Essential Wireless Network Security Tips for Small Business

Wireless network security tips from Pili Mar

In an age dominated by smartphones and tablets, wireless networks have become an increasingly attractive option for many small businesses. With a wireless network, team members can easily collaborate on mobile devices and laptops from anywhere in the office. Employees can join the network or change locations without any wires to manage.

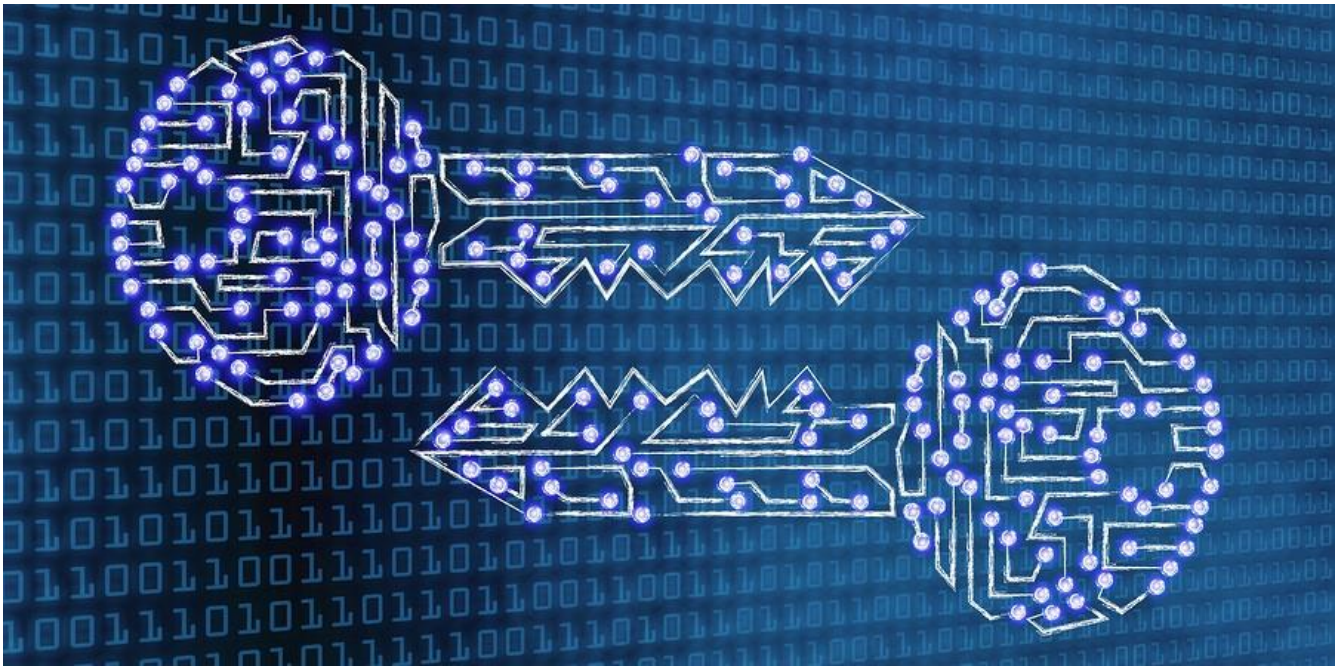
That convenience and portability brings challenges, however, and businesses that choose to go wireless must plan carefully. In addition to some reduction in speed, wireless networks pose an increased security risk. To minimize your risk, consider a few basic tips for wireless network security.

1. Protect the Router

The wireless router directs traffic between the internet and the internal network. The router sends a signal through the air, allowing devices within range to connect to the network. While this is essential in enabling employee access, proper router setup is critical to ensure that hackers within range do not also infiltrate your network.

When setting up and maintaining the router, keep in mind the following:

- **Change the default router password** – Most wireless routers come with a default administrator password. This is the first password hackers will try. Change the password, using the basic rules for strong passwords.
- **Enable the firewall** – While most routers come with firewalls built-in, they are not always turned on by default. Check to make sure that the firewall is enabled.
- **Disable remote management** – Unless you absolutely need to manage your wireless router remotely, turn off this feature. It is simply another avenue for hackers to access.
- **Change the SSID** – The SSID (service set identifier) is the name of the wireless network. Like the administrator password, many vendors use the same default SSID for multiple routers. Leaving the default name signals hackers that you may not have taken time to set up your router completely. Change it to something unique.
- **Keep the router's firmware up-to-date**



2. Use Strong Encryption Protocols

Any information that passes over the network must be encrypted for safety. Be sure that you turn on encryption when you set up the wireless router. In addition, keep in mind that not all encryption protocols are created equal. Look for a router with WPA2 capability, as this is the strongest encryption protocol. Avoid the outdated and highly vulnerable WEP protocol.

3. Limit Network Access

Instead of letting anyone connect to the network as long as they have the correct password, you can limit access to your network to only certain devices. Each device is identified by a unique Media Access

Control (MAC) address. You can configure your wireless router to only allow access to devices with MAC addresses that you specify.

4. Ensure Device-Level Security

As with any network, wired or wireless, individual users and devices still present the greatest vulnerability. Create and enforce security policies to ensure that the devices that access the wireless network are protected from attack. This includes:

- Password protocols for all devices that access the network, including personal smartphones and tablets
- Mandatory encryption
- Security apps on mobile devices
- Making sure that anti-malware and system software are kept up-to-date

Layered Approach Essential to Wireless Network Security

Whether you use a wired network or a wireless network, a defense in depth strategy is essential to keeping critical business data safe from malicious attacks. A single breach of your network can cripple your business with lost productivity, loss of reputation and even legal action.

Increase your wireless network security with proper router setup and strong encryption protocols. Limit access to known devices and implement security policies to maximize mobile device security. The security professionals at eMazzanti can help you design a multi-layer cyber-security strategy to protect your information assets.

Pili Mar graduated with a bachelor's degree in systems engineering from the Universidades de Los Andes in Venezuela. For the past 16 years, she has worked as a network engineer in various industries. She joined the eMazzanti team in the spring of 2019.