

PAYMENT PROTECTION RESOURCES FOR SMALL MERCHANTS

Guide to Safe Payments

Version 1.0 | July 2016



UNDERSTANDING YOUR RISK	4
PROTECT YOUR BUSINESS WITH THESE SECURITY BASICS	7
WHERE TO GET HELP	20



UNDERSTANDING YOUR RISK

Understanding your risk

As a small business, you are a prime target for data thieves.

When your payment card data is breached, the fallout can strike quickly. Your customers lose trust in your ability to protect their personal information. They take their business elsewhere. There are potential financial penalties and damages from lawsuits, and your business may lose the ability to accept payment cards. A survey of 1,015 small and medium businesses found 60% of those breached close in six months. (NCSA)

60%

OF SMALL BUSINESSES EXPERIENCED A CYBER BREACH. (HM Government)



71%

OF HACKERS ATTACK BUSINESSES WITH UNDER 100 EMPLOYEES (Verizon 2012)

\$20,752



AVERAGE COST TO A SMALL BUSINESS DUE TO HACKING, UP FROM \$8,600 IN 2013 (NSBA)

69%



OF AMERICAN CONSUMERS WORRY ABOUT THEFT OF THEIR PAYMENT CARD DATA (Gallup)

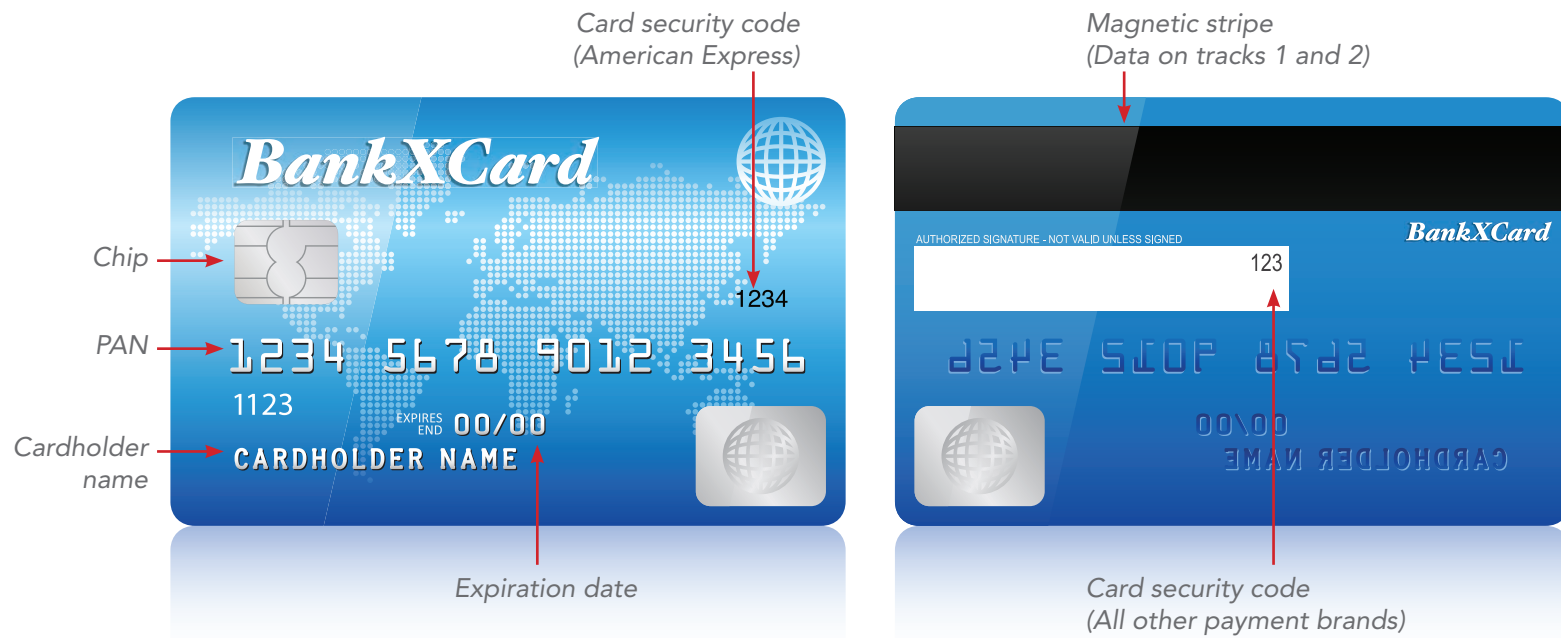
What's at risk?

