Franchise
Cyber Security
Best Practices

POWERED BY

WIRED

As a franchise owner of a small business, your worries are diverse and numerous, but studies show cyber attacks don't make the list.

Perhaps no one told you in a span of 12 months 50% of all small businesses were breached. Yes, that's right. According to Keeper and Ponemon Institute, half of the small brands in the United States experienced stolen information in 2016. An astonishing 60% of those data theft victims weren't able to bounce back, going out of business 6 months following the infiltration.

Given the size, minimal staff and fewer funds for defense, small franchises are painfully positioned to suffer from incoming threats. Are you willing to flip a coin on that type of risk?

Cyber Security is Everyone's Problem.

What is at Stake

- Customer records
- Customer credit and debit card information
- Intellectual property
- Business correspondences
- Financial information
- Employee data

Types of Threats

- Phishing
- Point-of-sale (POS) malware
- Viruses
- Ransomware

How prepared is your franchise?

Run through this basic checklist to ensure you're following best practices.

6 Month Password Update

When is the last time you reviewed password etiquette with staff? Franchises that have passcode best practices in place and do not strictly enforce the rules leave room for vulnerability. As a guideline, staff employees should curate a new computer password every 6 months. The new password should be at least eight characters in length, contain no recognizable whole words and include at least one symbol and number.

Restricted Access

Not everyone in your staff should be granted the same viewing privileges. Unless the information will help an employee's work performance, sensitive data needs to be sectioned off. If by chance a company device is lost or stolen, ensure you have the capability to wipe phones, computers and laptops remotely of all information to keep franchise information safe.

Secure Wifi

Avoid too common network names or service set identifiers (SSID). Selecting the Internet provider's name by default or using another common term, can make it that much easier for hackers to weasel there was through your WPA or WPA2.

Create Backups

With POS systems and business software residing in the cloud, a temporary Internet outage is an emergency. Imagine the revenue loss from a 30-minute Internet drop. This also affects customer experience and employee productivity.

Another form of security franchises require is a hybrid backup. This ensures your company's sensitive information is safe by simultaneously sending data to a server and the cloud for optimal coverage against malware and hard drive failure.

Properly Install and Test Your Firewall

Invest in a quality enterprise security appliance, like industry-leading Cisco products, to establish perimeter security. Cheap hardware and poor setup put your data and reputation in danger. To verify the effectiveness of your firewall, tests need to be conducted ideally every quarter.

Consider Hiring a Professional

If developing and managing a cyber security plan seems a little complicated, overwhelming or you just don't have the time, you're not alone. A team of experienced technicians, like WIRED, can curb stress by providing the basics noted above while also extending your encryptions, bolstering internal security and fortifying your firewall with 24/7 monitoring to proactively squash attacks.

Layering your cyber security protection methods makes it easier to eliminate incoming cyber threats and defend your franchise.

How much are you willing to risk?

This free resource is powered by WIRED, a full-service IT provider for franchises.

Connect with WIRED

Get your free quote today

info@wiredtelcom.com

315-326-0001

WIRED NATIONAL