Hotel News Now

Tech Impact Report

Hotel Wi-Fi: Balancing security with convenience

11 NOVEMBER 2020 1:10 PM

A recent warning from the FBI about hotels’ Wi-Fi brings network security back into focus, but tech experts said the federal agency’s PSA doesn’t tell the whole story.

By Bryan Wroten
bwroten@hotelnewsnow.com
@HNN_Bryan

REPORT FROM THE U.S.—Finding the right balance between making hotels’ Wi-Fi networks more secure against guests’ desire for easy-to-use Wi-Fi has been an ongoing struggle for hoteliers, and it’s recently come into the spotlight again.

After hotel companies had been marketing their properties for months as a refreshing change in scenery to people working remotely during the pandemic, the FBI recently put out a warning to the general public about the privacy risks of using hotels’ Wi-Fi networks. It warned of hackers spoofing hotels’ official networks to trick guests into using the wrong networks or taking advantage of a general lack of robust security protocols to access and steal guests’ work and private information.

While the FBI warning isn’t wrong, there’s more to it than what the warning says, said Ted Harrington, executive partner at Independent Security Evaluators.

“The main thrust is that it's not inherently that a hotel is problematic, it's that public Wi-Fi is problematic,” he said. “Second is that poorly secured networks are problematic—and many hotel networks are poorly secured, but that's not inherently true across the board.”

The FBI addresses valid concerns, but the timing of it is interesting because the hotel industry is trying to attract people to use hotel rooms as alternative remote-working sites, he said. However, prior to the pandemic, people used hotel Wi-Fi for work purposes as well.

"The thing is that I hope that people in hospitality don't panic about this, but do understand that people like me, this is what I get on a stage to advocate for multiple times a year, because (to) hospitality groups, this … isn't new information, but (when) presented this way I think is maybe alarming to people."

Improving security

Wi-Fi security in hotels is tough to get right because it's a balance between accessibility and security controls, and the two are often at odds with each other in public networks, said HTNG Chief Information Officer Patrick Dunphy.

"At the end of the day, convenience is king for customers and for guests, which is why guests overwhelmingly pick open networks," he said.

Guest and customer safety are the highest priority for any hotel company, from the largest brand to the single independent property, he said. It's wrong to say the industry doesn't have a Wi-Fi standard, as there are several standards the industry uses, such as Hotspot 2.0, WPA2 and now WPA3. It's up to the individual businesses and brands to understand which of these best suits their customers' needs, which can vary by location and jurisdictional regulations.

HTNG's Centralized Authentication and Improving the Guest Wi-Fi Experience workgroups are focusing on bringing together these technologies to make it easier to onboard guests outside of the traditional splash page or portal page that's asking for guests' room number and last name, he said.

They're also looking at things like piping into the loyalty program or other profile-based credentials that allow a guest to automatically log into a brand's network seamlessly at different hotels, he said. One of the added benefits of this is that these are more secure technologies. Another is better engagement with guests.

"Once you start thinking about Wi-Fi as a platform to engage with your customer, the byproducts of which are secure connectivity for the customer and also more opportunities to engage with the customer, the guests and certainly the staff at your hotels and then certainly your brand as well," he said. "It's important to start thinking about Wi-Fi as a tool to engage the guests, not just a way for your guests to get out of the internet to do whatever it is that they normally do."

It's also a myth to say hotel networks aren't as secure as home networks, as many people regularly turn off their security features for the sake of convenience, Dunphy said. Home networks generally use unsupported consumer-grade equipment that haven't been patched in years, while hotel networks use enterprise-grade equipment and receive frequent updates with trained professionals overseeing them.

Most of the online traffic today is already encrypted outside of hotels' networks by individual websites on their own, Dunphy said. Because of the nature of the internet now has changed over a period of time, it's essentially become an industry standard and best practice to encrypt websites, and it has been this way for at least the last 10 years.

"So even if a hotel Wi-Fi network is open, it does not by default mean that your information is being stolen or that your credit card numbers are in the clear or then anybody's got access to things that they shouldn't have," he said.

Competitive advantage

Improving security is a competitive advantage over poorly secured networks, Harrington said. The two steps involved are securing the technology and then proving it. What's wrong with a lot of security today is that many companies skip the first step and try to move directly to "proving it," but in the context of hospitality and Wi-Fi, hotel companies generally don't even attempt step two.

Some brands are investing in securing their Wi-Fi networks, using enterprise-class systems, but others aren't, he said. Some hotels are having guests connect to Wi-Fi through a small office or home office router, not business-class equipment.

"What's as crazy is that some of these properties are investing in equipment and processes and produces and people in order to actually be secure, and others aren't, but neither of them even try to prove that to the guests," he said. "That's an enormous opportunity that's being missed."

One way to think about this is it's a way in giving guests assurance, Harrington said. If hoteliers do the two steps correctly, by communicating that to guests, they can make guests trust the hotel and the brand more while also making them question why others aren't doing the same thing.

Addressing spoofing

Spoofing an official hotel Wi-Fi network, the other problem addressed by the FBI, has been an issue for years. One of the industry's responses to this problem was blocking Wi-Fi networks guests could create on their own. But in 2014, the FCC fined Marriott International $600,000 for blocking these networks.

The federal government hasn't supported the technologies necessary to fight this problem, even though the technology is commonly available, Dunphy said. This is something the federal government must support from a regulatory basis, he said.

"I think it's a valid use of that technology to prevent issues like that, and it's unfortunate that the (FCC) is taking the stance on that considering that's a very valid way to prevent a problem," he said.

Aside from a tech fix, there is another approach, and that's messaging. When a guest checks into a hotel, the front-desk associates should tell the guests exactly which Wi-Fi network to connect to, Harrington said. Most of the hotels he has stayed at do this, but there might be some who don't share that information specifically, either verbally or in writing.

"Make sure that you make it easy for the guests to know which network to connect to and to only connect to that network," he said.