YOUR CUSTOMERS' CARD DATA IS A GOLD MINE FOR CRIMINALS. DON'T LET THIS HAPPEN TO YOU!

Follow the actions in this guide to protect against data theft.

Examples of payment card data are the primary account number (PAN) and three or four-digit card security code. The red arrows below point to types of data that require protection.

TYPES OF DATA ON A PAYMENT CARD



WHAT IS PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security requirements that can help small merchants to protect customer card data located on payment cards.

Small merchants may be familiar with validating their PCI DSS compliance via a Self-Assessment Questionnaire (SAQ).

For more information on PCI DSS, see the Resources at the end of this guide.

Understanding your payment system: Common payment terms

Depending on where in the world you are located, equipment used to take payments is called by different names. Here are the types we reference in this document and what they are commonly called.



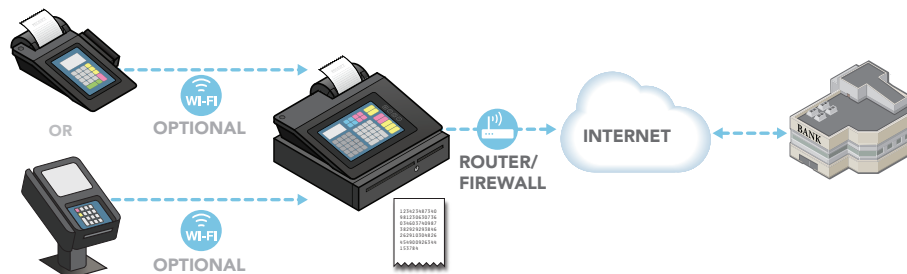
A **PAYMENT TERMINAL** is the device used to take customer card payments via swipe, dip, insert, tap, or manual entry of the card number. Point-of-sale (or POS) terminal, credit card machine, PDQ terminal, or EMV/chip-enabled terminal are also names used to describe these devices.



An **ELECTRONIC CASH REGISTER** (or till) registers and calculates transactions, and may print out receipts, but it does not accept customer card payments.



An **INTEGRATED PAYMENT TERMINAL** is a payment terminal and electronic cash register in one, meaning it takes card payments, registers and calculates transactions, and prints receipts.



A **PAYMENT SYSTEM** encompasses the entire process for accepting card payments in a retail location (including stores/shops and e-commerce storefronts), and may include a payment terminal, an electronic cash register, other devices or systems connected to a payment terminal (for example, Wi-Fi for connectivity or a PC used for inventory), servers with e-commerce components such as payment pages, and the connections out to the merchant bank.



A **MERCHANT BANK** is a bank or financial institution that processes credit and/or debit card payments on behalf of merchants. Acquirer, acquiring bank, and card or payment processor are also terms for this entity.

How is your business at risk?

The more features your payment system has, the more complex it is to secure. These extra features often provide easy ways for criminals to steal your customer card data. Think carefully about whether you really need these extra features (for example, Wi-Fi or cameras) for your business.

