Wi-Fi SECURITY

IN **7** EASY STEPS

Wi-Fi attacks are easy to deploy, and successful hackers can gain access to your valuable company data and customer information in under three minutes.

It's important to set up your organization's Wi-Fi for the best bandwidth while also maintaining security. **As cybersecurity threats increase across industries, securing your Wi-Fi is an often-overlooked vulnerability that you CAN fix.**

Follow these 7 steps today to secure your network and business data.

1 ROUTERS

MAKE SURE YOUR ROUTER IS PHYSICALLY SECURED

✓ Ensure that only authorized personnel can access your Wi-Fi router. A hacker who gains access to your router can easily hit the reset button and potentially gain access to your network.

✓ Secure your router in an office or another location that only authorized personnel can access.

CHANGE THE DEFAULT PASSWORD FOR YOUR ROUTER OFTEN

✓ The best passwords/passphrases are at least 15 characters long, with a mix of letters, numbers, and special characters.

CHANGE THE NETWORK SSID NAME

✓ When you connect to a wireless network you look for the network name or the service set identifier (SSID). This name is visible to your employees, partners, and customers so they can easily identify your network.

✓ You do not want to let everyone know the make and model of the router you are running. The default SSID name out of the box is often identified using "Linksys," or "Netgear3060," which is essentially giving a hacker the manual on how to access your network.

2 UPDATE YOUR FIRMWARE AND SOFTWARE REGULARLY

Check to see if there are software updates for your Wi-Fi router regularly. These patches are often intended to fix security vulnerabilities.

3 USE WPA2 OR WPA3

In simple terms, this is the way to ensure the data that you are transmitting and receiving is encrypted. If your router does not have WPA2 or WPA3, invest in a newer, more secure router. Older routers will have WEP (Wired Equivalent Privacy) or WPA (Wi-Fi Protected access) which, are older versions and much more hackable.

4 USE A BUSINESS GRADE FIREWALL

Consumer grade firewalls often sacrifice security for speed while, a business firewall prioritizes security, remote access, and scalability. A firewall is a must-have security feature for any business—it's a line of defense that separates your trusted internal network from the untrusted internet at large. Look for a firewall with built-in back up capabilities, options to control the applications on your network, and cloud protection and integration.

Without a firewall, company networks are much more susceptible to falling victim to one of the many cyber threats out there, like ransomware, botnets, trojans and more.

5 PUBLIC Wi-Fi

SET UP SEPARATE PRIVATE AND PUBLIC ACCESS

Your Wi-Fi should have separate access for the public and your employees, so you do not give unintended access to your internal business computers and networks to a hacker. You will want to create two different Service Set Identifiers (SSID) with two separate points of access to your network. One should be a business-grade secure access point for your employees, and a public one for customers.

PUBLIC Wi-Fi SAFETY TIPS

✓ If possible, avoid public Wi-Fi. Invest in a personal hotspot if you plan to travel for work or access Wi-Fi from remote locations.

✓ If you do use a public Wi-Fi network, check to ensure you're connecting to the intended network.

6 KNOW ALL OF YOUR ACCESS POINTS

New access points can be created by an employee who might have a bad network connection in their office. These access points are usually not configured for security and create vulnerabilities.

Plan to complete occasional access point scanning if you have a large office or network.

7 TURN OFF WPS

Unless you need it for something specific, you should turn off Wi-Fi Protected Setup, or WPS. It's designed to make pairing a device with your encrypted network, push button easy.

The problem is that it can open the door for someone with criminal intent.

> **Ready to bolster your cybersecurity strategy?** Partner with a New Charter Technologies Managed Service Provider.

CONTACT US TODAY TO GET STARTED!