Does your Wi-Fi need a workout?

Consider these four things when beefing up your retail wireless system.

By Amitesh Sinha

Customers expect a seamless shopping experience between your online and in-store presence these days, which means offering Wi-Fi is no longer considered a luxury, it's a necessity. And, offering Wi-Fi is one of the easiest ways you can provide a positive experience for your customers.

Eighty percent of customers feel in-store Wi-Fi would influence their purchase decisions, according to research conducted by JWire. In other words, customers would be more willing to purchase from a store that provides Wi-Fi.

Having in-store Wi-Fi doesn't just offer internet access to your customers, it enhances their experience by allowing them to browse, place an order and make payments through their mobile devices. There are three important things home furnishings retailers should consider when upgrading or installing an in-store Wi-Fi solution.

Customize your network

The key to servicing tech-savvy consumers and meeting the influx of applications and devices into the network depends on how you optimize your retail network.

When implementing a network, you'll have to take into account the context of users, devices, location, privileges, the applications used and duration of time. Consider investing in wireless hotspot equipment that provides the features you need in a retail environment—like being able to limit bandwidth, optimize roaming and cellular handoff and have captive portals that require users to accept Terms of Service (TOS). Traditional access points and routers don't have these same robust capabilities. Some examples of high quality Wi-Fi hotspots include: Aerohive (the AP170), Aruba (the MSr2000), Cisco (the Aironet 1570), Meraki (now owned by Cisco), Ruckus (the T300 series).

Apart from the hardware, consider installing a firmware that upgrades the features of the Wi-Fi connection. One example of firmware suitable for many WLAN routers is DD-WRT. It supports a lot of value-added features such as complex configurations, integrated captive portals, and support for third-party servers. Another good firmware is the CoovaAP firmware that offers many of the same features as DD-WRT firmware. However, it comes with additional functionality of allowing you to limit bandwidth on routers that don't have such capabilities, as well as offer automatic log-in to the customers. This allows you to create a captive portal page that lets the user confirm he is accessing and agrees to use it based on your terms; and you can limit the amount of bandwidth or internet power guest users can have at any time.

However, routers and firmware don't have the ability to segregate private and public internet connections for more security to internal networks. One way to protect your internal network is by investing in a Fonera Simpl router from Fon. Apart from segregating the networks, it also allows putting a limit to the daily Wi-Fi access by customers. Another benefit of setting up in-store Wi-Fi access using this router is that it requires users to sign up with Fon to access the network that adds an additional layer of security to the wireless network.

If you have a large retail setup, or want to offer Wi-Fi access to a large area, you should consider purchasing Open Mesh. This economical router offers both public and private wireless access including the usual features such as speed limits and captive portal; a captive portal is a Web page that the user of a public-access network is obliged to view and interact with, before access is granted. In addition, the hardware makes use of a proprietary mesh technique that allows easier installation.

Ensure compliance

Installing a Wi-Fi network without focusing on security is a reckless strategy. This can make your store vulnerable to lawsuits. Without focusing on security of the Wi-Fi network, you are exposing customers to online attacks. If hackers can infiltrate the network and steal customer information such as credit card numbers, they can sue you to recover the loss.

User privileges and identity are centric to VLAN/Wi-Fi SSID association and network access. It is also crucial for defining security policy in a VPN tunnel, firewall, or for application security. Users along with user groups define the QOS policies' definition for traffic management, and establish service level throughout the various parts of a network and entire security policy framework. This allows you to monitor the traffic on your network and limit the availability to guest users. For example, you can set up a guest SSID with no user id or password and only allowing a certain amount of bandwidth so in case it goes over, it does not affect the working of your business critical applications.

This model results from the fact that a particular user, especially staff or a store employee, is not restricted to using a single device or even location or the network access limited by SSID.

Therefore, enforcing security and meeting PCI-DSS compliance is dependent on the network where users connect.

To avoid legal complications, implement a high-grade wireless security policy to protect your customers against hackers. Install enterprise grade firewall, antivirus, malware, anti-spam and website content filtering solutions.

For a cool way to automate the authentication process, you should consider configuring QR codes with the router and embedded passphrase. This can be made possible by using a Wi-Fi QR code generator software easily found on the internet.

Why Wi-Fi?

IBM surveyed shoppers and found that 45 percent of consumers use two or more device technologies to shop and make buying decisions, typically a laptop and cell phone. Today's shoppers can choose from many outlets to shop, and expect a seamless experience in terms of placing the order, pickup-and-delivery and exchanges-and-return in any combination of outlets. Mobile connectivity is an essential part of this.

Cost effectiveness

It's important to strike a balance between both wired and wireless network infrastructures as well as deployment aids to your store's bottom line. Rightsizing and integrating a wired/wireless network for optimum capacity, efficient utilization and balanced planning of respective wired ports versus the wireless network all add towards cost-effective IT for your store.

When you have the right network platform, you can select an integrated access infrastructure that has deep visibility for the users and applications on the network. In other words, your IT administrator will be able to quickly and proactively troubleshoot and resolve problems before they affect any of your business services or end-user experience.

Cloud-control software

Retailers should install a cloud control software for monitoring traffic and data. Using the cloud control software, you can perform multiple actions such as monitor load on access points, track network usage, monitor number of clients, track devices and OS used to connect to the Wi-Fi network, and configure limited access to the network based on specific device IP (internet protocol) address.

A cool feature made possible by cloud controller software is splash page creation. This page can be displayed on the screen of the users who access the wireless network. You can create pages that highlight popular deals or items your users might be interested in knowing about.

Wi-Fi access can improve overall customer shopping experience by allowing them to connect to the network thorough their mobile devices. It helps extend sales experience from the store into the mobile devices of the customers. As a result, a retailer can better serve customers based on their needs and requirements. You can promptly engage the customers and promote content and brand to your target customers. The end result is better customer satisfaction, increased conversion rates, and higher chances of repeat customers. NOW

Amitesh Sinha is a technology consultant based in North America with over 20 years of experience developing and deploying solutions for retail. He can be reached at amitesh@iconnectgroup.com.