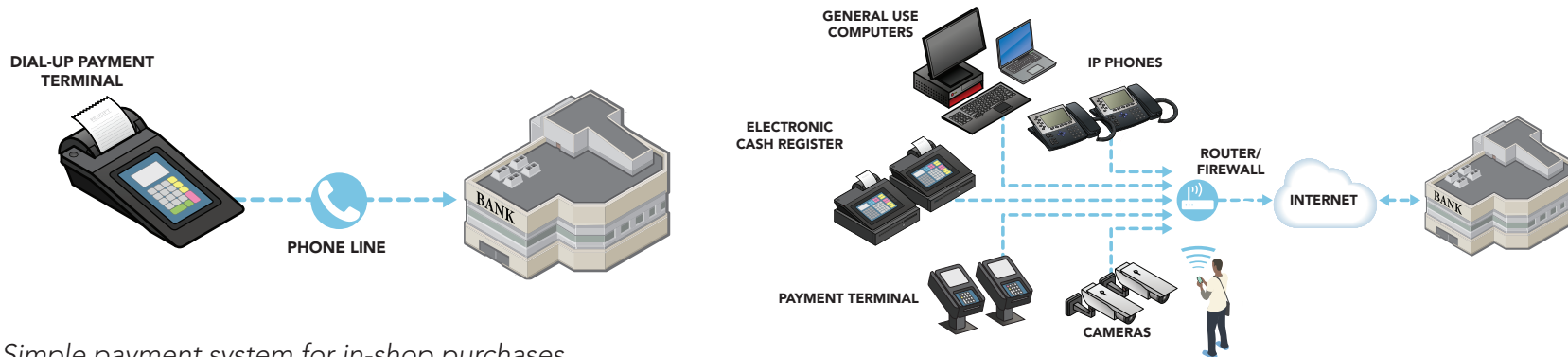


How do you sell your goods or services? There are three main ways:

- 1. A person walks into your shop and makes a purchase with their card.*
- 2. A person visits your website and pays online.*
- 3. A person calls your shop and provides card details over the phone, or sends the details in the mail or via fax.*

Understanding your risk: Payment system types

Your security risks vary greatly depending on the complexity of your payment system, whether face-to-face or online.



Simple payment system for in-shop purchases

Complex payment system for in-shop purchases, with Wi-Fi, cameras, Internet phones, and other attached systems



Complex e-commerce payment system for online shop purchases, with merchant managing their own website and payment page

















































Use the [Common Payment Systems](#) to help you identify what type of payment system you use, your risk, and the recommended security tips as a starting point for conversations with your merchant bank and vendor partners.



PROTECT YOUR BUSINESS WITH THESE SECURITY BASICS

How do you protect your business?

The good news is, you can start protecting your business today with these security basics:

How to Safeguard your Business Against Breaches	Cost	Ease	Risk Mitigation
 Use strong passwords and change default ones			
 Protect your card data and only store what you need			
 Inspect payment terminals for tampering			
 Install patches from your vendors			
 Use trusted business partners and know how to contact them			
 Protect in-house access to your card data			
 Don't give hackers easy access to your systems			
 Use anti-virus software			
 Scan for vulnerabilities and fix issues			
 Use secure payment terminals and solutions			
 Protect your business from the Internet			
 For the best protection, make your data useless to criminals			

These security basics are organized from easiest and least cost to implement to those that are more complex and costly to implement. The amount of risk reduction that each provides to small merchants is also indicated in the "Risk Mitigation" column.



Use strong passwords and change default ones

Cost



Ease



Risk Mitigation



Your passwords are vital for computer and card data security. Just like a lock on your door protects physical property, a password helps protect your business data. Also be aware that computer equipment and software out of the box (including your payment terminal) often come with default (preset) passwords such as "password" or "admin," which are commonly known by hackers and are a frequent source of small merchant breaches.

About

80%

of data breaches involve guessed or stolen passwords

Verizon PCI 2015

CHANGE YOUR PASSWORDS REGULARLY. Treat your passwords like a toothbrush. Don't let anyone else use them and get new ones every three months.

SEEK HELP. Ask your vendors or service providers about default passwords and how to change them. Then do it!

