There Has Never Been a Better Time To Invest in Multifamily Technology

Residents expect the convenience of on-site seamless connectivity. The right network is key to protection.

By Matthew Matlack / *Multifamily Broadband Council and CommScope*

The role of data privacy has become increasingly relevant to the multifamily industry as residents continue to demand more and better technology. Property management companies and building owners are experiencing the benefits of offering free wireless access in public areas on-site.

Public wireless access has become an important tool and somewhat of an expectation as students and working professionals are now more mobile than ever. They want to be able to access Wi-Fi for work and to stream entertainment platforms such as Netflix, Hulu, Pandora, Apple TV and Disney+ no matter where they are on a property.

Residents appreciate the convenience of public Wi-Fi, but many users tend to overlook the security risks associated with accessing it. Offering these complimentary services requires a robust technology infrastructure that is secure.

UNDERSTANDING SECURITY RISKS

Apartment communities must be conscious of the security risks of exposing Wi-Fi users' personal information. If a property provides free connectivity in common areas, such as a lobby, an outdoor space, a pool or a laundry facility, it should at minimum require a log-in page where a user must accept the terms and conditions and acknowledge that the network is not secure. Equipment meant for commercial traffic versus individual home use can provide additional network security.

Even with the right equipment and technology, residents need to understand the dangers of sharing sensitive data over an open wireless connection. Personal data – such as social security numbers, birthdays, driver's license information, credit card details or any other banking or financial information – should never be shared on an open wireless network. A compromise of a resident's data results in a loss of customer trust, and the process to address identity theft can be cumbersome.

According to Verizon's 2019 Data Breach Investigations Report, the most common motive behind data breaches is financial gain. Research from this report also shows that users are significantly more susceptible to social attacks when using mobile devices. The most common security threats include email-based phishing and spoofing attacks that mimic legitimate webpages. Social media is yet another way people share very personal information that may fall into the wrong hands.

Multifamily owners constantly upgrade facilities and add new services to make their buildings more appealing to residents. It is estimated that the average home has at least eight devices connecting to the internet; meanwhile, consider that one multifamily community has that number of devices multiplied by the total number of units and

residents. Because residents now expect a seamless wireless experience in their homes and throughout the property, it is becoming increasing important for multifamily owners to invest in robust, secure technology.

A DIFFERENTIATED AMENITY

Property owners often lack the time, IT resources and vision to build and manage solutions that meet the requirements of a reliable, integrated wired and wireless experience for residents and guests. Safety enhancements such as security cameras in public areas, parking lots and other facilities can now be managed as part of a single system. The goal is to deploy an intelligent system that can easily detect potential security threats before they become an issue. Today, automated door locks can help address lost keys, which is another security enhancement within the multifamily environment.

Communities can learn more about their residents by collecting data to help identify trends and consumer behavior. Learning about the traffic patterns within a multifamily environment can help owners and operators understand where residents congregate and relax and can confirm that investments are worthwhile. This may also help identify where to locate new retail outlets that support the needs of residents.

Each time a resident or guest connects to a network, there is an opportunity to market and expand brand awareness. This is often achieved with a simple onboarding portal that allows residents to enter a username and password to guarantee secure access, which is available throughout the facility. However, guests may have wireless access only in common areas, and their technology experience can be limited to when they are visiting a resident.

Residents will log into their tenant portal initially to onboard devices such as computers, laptops, printers and mobile devices. Once approved via the onboarding process, these devices will automatically connect to the network propertywide. IT automation will help save time for residents and make their initial move-in much smoother.

Finally, a secure portal for residents can also display data in real time from numerous sources, such as utility bills, rental payments, lease terms and other information that may be helpful, such as school information, local news and weather, etc. This portal can be easily customized to help share urgent information that could be useful in an emergency, such as preparing for severe weather. Valuable information within this portal can help apartment communities differentiate their offerings to residents.

A primary barrier to deploying reliable technology within a multifamily setting may be budgetary constraints. One possible reason for the lack of funding for Wi-Fi equipment is a perception that the network is merely an unnecessary expense, as residents typically have their own wireless equipment. A different approach is needed, and multifamily owners should see that pre-installed Wi-Fi at a community is a differentiated amenity. In addition, pre-installed Wi-Fi would be based on enterprise-grade equipment, offering better performance than what residents would typically access individually. Availability of higher-quality wireless service throughout a property's common areas is attractive to many prospective residents and creates a lasting positive impression that converts to leases. ❖

Matthew Matlack is a member of the Multifamily Broadband Council and territory account executive, Ruckus Networks, at CommScope. He can be reached at matthew.matlack@ commscope.com. MBC Executive Director Valerie M. Sargent also contributed to this article. For more information on MBC, please contact her at vsargent@ mfbroadband.org or 949-274-3434 or visit www.mfbroadband.org.