OUCH! January 2021

OUCH!

SANS SECURITY AWARENESS

The Monthly Security Awareness Newsletter for You

Securing Wi-Fi At Home

Overview

To create a secure home network, you need to start by securing your Wi-Fi access point (sometimes called a Wi-Fi router). This is the device that controls who and what can connect to your home network. Here are five simple steps to securing your home Wi-Fi to create a far more secure home network for you and your family.

Focus on The Basics

Often the easiest way to connect to and configure your Wi-Fi device is while connected to your home network. Point your web browser to the specific IP address documented in your device's manual (an example of this would be https://192.168.1.1), or use a utility or mobile app provided by your Wi-Fi device vendor.

1. **Change the Admin Password**: Your Wi-Fi access point was most likely shipped with a default password for the administrator account that allows you to change the device configuration. Often these default passwords are publicly known, perhaps even posted on the Internet. Be sure to change the admin password to a unique, strong password, so only you have access to it. If your device allows it, change the admin username as well.
2. **Create a Network Password**: Configure your Wi-Fi network, so it has a unique, strong password as well (make sure it is different from your device admin password). This way only people and devices you trust can join your home network. Consider using a password manager to select a strong password and to keep track of all of your passwords for you.
3. **Firmware Updates**: Turn on automatic updating of your Wi-Fi access point's operating system, often called firmware. This way you ensure your device is as secure as possible with the latest security options. If automatic updating is not an option on your Wi-Fi access point, periodically log into and check your device to see if any updates are available. If your device is no longer supported by the vendor, consider buying a new one that you can update to obtain the latest security features.

4. **Use a Guest Network**: A guest network is a virtual separate network that your Wi-Fi access point can create. This means that your Wi-Fi access point actually has two networks. The *primary* network is the one that your trusted devices connect to, such as your computer, smartphone, or tablet devices. The *guest network* is what untrusted devices connect to, such as guests visiting your house or perhaps some of your personal smart home devices. When something connects to your guest network, it cannot see or communicate with any of your trusted personal devices connected to your primary network.
5. **Use Secure DNS Filtering:** DNS is an internet-wide service that converts the names of websites into numeric addresses. It is what helps ensure your computer can connect to a website when you type in the website's name. Wi-Fi access points typically use the default DNS server supplied by your internet service provider, but more secure alternatives are available for free from services such as OpenDNS, CloudFlare for Families, or Quad9 that can provide extra security by blocking malicious or other undesirable websites. Log into your Wi-Fi access point and change the DNS server address to a more secure alternative.

Securing your home Wi-Fi access point is the first, and one of the most important, step in creating a secure home network. For more information about securing your Wi-Fi access point, refer to the device's manual, or if your internet service provider provided your Wi-Fi device, contact them for more information on security features.

Guest Editor

Joshua Wright (Twitter @joswr1ght) is a senior director at Counter Hack Challenges, LLC, leading the coordination and development of cyber challenges for NetWars and the Holiday Hack Challenge. Find Josh at LinkedIn here: https://linkedin.com/in/joswr1ght.

Resources

Making Passwords Simple: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Password Managers: https://www.sans.org/security-awareness-training/resources/password-managers-0
Updating: https://www.sans.org/security-awareness-training/resources/power-updating
OpenDNS Setup Guide: https://www.opendns.com/setupguide/#familyshield