MAKE THEM HARD TO GUESS. The most common passwords are "password" and "123456." Hackers try easily-guessed passwords because they're used by half of all people. A strong password has seven or more characters and a combination of upper and lower case letters, numbers, and symbols (like !@#\$%). A phrase can also be a strong password (and may be easier to remember), like "B1gMac&frieS."

DON'T SHARE. Insist on each employee having their own login IDs and passwords – never share!

Typical default passwords that **MUST BE** changed:

[none]

[name of product/
vendor]

1234 or 4321

access

admin

anonymous

database

guest

manager

pass

password

root

sa

secret

sysadmin

user

For more about password security, see these resources on the PCI Council website:

INFOGRAPHIC



It's Time to Change Your Password

VIDEO



Learn Password Security in 2 Minutes



Protect card data and only store what you need

Cost



Ease



Risk Mitigation



It's impossible to protect card data if you don't know where it is.

What can you do?

Tokenization has a similar goal to encryption but works differently. It substitutes card data with meaningless data (a "token") that has no value to a hacker.

ASK AN EXPERT. Ask your payment terminal vendor or merchant bank where your systems store data and if you can simplify how you process payments. Also ask how to conduct specific transactions (for example, for recurring payments) without storing the card's security code.

OUTSOURCE. The best way to protect against data breaches is not to store card data at all. Consider outsourcing your card processing to a PCI DSS compliant service provider. See Resources on page 22 for lists of compliant service providers.

IF YOU DON'T NEED CARD DATA, DON'T STORE IT. Securely destroy/shred card data you don't need. If you need to keep paper with sensitive card data, mark through the data with a thick, black marker until it is unreadable and secure the paper in a locked drawer or safe that only a few people have access to.

LIMIT RISK. Rather than accepting payment details via email, ask customers to provide it via phone, fax, or regular mail.

TOKENIZE OR ENCRYPT. Ask your merchant bank if you REALLY need to store that card data. If you do, ask your merchant bank or service provider about encryption or tokenization technologies that make card data useless even if stolen. (See "🔒" on page 19 for more info).

ENCRYPTION PRIMER

Cryptography uses a mathematical formula to render plaintext unreadable to people without special knowledge (called a key). Cryptography is applied to stored data as well as data transmitted over a network.

ENCRYPTION
changes plaintext into cyphertext.

DECRYPTION
changes cyphertext back into plaintext.

For example:

This is secret stuff,
do not

ENCRYPTION KEY

5a0 (k\$hQ%...

DECRYPTION KEY

This is secret stuff,
do not



Inspect payment terminals for tampering

Cost	
Ease	
Risk Mitigation	

“Skimming devices” sweep up your customers’ card data as it enters a payment terminal. It’s vital that you and your staff know how to spot a skimming device. You need to regularly check your payment terminals to make sure they have not been tampered with. Keep a record or log of which terminals were checked, when, who did the check, and whether anything was found.

See the [PCI Council’s guide: Skimming Prevention – Overview of Best Practices for Merchants](#)

Be vigilant and follow these steps:

KEEP A LIST of all payment terminals and take pictures (front, back, cords, and connections) so you know what they are supposed to look like.

LOOK FOR OBVIOUS SIGNS of tampering, such as broken seals over access cover plates or screws, odd/different cabling, or new devices or features you don’t recognize. The Council’s guide (referenceed below) can help.

PROTECT TERMINALS. Keep them out of customers’ reach when not in use and obscure their screens from public view. Make sure your payment terminals are secure before you close your shop for the day, including any devices that read your customers’ payment cards or accept their personal identification numbers (PINs).

CONTROL REPAIRS. Only allow payment terminal repairs from authorized repair personnel, and only if you are expecting them. Tell your staff too.

CALL your payment terminal vendor or merchant bank immediately if you suspect anything!



