lightspeed

A Primer on POS Security:

6 Smart Ways to Protect Retailer and Customer Data

Introduction

If you're reading this, you're likely concerned about retail security. Perhaps you're looking for ways to protect your business after hearing about the major data breaches in the industry. Or maybe you're already taking steps to safeguard your business, but you want to know if there's anything else you need to do.

Whatever the case, this resource can help. In the following pages, we'll shed light on the ways you can protect your business from hackers and fraudsters. By the end of this guide, you'll have a solid understanding of retail security, and you'll walk away with action steps you can immediately implement in your business.

Let's get started.

In this guide

01 Beef up physical security.

Failing to secure your POS and credit card terminals may lead to equipment tampering, which in turn could leave you vulnerable to breaches. Follow these tips to protect your data:

- ✓ **Closely monitor payment equipment.** Regularly inspect your POS equipment, credit card terminals, and PIN-entry devices for any signs of tampering. Such signs may include broken seals, missing screws, extraneous wiring, or additional labels that might hide signs that the device has been altered.

  You should also check each device's USB or network port. If you see anything plugged into them that isn't supposed to be there, report it immediately.

- ✓ **Keep a record of the serial and model numbers of your devices.** Take note of all the serial and model numbers of your POS equipment. During your routine inspections, verify that numbers match their assigned devices.

- ✓ **Only use devices that are compliant with the latest security standards.** See to it that the devices you use are approved by the Payment Card Industry Security Standard Council (PCI SSC). Visit the official website of PCI SSC to view a list of approved devices.

- ✓ **Keep the checkout area secure.** Keep important information away from prying eyes by ensuring that your POS, card terminals, and screens are positioned for maximum privacy.

  Make use of secure shelves, stands, and security cables to prevent unauthorized removal. Mount your PIN pads securely on the counter, and utilize locking stands to further protect your equipment.

- ✓ **Invest in surveillance.** Consider installing surveillance cameras in your stores. Doing so will allow you to monitor store activities 24-7 and will give you recordings you can revisit if necessary.

02 Secure your store network.

You've worked hard to safeguard your hardware and software; now it's time to ensure your store's network is also protected. Here's how to do it:

- ✓ **Run your POS system on a separate network.** Keep POS activity secure by running it on a network that's separate from guest Wi-Fi. You also want to make sure you encrypt network data so traffic and activities aren't visible to anyone else.

  Remember that not all encryption standards are created equal. When encrypting your network, opt for Wi-Fi Protected Access version 2 (WPA2) encryption, which is the newest and most secure standard in the industry.

  Compared to encryptions like WPA and WEP, WPA2 makes you less vulnerable to attacks because it adds Advanced Encryption Standard (AES) which can strengthen your encryption.

- ✓ **Choose a nondescript network name.** When naming your networks, avoid using something that would easily identify your store (e.g. "Julie's Dress Shop"). It's best to stick to something nondescript such as "network" – or better yet, to use a series of seemingly random letters and numbers.

- ✓ **Audit your network regularly.** Have your network audited on a regular basis to prevent remote access. A network audit may involve actions like scanning your network for weaknesses and ensuring hardware and software compliance.

03 Keep your software and apps in check.

Applications and software can certainly help you run your business better, but if they're not managed properly, they can make you vulnerable to data breaches and hacks. Here are some steps you can take to avoid that:

- ✓ **Keep your programs updated.** Don't ignore date prompts you get from your apps. The newest version of an app or solution contains the most updated features and security measures, so it's less vulnerable to hacks and breaches.
- ✓ **Uninstall programs or plugins you're no longer using.** All programs have vulnerabilities, so fewer apps means less risk of attacks. Go through all the programs installed on your computer and mobile devices, and remove the ones you're no longer using.
- ✓ **Use an antivirus, and keep it updated.** Keep your devices safe from viruses, worms, and malware by installing an antivirus program. Don't forget to update your antivirus on a daily basis to ensure you have the latest protection at all times.
- ✓ **Implement application control.** To further safeguard your devices, consider using application control to block or restrict unauthorized programs from running.


