Newsletter

Celebrating 30 years serving Central, N.C. *May 2020*

7 Best Security Practices to Keep Your Wireless Network Secure

Wireless connections are convenient, but deploying them carelessly can pose serious security risks. Unless they are well protected, intruders can get into the network without going inside the office or touching the equipment. They can bypass its defenses and steal data or install malware.

Proper wireless management will keep these risks to a minimum. Only authorized people and devices should be able to use your wireless network. To keep the access points safe, you need to set them up correctly and give their use ongoing attention.

Securing Wireless Network

The easiest and worst way to set up an access point is to make it public. There is no password, and anyone can get into the network. Worse yet, anyone within range can use some simple equipment to intercept all the data going back and forth. They can read passwords, email, database responses — anything.

Shopping malls and libraries use public access points because they are convenient, but they put them on-- networks that do nothing but connect through to the Internet. There is nothing to steal. A network that holds business data needs to be more cautious.

Business networks should always select a secure access protocol for their networks. They admit only users who have the password. Equally important, they encrypt all traffic. Anyone intercepting the data will see only meaningless bits.

The designers of wireless protocols have created several over the years. The older ones, WEP and WPA, have known flaws that severely weaken their security. The state of the art is WPA2. It's been around long enough that every device that is not ancient supports it, so there is no excuse for using less.

Keeping access points updated with the latest firmware is important. Last year, a vulnerability was discovered that affected all WPA2 access points. Firmware patches are available now for most devices to avoid the problem. Access points that never get updates, though, could be exploited, letting an intruder decode encrypted data.

The password needs to be a strong one. If it is one that's easy to guess, like the company name, the access point will not stay secure for long.

Upcoming Events

Webinar: How WiFi Can Boost Your ROI
May 14, 2020

Life in the Cloud: Security & Backups Panel Discussion
June 17, 2020

Lunch & Learn: Disaster Recovery- Is Your Backup Good Enough
June 25, 2020

For more information on our upcoming events, please visit https://www.tcsusa.com/calendar/.

336.804.8449 I info@tcsusa.com I www.tcsusa.com

"Security Practices," Continued

Security Best Practices

After setting up a secure network, good practices will further help to avoid break-ins. Here are some steps, most of them relatively easy, to take:

- Most access points allow administrative access to change their settings. Change the administrative account and password from the default (typically something like "admin" and "111111") to something else. If you have the option, allow access to the account only from the local network.
- Set policies on what devices people can use to access the network. A BYOD (bring your own device) policy is convenient for employees, but letting possibly infected phones onto the network is dangerous. Only devices with approved configurations should have access to the network. Mobile device management software is available to enforce policies.
- Use an SSID (access point name) that provides no identifying information. There is no point in calling attention to your network. You do not have to be cryptic; something unique and neutral like "WIRELESS7520" will do nicely.
- If it is feasible, segment the network so that wireless devices do not have access to sensitive data. Usually, there is no need for them to have direct access to databases.
- Enable the access point's firewall if it has one, or put a firewall behind the access point. That will make it harder for infected devices or intruders to do damage.
- If you can control the signal strength, make it just strong enough to cover the area of legitimate use. The closer the bad guys have to get, the fewer chances they have. This is only mild protection, though, so avoid turning the signal down so much that authorized users have slow connections.
- Keep your access points physically secure. Protecting any device against people with hands-on access is hard.

You never know who is lurking outside your office walls. Paying attention to wireless security will make your network safer and prevent costly problems.

Follow us on social media!

What WiFi 6 Means for Your Organization

2020 is the year when Wi-Fi 6 becomes mainstream. It comes with better performance and security than ever for wireless devices. If you are running a business, you need an adoption strategy. Do you want to be an early adopter, upgrading as quickly as possible? Are you going to hang onto the old technology as long as you can? Or is the best approach somewhere in the middle, adding updated equipment in the course of regular replacements?

The best answer depends on your business's needs and how well the current infrastructure meets them, but generally, you should wait until the technology matures some more.

What is Wi-Fi 6?

Until recently, new versions of the Wi-Fi standard had confusing names as editions of IEEE 802.11. To make the versions easier to follow, the Wi-Fi Alliance has created a new terminology. The dominant standard as of 2019, 802.11ac, is now also known as Wi-Fi 5. The new standard is 802.11ax or Wi-Fi 6. For all but the most technical purposes, the names mean the same thing.

