

# 8 WAYS TO PREVENT A SECURITY OR DATA BREACH



business.com

---

# 8 Ways to Prevent a Security or Data Breach



Here are some security tips all small businesses should heed and implement to protect their customers — and business.

You may not think your small business is large enough to attract the attention of virtual thieves and cybercriminals, but any business that processes customer payment information is a potential victim of a security or data breach.

Here are some security tips all small businesses should heed and implement to protect their customers and business:

## **Address the basic security risks you can easily manage**

Most credit and debit cards issued to cardholders in the United States now include an EMV chip on the card's front and a magnetic strip on the back for choice in payment processing. EMV technology conceals sensitive account information during transaction processing with technology such as encryption and tokenization to render data meaningless for virtual thieves who may succeed in intercepting it. If you haven't invested in point-of-sale terminals that are EMV-enabled, or you have but still allow customers to choose if they want to

swipe or insert their EMV chip, you're exposing your business and its customers to the risk of a breach.

## **Educate the employees who operate your point-of-sale terminals**

Any employee who is involved in your payment processing should be aware of how their actions could expose your business to potential risk — or help prevent it. For example, a customer's credit card number should never be sent over unsecured email; mobile payments should be processed only when the device is connected to a private, password-protected Internet connection.

## **Rely on payment partners who can keep you protected**

The Payment Card Industry security standards outline the payment security best practices a business should follow based on the number of credit card or debit card transactions processed over the course of a 12-month period. While you are responsible for adhering to the security protocols outlined for your business, partnering with a payment processor that guarantees PCI compliance can improve the security of every customer transaction and, ultimately, protects your business from unnecessary risk.

## **Manage your risk based on the big picture**

Customer payment data is one major security concern any business that accepts customer credit and debit cards should actively protect, but the many other systems you use to facilitate and store your business's data — including email and cloud-based servers — can also provide easy entryways for virtual thieves if they're not properly secured, protected and monitored for potential vulnerabilities.

## **Backup files in more than one place**

There are many low-cost cloud storage providers that meet the needs of a small business. But if you don't understand all the details of your cloud provider's service agreement — including how the cloud provider protects the data you trust it to manage, who is authorized to access it, and what happens to your data if you end the agreement — you're putting your business at risk. Be selective about the cloud providers you consider, based on more factors than just price. Read service agreements carefully so that you understand what it entails and why; ask

questions about who will handle your data or have access to it.

Even when you do find a cloud provider you're comfortable with, back up the data you store in the cloud on a hard drive or USB drive as an additional security measure. Ideally, you'll also store it at a location separate from your physical business, just in case of a major disaster. This ensures you are not at the mercy of your cloud provider's security, which could also be compromised, and can protect you against ransomware. Consider it another line of defense, in addition to your other security protocols.

## **Be vigilant about the access you authorize**

You hire employees, vendors and third-party suppliers — and all of them may be given access to your sensitive business information to do their jobs. Manage what they can access to the best of your ability. If you allow employees to access business-related information on their phones or tablets, for example, issue company devices that empower you to maintain some level of control over the types of data employees can download and access (and from what kinds of online networks) rather than hoping that they'll abide by a BYOD policy that allows personal devices to be used for business.

## **Develop controls for passwords**

Multifactor authentication (MFA) can help you manage how far-reaching any cybercrime is able to extend; don't trust that employees will choose secure passwords on their own. Adjust your security settings so that every employee has to use MFA, and automate when passwords will expire and need to be changed.

## **Pay for security that is outside of your expertise**

It's wise to want to manage costs when you run a small business, but the average breach can cost a business more than \$20,000. Not sure your firewalls, networks or websites are secure from virtual thieves? Hire an IT expert who can test your systems and consult you on what is needed — before you're a victim.

Securing your business's sensitive data — along with the information it handles on behalf of customers — is a necessary function of doing business in our tech-based world. Educate yourself on the best practices to enhance your security, and hire experts who can help you navigate what you don't know. You

cannot prevent virtual thieves from targeting your business, but you can control what they're able to accomplish if they set their sights on it.

*Photo credit: Shutterstock*

---

A man with a beard and short brown hair, wearing a light blue button-down shirt, is smiling and looking down at a device in his hands. The background is a blurred office setting with vertical lines.

# Purch is driving the future of content and commerce

## **We Are Purch**

Purch is a rapidly growing, constantly evolving digital content and services company that helps millions of people make smarter purchases. We bring together 350 employees from around the globe who share a commitment to serve our customers with integrity, collaborate to deliver better results, and shape the future of digital publishing.

To view more content like this, visit [www.business.com](http://www.business.com)

To learn more about Purch, visit [www.purch.com/about](http://www.purch.com/about)