VAULT
lightspeed

04 Create strong passwords

Keep your accounts, POS, and other devices secure with strong passwords. Below are some pointers to help you do just that:

- ✓ **Never use default passwords.** Immediately change the default passwords on your computer, POS, Wi-Fi, and other accounts or devices. This will help keep everything safe from unauthorized use.

- ✓ **Come up with strong passwords – or better yet, use passphrases.** If you want to make a password more secure, turn it into a passphrase. Longer passwords are harder to crack, so rather than just using one word or set of characters, create something composed of multiple words.

  The best route is to go for long, unique passphrases you can easily remember. For example, if you drive a 2015 Toyota Corolla, your passphrase could be "ILoveMy2015Corolla."

- ✓ **Don't use the same password for multiple accounts.** If someone gets their hands on your password for one website or account, the last thing you want is for them to access your other accounts. That's why it's incredibly important to use a unique password for each website or app.

- ✓ **Consider using a password manager.** Keeping track of unique passphrases can be difficult, which is why you should consider getting a password manager. These applications can create, manage, and safeguard your passwords for you. All you need to do is remember one "master" password (or passphrase) so you can access the service.

- ✓ **Use multi-factor authentication (MFA).** An increasing number of websites and solutions providers are offering multi-factor authentication systems. MFA means the user goes through multiple authentication methods upon login. For instance, in addition to signing in with your username and password, the system will further authenticate you by asking you to enter a code sent to your mobile device.

  MFA adds an extra layer of security to your accounts, and it's highly recommended that you enable it whenever possible.

05 Safeguard customer data.

It's not enough to secure your own data. As a retailer, you should go to great lengths to protect customer information. Follow these pointers to safeguard your customers' data:

- ✓ **Avoid collecting and storing customer data.** The best way to prevent thieves from stealing data is to not give them anything to steal in the first place. So before collecting any type of customer information, ask yourself: do you need it? If the answer is no, don't collect it.

  And if you do obtain information from your customers, don't store it for longer than necessary. Delete their information if and when you don't need it anymore.

  You may also have to follow legal and regulatory requirements to protect personally identifiable information (i.e. that which a retailer would collect). Before handling shopper information, check the consumer protection laws in your area, particularly when it comes to obtaining consent and using consumer information, as well as disclosure, storage, and retention.

- ✓ **Adopt EMV.** EMV can protect you and your customers from credit card fraud, so if you haven't transitioned to this payment standard just yet, it's high time to do so.

  For the uninitiated, EMV was developed by Europay®, Mastercard®, and Visa® (hence the name) as a way to combat fraud. It's a technology that powers chip-and-pin cards, a breed of debit and credit cards that's far more secure than magnetic stripe (i.e. swipe-and-sign) cards.

  Unlike a mag stripe card (which stores static information about the cardholder), an EMV card is embedded with a chip, which creates a unique code that changes for every transaction. This makes it less susceptible to fraud – because even if a hacker manages to counterfeit a chip card, the original transaction code is no longer usable, and the card will be declined.

- ✓ **Ensure PCI compliance.** PCI standards apply to companies that accept, process, store, or transmit payment card information.

  In other words, companies that need to comply with PCI standards are those that handle cardholder information. In a typical retail environment, payment terminal providers deal with cardholder data, which means they're the ones that avvneed to be PCI-compliant.

  What does this mean for you? If you don't deal with payment card data directly, you need to make sure the companies you assign to handle cardholder data are PCI-compliant.

  Again, you can learn more about the devices and practices approved by PCI SSC by visiting their website.

06 Ensure your staff upholds your security standards.

Your employees play an important part in upholding retail security, so see to it that they're knowledgeable and well-trained in keeping your store secure. Here are a few tips:

- ✓ **Screen employees.** In addition to the usual application and interview process, conduct background checks on potential hires – especially if they're going to handle sensitive information.

- ✓ **Conduct security training.** Once you have employees on board, formally train them on your store's security practices and policies. Educate them on how to secure your POS, as well as on how to spot equipment tampering.

  Additionally, make sure they know how to stay safe when using different programs and browsing the internet. Your staff should know about the importance of app updates, password security, and multi-factor authentication. To be safe, restrict your staff from using applications on the devices where your POS system is installed.

