Preventing data theft and payment fraud.

Here's a sobering statistic: 43% of all phishing attacks targeted small businesses, according to a 2015 report from Symantec.*

Phishing, which involves the use of email to trick employees into revealing business-related information—such as the login and password that accesses the company's network, is one of the most common ways that payment fraud happens. Still, it's just one type of threat that small businesses face. Malware, ransomware and denial-of-service, which has the potential to shut down your website, can all threaten your ability to operate.

IT security matters.

Why do small businesses so often find themselves under attack? The answer may be simple. What small businesses lack in terms of the volume of data in their possession, they make up for in terms of ease of access. Many business owners don't believe they have enough data to attract the attention of cybercriminals, therefore, they often overlook the importance of security in protecting their business from attack. That's a critical mistake. While cybercriminals prefer access to vast amounts of stolen data, with an active black market for it, they can still make money from the information taken from small companies.

*Symantec, Attackers Target Both Large and Small Businesses (2015).

Key takeaways

43% of all phishing attacks targeted small businesses.

Phishing is one of the most common ways payment fraud happens.

Many business owners overlook the importance of security.

There are five steps companies can take to help protect themselves.

Five ways to protect your business.

It's easy to become overwhelmed at the size and complexity of the threats your company faces. The following tips can help your business withstand the onslaught of attacks:

1. Figure out how much employee and customer data you really need.

Less data in your possession translates to less data for criminals to steal. Examine the types of employee and customer data you collect and whether it's necessary to retain it. If you maintain paper employee or customer records and decide to destroy them, make sure you do so using a confidential waste service that shreds the documents in their truck at your business.

2. Educate employees on their role in protecting the business.

By using a password that can be easily guessed, or opening a suspicious email attachment, employees often play a big role in facilitating data breaches. Take the time to explain how they can help protect the organization with robust passwords, etc. Also, limit administrative access to your computers for employees. By doing so, you'll limit their ability to install unapproved software, which can often provide cybercriminals with an entry point to your business.

3. Update software frequently.

In response to attacks, technology companies, such as Microsoft, often issue updates, or "patches," to their software. It's easy to avoid updating software, but make sure your business installs the update as soon as it's available. Cybercriminals often exploit known security issues months, sometimes years, after a patch exists.

4. Mandate the use of complex passwords.

Criminals can use a number of sophisticated tools to guess a user's password. However, that's not always needed because some users don't change their password from a default. Make sure employees use strong passwords that include uppercase and lowercase letters as well as numbers and characters. If in doubt regarding the strength of a password, Kaspersky provides a tool to test how long it would take to crack it.

5. Consider encrypting your data.

In layman's terms, encryption makes it impossible to read data unless in possession of the credentials, or key, to unlock it. Consequently, encrypted data in the hands of an unauthorized third party has no value. In addition to encryption, back up your data often in a separate, off-site location. In the event of an attack, you'll still have access to critical data.

While estimates vary widely regarding the costs associated with a breach, in the aftermath, small businesses will need help to determine how the breach took place, as well as help to prevent future breaches. With so much demand for cybersecurity professionals, such expertise is extremely expensive. Customers may leave and some employees may sue, prompting the need for legal counsel as well. Not to mention the stress and loss of productivity that a breach can cause. It's easy to see why preventing a breach is well worth the effort.

We can help you stay secure.

If you'd like help safeguarding your company against these potential threats, contact your Relationship Manager today.

KeyBank
Use the red key.®