Is Wi-Fi Security Top of Mind? It Should Be.

Bulk managed Wi-Fi must have airtight network security plans to protect multifamily owners and residents. Here's what that takes.

By Ed Neipris / *Blueport*

The ever-changing technology landscape of today, coupled with a competitive marketplace that seems steeper than ever, means many multifamily owners and property managers have turned to managed Wi-Fi to help set themselves apart from competitors. A network that is always on benefits everyone in a multifamily community, providing a seamless resident experience and enabling owners and managers to optimize profits and prevent expensive problems.

Potential residents now cite fast, reliable broadband as one of the top amenities they look for when evaluating an apartment complex today. Before blaming millennials, owners and operators should consider this: The National Multifamily Housing Council found that more than 80 percent of people over the age of 55 cited pre-installed Wi-Fi as a preference. In fact, they desired it more than reserved parking (No. 2) or stand-alone showers (No. 3). When looking at the overall preferences of residents, short-term rentals and on-site pet facilities ranked slightly lower than virtual assistants and smart locks.

> Managed networks authenticate users and make sure traffic on the network moves smoothly.

No one can predict the future with 100 percent accuracy, but it is safe to say that the amenities that were seen as "must haves" just a short time ago are being outpaced by the lure of shiny new technology designed to make life just a little bit easier.

For multifamily owners and operators, communitywide Wi-Fi and peripheral add-ons such as smart thermostats and water sensors help control costs on empty units and prevent excessive damage when problems do arise.

When implemented with *secure technology,* managed networks can be an essential driver in maintaining brand loyalty, attracting new residents and increasing revenue.

SECURITY A GROWING THREAT

Navigating internet and TV providers is one of the biggest challenges facing multifamily owners and operators. Until now, the default has been to let legacy cable and phone companies handle the service. But that approach leaves multifamily owners and operators, along with their residents, at the mercy of the provider, waiting days for installation only to receive limited direct access within the confines of residential units. Or, residents may be instructed to contact local providers and negotiate service on their own. In either case, a critical layer of security often is overlooked.

Residents are very vulnerable whether they have "choice networks" (non-bulk communities in which residents call a cable company for a la carte internet) or bulk Wi-Fi programs. Multifamily staff is vulnerable when accessing confidential resident and company information.

It is becoming more and more difficult to control where data ends up and who can access it. As multifamily executives seek technology to power business innovation and attract residents, safeguarding data is more vital than ever.

A few years ago, the General Data Protection Regulation and the California Consumer Privacy Act brought awareness to the inherent flaws of Wi-Fi. Today's security landscape is even more challenging; cyberattacks are on the rise and predicted to cost the world $6 trillion annually by 2021.

Most communitywide Wi-Fi networks are unencrypted, meaning any device connected to Wi-Fi effectively sends all data in clear text, essentially leaving an open door for hackers to identify and extract personal information. Even websites with an SSL certificate (https://) aren't necessarily safe.

There are three indicators staff and residents of multifamily properties are not protected:

- The network uses a captive portal (sign-in page) to authenticate users.
- Staff, residents and/or visitors share one Wi-Fi password.
- Using a single SSID with no passphrase provides a breeding ground to "man in the middle" (MITM) attacks.

The surge in residential internet access has created an open door for cybercriminals to easily capture private information. With security breaches on the rise and a spotlight on privacy laws, multifamily executives need to evaluate and block security risks now to stop MITM attacks, rogue access points and other threats.

ADVANTAGES OF MANAGED NETWORKS

Managed networks offer a number of advantages when it comes to security and service. When someone begins waxing eloquent about a "managed Wi-Fi solution," you should think "traffic cop." But think of a traffic cop who can check your ID as you roll past at the speed limit. The cop is not invasive, helps keep you safe and, frankly, got everyone out of your way so you could make it through that intersection quickly.

The managed network authenticates users. Are you supposed to be on this network? If so, please, pass right on through. The managed network makes sure that traffic on the network moves smoothly. I may never notice that my game of Words with Friends was slowed by half a second, but the person making a Wi-Fi call next door will notice if her call is delayed. The network prioritizes traffic to the internet and removes the bottleneck.

From an operator's perspective, a managed network that offers tenants a 300 Mbps experience can accomplish that far better than if each device fights for priority. A standard network requires that fight, and all devices must stand by while the winner is sorted out.