Install patches from your vendors

Cost



Ease



Risk Mitigation



Often, software has flaws or mistakes made by programmers when they wrote the code, also called security holes, bugs or vulnerabilities. Hackers exploit these mistakes to break into your computer and steal account data. Protect your systems by applying vendor-supplied “patches” to fix coding errors. Timely installation of security patches is crucial!

ASK your vendor or service provider how it notifies you of new security patches, and make sure you receive and read these notices.

WHICH VENDORS SEND YOU PATCHES? You may get patches from vendors of your payment terminal, payment applications, other payment systems (tills, cash registers, PCs, etc.), operating systems (Android, Windows, iOS, etc.), application software (including your web browser), and business software.

MAKE SURE your vendors update your payment terminals, operating systems, etc. so they can support the latest security patches. Ask them.

E-COMMERCE MERCHANTS. Installing patches as soon as possible is very important for you too. Also look out for patches from your payment service provider. Ask your e-commerce hosting provider whether they patch your system (and how often). Make sure they update the operating system, e-commerce platform and/or web application so it can support the latest patches.

FOLLOW your vendor’s/service provider’s instructions and install those patches as soon as possible.



Use trusted business partners and know how to contact them

Cost



Ease



Risk Mitigation



You use outside providers for payment-related services, devices and applications. You may also have service providers that you share card data with, that support or manage your payment systems, or that you give access to card data. You may call them processors, vendors, third parties, or service providers. All of these impact your ability to protect your card data, so it's critical you know who they are and what security questions to ask them.

KNOW WHO TO CALL. Who is your merchant bank? Who else helps you process payments? Who did you buy your payment device/software from and who installed it for you? Who are your service providers?

KEEP A LIST. Now that you know who to call, keep company and contact names, phone numbers, website addresses, and other contact details where you can easily find them in an emergency.

CONFIRM THE SECURITY OF YOUR SERVICE PROVIDERS. Is your service provider adhering to PCI DSS requirements? For e-commerce merchants, it is important that your payment service provider is PCI DSS compliant too! See Resources on page 22 for lists of compliant service providers.

ASK QUESTIONS. Once you know who your outside providers are and what they do for you, talk to them to understand how they protect card data. Use [Questions to ask your Vendors](#) to help you know what to ask.

UNDERSTAND COMMON VENDORS. Review the sidebar to the right to understand common types of vendors or service providers you may work with.

COMMON VENDORS

Refer to the table in the [Questions to ask your Vendors](#) for more details about these common vendors:

Payment terminal vendors

Payment application vendors

Payment system installers (called Integrators/Resellers)

Service providers that perform payment processing, or e-commerce hosting or processing

Service providers that help you meet PCI DSS requirement(s) (for example, providing firewall or antivirus services)

Providers of Software as a Service



Protect in-house access to your data

Cost



Ease



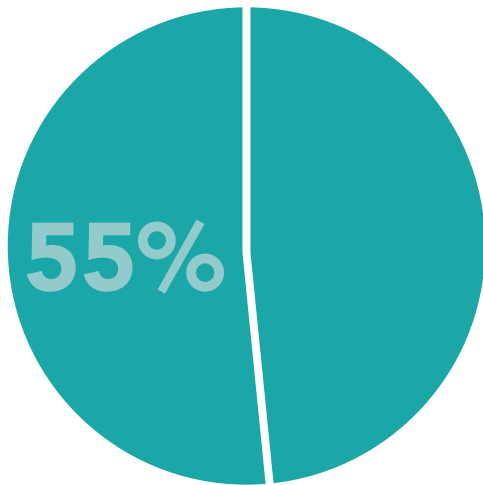
Risk Mitigation



Privilege abuse means a person using...

Someone else's access and privileges to gain access to systems or data that person is not authorized to have access to.

PRIVILEGE ABUSE IS THE TOP ACTION LEADING TO BREACHES – ABOUT 55% OF ALL INCIDENTS REPORTED.



Verizon 2015

ACCESS CONTROL IS ALL IMPORTANT. Set up your system to grant access only based on a "business need-to-know." As the owner, you have access to everything. But most employees can do their job with access only to a subset of data, applications, and functions.

