Home Wi-Fi Security Best Practices

By C. Frank Watson IV, and Madison Dewey

About the Authors:

C. Frank Watson IV is a Business Risk Assurance Associate at Fairview Cyber. He can be reached at cfrank.watson@fairviewcyber.com.

Madison Dewey is a Business Risk Assurance Associate at Fairview Cyber. She can be reached at madison.dewey@fairviewcyber.com.

In today's hybrid work environment, firms are increasingly reliant on home networks that employees use to work remotely. Securing home Wi-Fi networks has become critical to safeguarding firm and client information. The best practices below can be used to guide employees on how to secure their home Wi-Fi networks.

1. **Change the default password:** When you first install your Wi-Fi router, it comes with a default password that is easily accessible to anyone who knows the make and model of the router. Therefore, the first step in securing your home Wi-Fi is to change the default password to a strong, unique password that is difficult to guess.
2. **Use WPA3 encryption:** WPA3 is the most secure encryption protocol currently available for Wi-Fi networks. Make sure that your home Wi-Fi network is configured to use WPA3 encryption. This will prevent unauthorized access to your network by encrypting all the data that is transmitted over the network. NOTE: WPA3 is not supported by some older devices, which may require updating or using WPA2.
3. **Change the network name:** The name of your Wi-Fi network, also known as the Service Set Identifier (SSID), should not contain any personal information or identifiable information. Using your name, address, or phone number in your network name can make it easy for hackers to find your network and gain access.
4. **Enable MAC address filtering:** A MAC address is a unique identifier assigned to each device that connects to a Wi-Fi network. By enabling MAC address filtering, you can specify which devices are allowed to connect to your network. This prevents unauthorized devices from accessing your network.
5. **Disable remote management:** Remote management allows you to manage your Wi-Fi network from a remote location. However, this feature also allows hackers to access your network from anywhere in the world. It is recommended to disable remote management unless it is absolutely necessary.
6. **Update your router firmware:** Router manufacturers regularly release firmware updates that include security patches and bug fixes. Make sure that you update your router firmware regularly to protect against known vulnerabilities.
7. **Network Segmentation:** Most modern routers have the ability to create a guest network separate from your home Wi-Fi network. Segmenting your network allows for your work computer to be unreachable from a guest's infected computer or device. For further security, put Internet of Things ("IoT") devices such as Ring Cameras, Nest Thermostats, etc. on the guest network due to vulnerabilities being exploited allowing bad actors access to your network remotely.
8. **Firewall:** One of the most important features that should be enabled is the firewall. Depending on the router manufacturer will depend on how advanced the protection will be. Most routers will have features such as Stateful Packet Inspection ("SPI") and Denial of Service ("DOS") protection. SPI validates the traffic coming into your network based on the protocol. DOS protection prevents FLOOD attacks such as Internet Control Message Protocol ("ICMP"), User Datagram Protocol ("UDP"), and Transmission Control Protocol-Synchronize ("TCP-SYN").

In addition to the above, firms that want to ensure their remote employees are following best practices should consider providing company-owned routers that are pre-configured with security measures.

In conclusion, securing home Wi-Fi networks has become an essential task, especially for employees working from home. Employers and employees must take the necessary precautions to protect sensitive work data from unauthorized access. Following the best practices mentioned above will ensure that home Wi-Fi networks are secure, and confidential work data remains safe. ■

Home Wi-Fi Security Best Practices
Configuration Checklist

Accessing Your Router

To access your router's configuration page, there is typically an IP address listed on the router which you then type into your browser. If not, Google your router brand/model to find out the default IP.

Here is a short list of the most common IPs for routers:

- 192.168.1.1
- 192.168.0.1
- 192.168.1.254
- 10.0.0.1

Strongly Recommended Settings

- [ ] 1. Change the default password.
- [ ] 2. Change the network name (SSID). Do not use any personal information: name, address, or phone number.
- [ ] 3. Ensure WPA3 encryption is enabled.
- [ ] 4. Disable remote management.
- [ ] 5. Enable the Firewall. Enable the following additional firewall settings if available:
    - [ ] a. Stateful Packet Inspection ("SPI")
    - [ ] b. Denial of Service ("DoS")
- [ ] 6. Enable Automatic Firmware Update / Update Firmware Regularly.

Additional Settings

- [ ] 1. Segment network by enabling Guest Wi-Fi.
    - [ ] a. Do not allow anyone to connect to the main network where your work PC will be connected.
    - [ ] b. Connect all IoT devices (Ring Camera, Nest Thermostat, etc.) to the guest network.
    - [ ] c. Use a different password for the guest network.
- [ ] 2. Enable MAC address filtering. (Prevents unauthorized devices from connecting to your network)