling to add configuration safeguards because configuration seems too difficult or users are reluctant to spend the time with advanced configuration settings.

Unfortunately, the default configuration of most home routers offers little security and leaves home networks vulnerable to attack. Small businesses and organizations often use these same home routers to connect to the Internet without implementing additional security precautions and expose their organizations to attack.

Why secure your home router?

Home routers are directly accessible from the Internet, are easily discoverable, are usually continuously powered-on, and are frequently vulnerable because of their default configuration. These characteristics offer an intruder the perfect target to obtain a user's personal or business data. The wireless features incorporated into many of these devices add another vulnerable target.

How can you prevent unauthorized access to your home network?

The preventive steps listed below are designed to increase the security of home routers and reduce the vulnerability of the internal network against attacks from external sources.

- **Change the default username and password:** These default usernames and passwords are readily available in different publications and are well known to attackers; therefore, they should be immediately changed during the initial router installation. It's best to use a strong password, consisting of letters, numbers, and special characters totaling at least 14 characters. Manufacturers set default usernames and passwords for these devices at the factory for their troubleshooting convenience. Furthermore, change passwords every 30 to 90 days. See *Choosing and Protecting Passwords* for more information on creating a strong router password.
- **Change the default SSID:** A service set identifier (SSID) is a unique name that identifies a particular wireless local area network (WLAN). All wireless devices on a WLAN must use the same SSID to communicate with each other. Manufacturers set a default SSID at the factory, and this SSID typically identifies the manufacturer or the actual device. An attacker can use the default SSID to identify the device and exploit any of its known vulnerabilities. Users sometimes set the SSID to a name that reveals their organization, their location, or their own name. This information makes it easier for the attacker to identify the specific business or home network based upon an SSID that explicitly displays the organization's name, organization's location, or an individual's own name. For example, an SSID that broadcasts a company name is a more attractive target than an SSID broadcasting "ABC123." Using default or well-known SSIDs also makes brute force attacks against WPA2 keys easier. When choosing an SSID, make the SSID unique and not tied to your personal or business identity.
- **Don't stay logged in to the management website for your router:** Routers usually provide a website for users to configure and manage the router. Do not stay logged into this website, as a defense against cross-site request forgery (CSRF) attacks. In this context, a CSRF attack would transmit unauthorized commands from an attacker to the router's management website.

- **Configure Wi-Fi Protected Access 2 (WPA2)-Advanced Encryption Standard (AES) for data confidentiality:** Some home routers still use Wired Equivalent Privacy (WEP), which is not recommended. In fact, if your router or device supports only WEP, but not other encryption standards, you should upgrade your network device.[1] One newer standard, WPA2-AES, encrypts the communication between the wireless router and the wireless computing device, providing stronger authentication and authorization between the devices. WPA2 incorporates the Advanced Encryption Standard (AES) 128-bit encryption that is encouraged by the National Institute of Standards and Technology (NIST). WPA2 with AES is the most secure router configuration for home use.
- **Immediately disable WPS:** Wi-Fi Protected Setup (WPS) provides simplified mechanisms to configure moderately secure wireless networks. A design flaw that exists in the WPS specification for the PIN authentication significantly reduces the time required to brute force the entire PIN because it allows an attacker to know when the first half of the 8-digit PIN is correct. The lack of a proper lockout policy after a certain number of failed attempts to guess the PIN on many wireless routers makes a brute-force attack much more likely to occur.
- **Limit WLAN signal emissions:** WLAN signals frequently broadcast beyond the perimeters of your home or organization. This extended emission allows eavesdropping by intruders outside your network perimeter. Therefore, it's important to consider antenna placement, antenna type, and transmission power levels. Local area networks (LANs) are inherently more secure than WLANs because they are protected by the physical structure in which they reside. Limit the broadcast coverage area when securing your WLAN. A centrally located, omnidirectional antenna is the most common type used. If possible, use a directional antenna to restrict WLAN coverage to only the areas needed. Experimenting with transmission levels and signal strength will also allow you to better control WLAN coverage. Note that a sensitive antenna may pick up signals from further away than expected, a motivated attacker may still be able to reach an access point that has limited coverage.
- **Turn the network off when not in use:** While it may be impractical to turn the devices off and on frequently, consider this approach during travel or extended offline periods. The ultimate in wireless security measures—shutting down the network—will definitely prevent outside attackers from being able to exploit your WLAN.
- **Disable UPnP when not needed:** Universal Plug and Play (UPnP) is a handy feature allowing networked devices to seamlessly discover and establish communication with each other on the network. Though the UPnP feature eases initial network configuration, it is also a security hazard. For example, malware within your network could use UPnP to open a hole in your router firewall to let intruders in. Therefore, disable UPnP unless you have a specific need for it.
- **Upgrade firmware:** Just like software on your computers, the router firmware (the software that operates it) must have current updates and patches. Many of the updates address security vulnerabilities that could affect the network. When considering a router, check the manufacturer's website to see if the website provides updates to address security vulnerabilities.
- **Disable remote management:** Disable this to keep intruders from establishing a connection with the router and its configuration through the wide area network (WAN) interface.
- **Monitor for unknown device connections:** Use your router's management website to determine if any unauthorized devices have joined or attempted to join your network. If an unknown device is identified, a firewall or media access control (MAC) filtering rule can be applied on the router. For further information on how to apply these rules, see the literature provided by the manufacturer or the manufacturer's website.

[1] If you must use WEP, it should be configured with the 128-bit key option and the longest pre-shared key the router administrator can manage. Note that WEP at its strongest is still easily cracked.

Author

US-CERT Publications