LIMIT ACCESS to payment systems and unencrypted card data to only those employees that need access, and only to the data, applications and functions they need to do their jobs.

KEEP A LOG. Track all "behind the counter" visitors in your establishment. Include name, reason for visit, and name of employee that authorized visitor's access. Keep the log for at least a year.

SECURELY DISPOSE OF DEVICES. Ask your payment system vendor or service provider how to securely remove card data before selling or disposing of payment devices (so data cannot be recovered).

SHARE THIS INFORMATION. Give this guide to your employees and business partners so they know what is expected.

Consider giving employees access to take payments but not to process refunds, or to take new bookings/orders but not to access payment card data related to existing booking/orders. Some employees should have no access at all.



Don't give hackers easy access to your systems

Cost



Ease



Risk Mitigation



HACKERS = CRIMINALS

One of the easiest ways for hackers to get into your system is through people you trust. You need to know how your vendors are accessing your system to make sure it's not opening up any holes for hackers.

Multi-factor authentication uses a username and password plus at least one other factor (like a smart card, dongle, or one-time passcode).*

*a handy device that connects to a computer to allow access to wireless, software features, etc.

FIND OUT. Ask your payment system vendor or service provider if they use remote access to support or access your business.

ASK HOW TO LIMIT USE OF REMOTE ACCESS.

Many remote access programs are always on by default. Reduce your risk – ask your vendor how to disable remote access when not needed, and how to enable it when your vendor or service provider specifically requests it.

DISABLE IT WHEN DONE.

USE STRONG AUTHENTICATION. If you must allow remote access, require multi-factor authentication and strong cryptography.

ENSURE SERVICE PROVIDERS USE UNIQUE CREDENTIALS.

Each one must use remote access credentials that are unique to your business and that are not the same ones used for other customers.

ASK FOR HELP. Ask your vendor or service provider for help disabling remote access, or (if your vendor or service provider needs remote access) for help setting up multi-factor authentication. See [Questions to ask your Vendors](#) to help you know exactly what to ask them.

If your vendor supports or troubleshoots your payment terminal from their office (and not from your location) they are using the Internet and remote access software to do this.

Examples of products your vendor may install on your terminal and use to support you remotely include VNC & LogMeIn.



Use anti-virus software

Cost	
Ease	
Risk Mitigation	

Systems and software are extremely flexible and offer a wide range of functions and features. Hackers write viruses and other malicious code to exploit those features and coding mistakes, so they can break into your systems and steal card data. Using up-to-date anti-virus (also called anti-malware) software helps to protect your systems.

INSTALL ANTI-VIRUS SOFTWARE TO PROTECT YOUR PAYMENT SYSTEM. It is easy to install and can be obtained from your local office supply shop or IT retailer.

SET THE SOFTWARE TO "AUTOMATIC UPDATE" so you always get the most recent protection available.

GET ADVICE. Ask your IT retailer about products they recommend for anti-virus/anti-malware protection.

RUN PERIODIC SCANS. Regularly run full system scans, since your systems may have been infected by new malware that was released before your anti-virus software was able to detect it.



Scan for vulnerabilities and fix issues

Cost	
Ease	
Risk Mitigation	

New vulnerabilities, security holes, and bugs are being discovered daily. It's vital to have your Internet-facing systems tested regularly to identify these new risks and address them as soon as possible. Your Internet-facing systems (like many payment systems) are the most vulnerable because they can be easily exploited by criminals, allowing them to sneak into your systems.

The PCI Council's Approved Scanning Vendors (ASVs) perform external vulnerability scanning and reporting. See PCI's [List of PCI-Approved Scanning Vendors](#)

GET ADVICE. Ask your merchant bank if they have partnerships with any PCI Approved Scanning Vendors (ASVs). Ask your vendors and service providers too.

