OPERATIONS

Open Season for Hacking: How to Prevent Data Theft When You Offer Free Wi-Fi

Free Wi-Fi may be in-demand with customers, but is it worth the liability? Coffee shops and restaurants are clamoring to install Internet services, yet forgetting to implement critical cybersecurity measures for their restaurant. With public Wi-Fi becoming standard, preventing hackers in your restaurant means beefing up your security, data breach prevention, and properly installing your networks.

As experts say, it's not *if* a problem happens, it's *when*. Just by having a Wi-Fi network, you hold the keys to social security numbers, banking transactions, tax documents, and other critical personal info that hackers could gain access to. By putting these tactical steps for hacker prevention in your restaurant into practice today, you're not only protecting your customers' sensitive information, but your business' as well.

Set Up Two Secure Networks Through a Reputable Installer

"Security is important especially since people are relying on the network to do some pretty sensitive stuff," says Dror Liwer, chief security officer at Coronet. Liwer cites a study he read stating that 62 percent of Americans conduct banking transactions on public Wi-Fi networks, and they probably have no idea how dangerous that is, he adds. However, if restaurants set up secure networks, the data breach prevention in your restaurant and the protection of your customers info can be increased.

Install two separate encrypted Wi-Fi networks; one for your business and one for customers, on different routers, says Robert Siciliano, Cybersecurity Analyst for ETFMG.com. And even if you have to spend a bit more money to prevent Wi-Fi hacking, it's always best to err on the side of caution, he advises.

Use a reliable, well-reviewed company for installation, too, because "not all public Wi-Fi products and installers are created equal. You need to ask a lot of questions, and you need to do your own research," explains Kevin Levy, chair of technology transaction practice at GrayRobinson, "After you've put [your systems] in place, you need to protect yourself by letting [customers] know as often as you can that this is public, open Wi-Fi. If they have something that's confidential, they shouldn't be accessing it through the Wi-Fi."

Use Passwords and Change Them Often

Setting passwords may seem obvious, but Liwer says he's seen a "vast majority" of restaurants and coffeeshops have password-free networks. Why? It's too annoying to be asked, "What's the password?" multiple times per day. Yet, having passwords improves your data breach and hacker prevention for your restaurant. If you changed the password daily, or at the very least weekly, you and your customers are much better off, says Liwer.

It's true that hackers could walk in and get your general password from your staff. However, it's not just preventing hackers inside your restaurant that are the problem. Siciliano says hackers can sit in parking lots to conduct their illegal activities. But if your network is password protected, you're safer from them wreaking total havoc.

If you really want to take the cybersecurity for your restaurant to the next level, you could invest in a receipt system that prints unique Wi-Fi passwords for each customer. That way, the customer network has another layer of security. "To me, that's the best because even if an attacker spoofs the network, they'll have a password that's only going to be good for themselves...if every customer gets their own five-digit code, that's the safest thing to do. It comes with a cost...but it's the safest," says Liwer.

Have a Pro Team On-Hand, and Train Employees to Handle a Data Breach

The most prepared companies have a PR firm, law firm, and breach notification company on speed dial so if something does happen, they can get the team together to make decisions quickly, says Levy. If nothing else, experts recommend training staff on what to do in the event of a data breach and identify which employees can serve as a crisis management team. The quicker you respond during a cybersecurity emergency, the better. If a hacker breaks into your public Wi-Fi, steals important files, and customers find out they're part of a data breach, it's unlikely, but still possible, that they could sue your restaurant, Levy explains.

It's possible your restaurant could be held responsible for the open Wi-Fi network even though it's a service and considered a shared responsibility between customer and operator, adds Liwer, "Keep rotating passwords, and make sure they're not obvious...the harder the password is, the higher the encryption and therefore, the more secure the network is going to be."

Back to Top

Up Next

Restaurant Equipment Maintenance: Failing to Plan is Planning to Fail

Read More —

DIGIDAY
CONTENT MARKETING
AWARDS
2020 FINALIST