HN Hospitality Network

How to Make Hotel WiFi Networks Secure

From checking emails to streaming shows, hotel guests rely on the internet for various activities. While this can be incredibly convenient for guests, using such networks can also come with risks. For hoteliers, it is essential to establish secure, high-speed networks for guests.

How Secure is Hotel WiFI?

Like any WiFi network, hotel WiFi networks are only as secure as they are built to be. Unfortunately, in many hotels, hotel WiFi networks can be just as vulnerable as public networks.

Hospitality Industry

2nd Largest

Number of Cyber Security Breaches

Behind Retail Sector, According to PwC[1]

The Three Largest Threats to Hotel Wifi Security

1. Ransomware

Ransomware is malicious software that encrypts a victim's files and demands a ransom be paid to decrypt them. This attack can be devastating for hotels, as it can prevent them from accessing important guest data or even cripple their ability to operate altogether.

2. Phishing

Phishing is a type of cyberattack that involves tricking victims into clicking on malicious links or attachments. These links or attachments often appear to come from legitimate sources, which makes phishing attempts all the more difficult to spot.

3. Encrypted Malware

Encrypted malware is used to evade detection by antivirus software. This type of malware is particularly dangerous because it can give attackers access to sensitive data like credit card numbers and guest information without being detected.

Both Consumers & Businesses Are Integrating Cybersecurity

62%
of Organizations
Have an Encryption Strategy in Place[2]

85%
of American Adults
Use Antivirus Software[3]

Tips to Make Hotel WiFi Networks Secure for Guests

How can hotels protect themselves and their guests from these threats? Although it's impossible to avoid potential threats altogether, each of these steps can lower a hotel's risk.

Harness Strong Encryption Technology

Robust encryption technology, such as WPA2 & WPA3 encryption, helps to prevent data breaches and protects guest information.

Install Reliable Antivirus Programs

Hotels should also consider installing a robust antivirus solution to protect property from encrypted malware and better detect potential threats.

Closely Monitor Hotel WiFi Activity

Monitoring activity on the hotel WiFi network is a crucial safety step to protect hotels from hackers. By keeping an eye on any suspicious activities, hoteliers can quickly spot any potential threats and take steps to mitigate them.

Implement a Log-In Portal Requirement

Log-in portals ensure that all guests enter their usernames and passwords to access the internet. By implementing this extra step, hotels can deter many would-be hackers and gain valuable information about who is using a network.

Let Hospitality Network Handle Your Hotel WiFi Security

At Hospitality Network, we understand the unique challenges hotels face when managing their WiFi network. As a secure, reliable WiFi provider, we can help you take the necessary steps to protect your property from hackers and keep your guests safe while they use your WiFi network. Contact us today to learn more about how we can help you improve your hotel WiFi security.

1 PwC Hotels Outlook Report 2018–2022
2 Ponemon 2022 Global Encryption Trends Study
3 Security.Org 2023 Antivirus Market Annual Report