TALK TO A PCI ASV. These vendors can help you with tools that automatically search your network to find vulnerabilities and provide you with a report if, for example, you need to apply a patch. The PCI Council's list (referenced below) can help you find a scanning vendor.

SELECT A SCANNER. Contact several PCI ASVs to find one with a program suitable for your small business.

ADDRESS VULNERABILITIES. Ask your ASV for help correcting issues found by scanning.



Use secure payment terminals and solutions

Cost	
Ease	
Risk Mitigation	

A sure way to better protect your business is to use secure payment solutions and trained professionals to help you. Here's how to choose safe products and make sure they are set up securely.

For PCI payment terminals and secure card readers that encrypt card data, see  on page 19.

USE SECURE PAYMENT TERMINALS AND PIN ENTRY DEVICES.

The PCI Council approves payment terminals that protect PIN data. Make sure your payment terminal or device is on the [List of PCI Approved PTS Devices](#) for equipment that provides the best security, and supports "EMV chip."

USE SECURE SOFTWARE. Make sure your payment software is on the [List of PCI Validated Payment Applications](#).

USE QUALIFIED PROFESSIONALS. Make sure the person installing your PA-DSS validated application does it correctly and securely. Choose from the [List of PCI QIRs](#) for companies qualified by the PCI Council to help you. Ask your merchant bank to help you make the selection.

REFER TO THIS LIST OF VENDOR QUESTIONS.

Use [Questions to ask your Vendors](#) to help you know what to ask your vendors and service providers.

Your customers enter their personal identification numbers (PINs) for their payment cards into your payment terminal or PIN entry device. It is important to use secure devices to protect your customers' PIN data.



Protect your business from the Internet

Cost



Ease



Risk Mitigation



The Internet is the main highway used by data thieves to attack and steal your customers' card data. For this reason, if your business is on the Internet, anything you use for card payments needs extra protection.

ISOLATE USAGE. Don't use the device you take payments with for anything else. For example, don't surf the web or check emails or social media from the same device or computer that you use for payment transactions. When necessary for business (for example, updating your business's social media page), use another computer and not your payment device for these updates.

PROTECT YOUR "VIRTUAL TERMINAL." If you enter customer payments via a virtual terminal (a web page you access with a computer or a tablet), minimize your risk - don't attach an external card reader to it.

PROTECT WI-FI. If your shop offers free Wi-Fi for your customers, make sure you use another network for your payment system (this is called "network segmentation"). Ask your network installer for help with safely configuring Wi-Fi.

USE A FIREWALL. A properly configured firewall acts as a buffer to keep hackers and malicious software from getting access to your computers and information. Check with your payment terminal vendor or service provider to make sure you have one and ask them for help configuring it correctly.

USE PERSONAL FIREWALL SOFTWARE OR EQUIVALENT when payment systems are not protected by your business firewall (for example, when connected to public Wi-Fi).



For the best protection, make your data useless to criminals

Cost



Ease




Risk Mitigation



Your data is vulnerable when it travels to your merchant bank, and when it's kept or stored on your computers and devices. The best way to keep it safe is to make it useless even if it's stolen by hiding it, and removing it altogether when it's not needed. While this can be more complex to put in place, in the long run, it can make security much easier to manage.

ASK YOUR PAYMENT SYSTEMS VENDOR OR SERVICE PROVIDER whether your payment terminal is using encryption and /or tokenization technology.

USE PCI DEVICES THAT ENCRYPT CARD DATA.

The PCI Council approves payment terminals that protect PIN data (see  on page 17) and payment terminals and "secure card readers" that additionally encrypt card data. See the [List of PCI Approved PTS Devices](#).

USE SECURE PCI ENCRYPTION SOLUTIONS. Ask whether your payment terminal encryption is done via a Point-to-Point Encryption solution and is on the PCI Council's [List of PCI P2PE Validated Solutions](#).

UPGRADE YOUR SOLUTION. Reduce your risk – consider getting a new payment terminal that uses both encryption and tokenization technology to remove the value of card data for hackers.