Newly shipped Wi-Fi 6 devices are backward compatible with older clients. If you get a Wi-Fi 6 router, your old devices will likely communicate as they always had. If the client's phone or computer supports Wi-Fi 6, it has access to faster speeds and better security while experiencing less interference from other devices.

What is new in Wi-Fi 6?

The new version of Wi-Fi gives you advantages in three main areas.

Devices share bandwidth more efficiently. The latest standard supports a new multiplexing method, called OFDMA (orthogonal frequency-division multiple access). It divides the available frequency into groups or sub-channels that are assigned to different client devices. This technique reduces contention and packet overhead. The advantage is especially significant when the packets are short, as they often are in highly interactive applications.

Higher data rates are possible. The theoretical maximum data rate is 9.6 Gbps. Not all devices need or support the top speed, but it means a higher ceiling on the rate of transmission. More devices can connect to the same access point without reaching the maximum data capacity.

If you would like to receive our newsletter digitally, please email alimbers@tcsusa.com.

New frequency band creating more channels. Wi-Fi 6 branches off from its predecessor, most notably in its change, are frequency band. Everyone is familiar with the 2.4 and 5 GHz dual-band radios touted by modern Wi-Fi routers, but Wi-Fi 6 is actually in the 6 GHz band. The advantage of this is the additional availability of channels, but there is one hurdle yet. The FCC has not yet signed off on the usage of this band for the fledgling Wi-Fi standard. However, this hasn't stopped manufacturers from developing and shipping products. The vote to officially ratify the 6 GHz band for use by Wi-Fi 6 is scheduled to occur towards the end of April 2020 and is widely expected to pass.

Do you need it, and why?

While Wi-Fi 6 will provide some significant benefits, there is no reason to rush into it.

If your current network is performing well enough, there is no urgency. If your company has many devices and their connections are sometimes sluggish, Wi-Fi 6 will help considerably. If you work in a busy office building and many neighbors have routers within range, Wi-Fi 6 will keep them from slowing down your network as much. However, the choice of equipment is still limited.

Wi-Fi 6 will likely reach widespread availability in 2020 or 2021, pending the vote from the FCC. The cost of routers that support it is going down. When you are ready to move forward, you should look for devices that say "Wi-Fi Certified 6" on them. The "certified" part is essential; other devices may have only partial support or follow pre-release versions of the standard.

Upgrading the client-side will take longer. Some high-end phones, such as the Samsung Galaxy Note 10 and S10 and the iPhone 11, support Wi-Fi 6. Support will trickle down to the less expensive models. Adapter cards are available to upgrade existing computers. There is no need to replace all your hardware; you can decide on a case-by-case basis whether the new wireless protocol is necessary.

How long can you wait?

New devices shipping with Wi-Fi 6 are still backward compatible, so your regular devices will maintain connectivity even after the upgrade. Five years from now, your network may look outdated, but there is no immediate danger of obsolescence. Because the approach should be to phase in Wi-Fi 6 and phase-out of the older technology over some time, appropriate planning will mitigate most difficulties. In the long run, Wi-Fi 6 will become the new standard for organizations.

For now, though, our recommendation is to wait to implement it, because it is so new.

totalcomputersolutions
5601 New Garden Village Dr.
Greensboro, NC 27410

In this Issue

Webinar: How WiFi Can Boost Your ROI

Join us for our upcoming webinar!

Date: Thursday, May 14th
Time: 11:00 AM ET
Presenter: *Ian Collins, Analyst,Total Computer Solutions*
Registration: Visit www.tcsusa.com/calendar/ or call 336.804.8449

A strong WiFi connection is a core aspect of any organization's infrastructure. Whether you run an accounting office, manufacturing plant, retail location, or everything in between, WiFi is crucial for both on-site employees and visiting business partners. Unfortunately, not every organization's WiFi network is designed with comprehensive coverage in mind. Having a weak wireless signal or dead spots can harshly affect your bottom line.

Key Takeaways:

- Understand the functions of how WiFi works
- Learn the basics of real-world WiFi deployments in a small-and-medium-sized business environment
- Requirements for a successful wireless integration

In this webinar, we will provide an understanding that can lead to a transformation of the network environment and help maximize business performance.