Another advantage a managed network offers is white-labeled support. Most firms offering managed networks will happily take calls from tenants when there is an issue. If connectivity is the No. 1 amenity your tenants look for, and it is, then you had better make sure it is good! I will never understand why so many properties happily offload that amenity and leave it to providers.

THWART SECURITY THREATS

Let's say you decide to install a managed network. Congratulations! You have blazing fast speeds, and it didn't cost you an arm and a leg. Now let's talk specific security threats.

As part of your agreement, you likely have your office staff working on that nice, new, fast internet. Are they secure when they enter residents' information? Are the residents secure as they check their bank accounts at home? Are you liable for any of this?

With great technology follows great ways that bad people can exploit it. Two

CONSIDERING A MANAGED NETWORK? ASK THESE QUESTIONS.

Let's assume you are sold on the idea of a managed network. You've even had someone quote the cost of installation. Now you must figure out how to pay for it. Odds are that one of the phone calls you made was to a major provider that already services your building on a retail basis. It made the case for a "bulk" agreement, and you have questions. Here's what you should do.

1. **Ask residents about their experience.** How many residents rate their experience with the provider as an 8, 9 or 10 on a 1-to-10 scale? If the majority do not, end the conversation. You don't want to trust that provider with your entire property. It can't keep existing customers happy.
2. **Look into taxes and fees.** The provider will undoubtedly bring up the additional cash flow that can be generated: You commit to buying 400 units worth of TV and internet, so you get a hefty discount. But when evaluating your potential revenue stream, find out how much the taxes and fees will be. Taxes are easy – it should be sales tax. Fees – well, no one really knows what those fees are. Get the all-in cost!
3. **Review the service level agreement (SLA).** An SLA tells you how slow service can be and still comply. Next time you see the big ad for "Fastest starting speeds 300 Mbps!," read the fine print. In very small font, it will say "up to" right in front of the *3*. When you sign the contract, you'll notice an SLA for more like 20 Mbps. That is the speed at which your tenants will surf the internet most of the time.

major assaults being used today are the MITM attack and the Pineapple attack.

Imagine this: You want to know where and when most of the bandwidth of your network is being soaked up, so you buy a Pineapple device. It costs about $80 and is a great tool for finding out what the traffic on your network looks like. If you have a little technical talent and nefarious intentions, you can look more deeply at that traffic. You can look at which computer is getting on which site. Then you can look closer to see keystrokes. Suddenly, you know that apartment 305 went to a bank website, typed in myname@hotmail.com and entered my wife's birthday as the password. It really is that simple; you don't have to be an administrator for the network. Most networks are secure only to the point of whom they let on. For security, Blueport suggests that operators either encourage residents to protect themselves with a simple investment in a VPN or install software on the network that encrypts the data from device to access point.

The MITM is even more simple. Let's say your network name, or SSID, is "MyCommunityWi-Fi." You open your device, you see "MyCommunityWi-Fi" and you connect. You've just joined a network being run by a third party and you have no idea. This third party is now watching in real time everything you do. Bank account information is taken, social media hacked, even the pictures of your family are at risk.

PROTECT YOUR NETWORK

A host of companies, including Blueport, offer network security solutions, helping multifamily properties beef up security in managed networks. For instance, Blueport's patent-pending Global Roaming Passphrase solution includes portal-less options and fully encrypts residents' data without the need to switch internet providers or install expensive hardware.

The technology is cutting edge, but it's very simple. If my device speaks a different language than your device does, then an MITM or a Pineapple attack is rendered useless.

Most networks focus on securing who gets on the network, but once on, all devices speak the same language. Something like a Global Roaming Passphrase makes sure all devices speak different languages. Then, the Pineapple or MITM will speak a different language than my device does.

Resort-style, managed networks are wonderful things, but finding ways residents can enjoy them safely is essential. ❖

Ed Neipris is the CTO and co-founder of Blueport, a provider of network security solutions.

Fiber-To-The-Home TOP 100 Broadband Communities Magazine 2020

AEG
ATLANTIC ENGINEERING GROUP

706.654.2298
www.aeg.cc

Fiber-to-the-Home Experts with 63 City-wide FTTH Projects Completed

50,000 Miles of Outside Plant Constructed

2.5 Million Homes Passed with Last Mile Fiber

Fiber Optic Solutions

Outside Plant Engineering | Aerial & Underground Outside Plant Construction | Project Management & Planning