ARE YOU A MERCHANT NOW MOVING TO EMV CHIP TERMINALS? This is a great opportunity to make an investment in a terminal that supports EMV and also provides the added security of encryption and tokenization.

ASK. See [Questions to ask your Vendors](#) for help with questions to ask your vendor or service provider.

PCI approved secure card readers and payment terminals that encrypt card data do it using technology called "Secure Reading and Exchange of Data (SRED)" - ask your vendor if your payment terminal encrypts card data with SRED.

An illustration of three stylized human figures in business suits, standing side-by-side within a large, dark teal circle. The figures are rendered in a lighter teal color. The background of the entire slide is a solid teal color.

WHERE TO GET HELP

Resources

PCI Council Listings

Resource	Link	URL
List of Validated Payment Applications	<i>PCI Council's Validated Payment Applications</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/vpa_agreement
List of Approved PTS Devices	<i>PCI Council's Approved PTS Devices</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices
List of Approved Scanning Vendors	<i>PCI Council's Approved Scanning Vendors</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
List of Qualified Integrators / Resellers	<i>PCI Council's Qualified Integrators Resellers</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_integrators_and_resellers
List of P2PE Validated Solutions	<i>PCI Council's P2PE Validated Solutions</i>	https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

Payment Brand Lists

Resource	Link	URL
Lists of Compliant Service Providers	<i>MasterCard's List of Compliant Service Providers</i>	https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html
	<i>Visa's Global Registry of Service Providers</i>	http://www.visa.com/splisting/
	<i>Visa Europe's Registered Member Agents</i>	https://www.visaeurope.com/receiving-payments/security/downloads-and-resources

PCI DSS and Related Guidance

Resource	Link	URL
More about PCI DSS	<i>How to Secure with PCI DSS</i>	https://www.pcisecuritystandards.org/pci_security/how
PCI DSS Self-Assessment Questionnaires	<i>Self-Assessment Questionnaires</i>	https://www.pcisecuritystandards.org/pci_security/completing_self_assessment
Guide: Skimming Prevention: Overview of Best Practices for Merchants	<i>Skimming Prevention: Overview of Best Practices for Merchants</i>	https://www.pcisecuritystandards.org/documents/Skimming_Prevention_At-a-Glance_Sept2014.pdf

Resources

Infographics and Videos

Resource	Link	URL
Infographic: It's Time to Change Your Password	<i>It's Time to Change Your Password</i>	https://www.pcisecuritystandards.org/pdfs/its_time_to_change_your_password_infographic.pdf
Infographic: Fight Cybercrime by Making Stolen Data Worthless to Thieves	<i>Fight Cybercrime by Making Stolen Data Worthless to Thieves</i>	https://www.pcisecuritystandards.org/documents/PCI-CyberCrime-FinalR.pdf
Video: Learn Password Security in 2 Minutes	<i>Learn Password Security in 2 Minutes</i>	https://www.youtube.com/watch?v=FsrOXgZKa7U

PCI Payment Protection Resources for Small Merchants

Resource	Link	URL
Common Payment Systems	<i>Common Payment Systems</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Small Merchant Questions for Vendors	<i>Small Merchant Questions for Vendors</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Questions_To_Ask_Your_Vendors.pdf
Small Merchant Glossary	<i>Small Merchant Glossary</i>	https://www.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

Sources

Gallup – *Gallup Poll*, October 2015

HM Government - *Small Businesses: What You Need to Know about Cyber Security*, UK 2014

NCSA – *National Cyber Security Alliance survey*, 2012

NSBA – National Small Business Administration, *2014 Year End Economic Report*

Verizon 2012 – *Verizon 2012 Data Breach Investigations Report*

Verizon 2015 – *Verizon 2015 Data Breach Investigations Report*

Verizon PCI 2015 – *Verizon 2015 PCI Compliance Report*