  You should also educate them on phishing, which is the use of legitimate-looking emails and websites to trick users into providing information such as passwords, account numbers, and payment card information.

  Phishing is one of the most common ways to compromise an organization, so it's important to educate employees on how to spot phishing attempts. Train them to be vigilant when opening their emails, and highlight the importance of not readily providing personal information and passwords to other parties – even if they recognize the email address or website asking for their details.

  Finally, emphasize the importance of securing your customers' information. Make sure your employees know that customer data protection is paramount and that they follow your policies on customer data use, disclosure, accuracy, storage, and retention.

✓ **Assign a unique user ID to each employee.** If you have multiple employees (i.e. several associates and managers), create separate IDs and login information for each person to get into your POS and other programs. Don't allow any two associates to use the same login information.

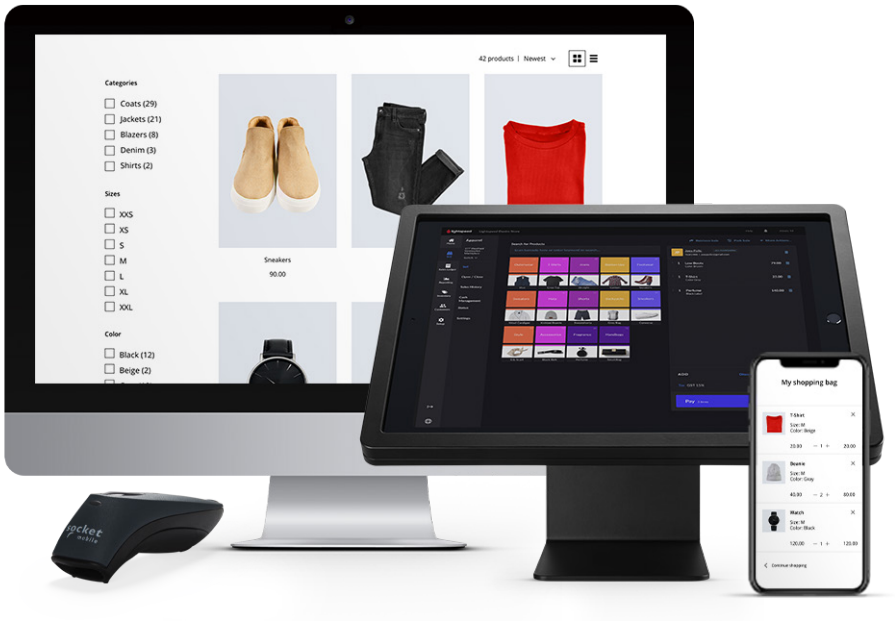
Doing so will help you monitor who's doing what in your store. It will also make investigations much easier should any incidents arise.

Final words

Taking steps like securing your network and strengthening your passwords are incredibly important – but doing them once won't be enough to protect you for the long-term.

Data security isn't something you can just "set and forget." Technologies and standards are constantly evolving, and there's always a new threat to security. The best way to stay secure is to constantly keep an eye on your business and the industry to ensure your security measures are up to snuff.

It's also important to remember that you're not operating your business in a vacuum. Protecting yourself and your customers entails working with security professionals, vendors, and even consumers, and seeing to it that everyone is doing his or her part to stay secure.



About Lightspeed

Powering the businesses that are the **backbone of the global economy**, Lightspeed's **one-stop commerce platform** helps merchants innovate to **simplify, scale** and **provide exceptional customer experiences**. The cloud solution **transforms and unifies online and physical operations**, multichannel sales, expansion to new locations, global payments, financing and connection to supplier networks.

Founded in Montréal, Canada in 2005, Lightspeed is dual-listed on the New York Stock Exchange and Toronto Stock Exchange (NYSE: LSPD) (TSX: LSPD). With teams across North America, Europe and Asia Pacific, the company serves retail, hospitality and golf businesses in over 100 countries.

For more information, please visit: lightspeedhq.com
On social media: LinkedIn, Facebook, Instagram, YouTube, and Twitter

Want more retail pro tips?

Find free tools, insights and expert advice in our resource center.

More retail resources