BEYOND WIFI SECURITY WHITE PAPER

GETBEYOND.COM

Best Practices for Business WiFi

WiFi is an important feature of casual dining restaurants. When it comes to WiFi, speed and accessibility are important to patrons. Consumers view WiFi as a commodity and smart restaurants view it as a tool to enhance the guest experience. However, if you are using WiFi to support payment acceptance, POS system and information management, it's important to separate consumer and business WiFi use.

When guests visit your business, it's likely they'll want access to your wireless network. While this is a great benefit to offer your customers—and often necessary—it's important to keep customer access separate from that of your business systems and your users. With recent advancements in WiFi technology, it's easy to allow guests to use your wireless network while segregating them to only have Internet access. However, a better strategy is to have totally separate WiFi networks. Ensuring that they are kept separate can help to keep your business secure.

Security aside—customers expect fast payment authorization, they don't want to wait for slow and overtaxed networks. When consumer WiFi access is combined with the communication needs of a business, you may be putting your payment authorization speed at risk. Adding back in security considerations, separating business and specifically payments authorization is a requirement for PCI compliance (version 3.2.1, May 2018.)

Use WiFi Protected Access 2 (WPA2)

WPA2 is currently the most secure choice. Additionally, Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) are the two different types of encryption you'll see used on networks secured with WPA2.

WPA2 is a security protocol that uses all the important security elements associated in the 802.11i IEEE security specification, and it will help to keep your business wireless network secure.

There are two different types that you need to know about:

- WPA2 Enterprise—this type uses 802.1x authentication
- WPA2 Personal—this type uses a standard pre-shared key

When it comes to keeping your business secure, WPA2 Enterprise is the best option, as it requires systems and users to authenticate using a unique username and password.

There are several additional steps you can take to further secure your business WiFi, among which include securing access points, limiting WiFi coverable, deploying a wireless intrusion prevention system and mobile device management.

Secure All Access Points

To provide optimal coverage, your business wireless LAN will need to be evenly distributed, placing access points in inconvenient locations, such as ceilings and closets. While you may need to gain access to these access points, it's important to physically secure those access points as best as possible in order to prevent tampering and potential theft. Select access points that will allow you to mount the device in place and secure it with a lock. In addition to physical security, make sure that local access to WiFi access points require unique passwords. Securing and checking access points is a requirement to maintain PCI compliance (section 1.2.2, version 3.2.1, May 2018.)

Limit WiFi Signal Strength

While strong WiFi is great for your customers, a strong signal isn't always a good thing for business WiFi. You need your signal to be strong enough for your systems to interoperate but don't want unauthorized users to gain access. You may put your business at risk if your business WiFi signal extends beyond the walls of your building to public areas.

Use Wireless Intrusion Prevention Systems

To keep your WiFi and business communications secure, it is recommended to include a dedicated wireless intrusion prevention system (IPS) as part of your wireless security. IPS devices monitor and detect nefarious and targeted WLAN attacks using AP spoofing, packet floods, malicious broadcasts, and other techniques.

Access Point Placement

There should be 60 feet between access points for commercial deployment that does not have walls that block RF. You might want to use a signal meter on your phone to measure signal strength just to be sure. If you plan to do voice, you will end up putting them closer together. Correct placement minimizes coverage overlap, which can happen when an access point's area of coverage intersects with another.

Minimizing Wireless Interference

Noise and interference are unfortunate side effects of a wireless network that can inhibit a network's performance and availability. Wireless flow can be intercepted and blocked, preventing devices from connecting to the wireless network. There are a few ways you can improve access point placement around known areas of interference:

- Devices, such as microwaves emit electromagnetic signals and can block wireless signals. Access points should be placed as far away from these devices as possible.
- The concrete, brick, and other dense materials that comprise your building can also block WiFi signals. Access point placement should consider the building materials around it in order to maximize wireless access efficiency.
- Neighboring wireless networks can also cause interference.

Conclusion

Your patron's enjoyment at your place of business is important but securing the future of your business is equally, if not more important. Separating customer use and business use of WiFi is a step in the right direction.