BANK OF AMERICA

# Merchant Guide to Safe Payments and PCI Compliance

# Table of contents

# What’s the risk for merchants?

## Smaller merchants are major targets for data thieves.

Hackers are mainly interested in payment card data because they can sell card numbers to fraudsters. Small businesses are generally easier to target because they have weaker security. Many hackers use automated bot armies to search for weak or unlocked systems and steal information.

## Data breaches can be very expensive because of:

- Fines and fees from card brands
- The cost of a PCI forensics investigation
- Costs to update or upgrade systems and security monitoring

## Other costs can include:

- Loss of business due to reputational harm — all U.S. states, the District of Columbia and most U.S. territories require merchants to report data breaches
- Customer lawsuits

63% of SMBs report experiencing a data breach in the previous 12 months.[1]

59% of customers don’t believe that companies have their best interests in mind.[2]

The middle 80% of breaches cost between $2,038 and $194,035.[3]

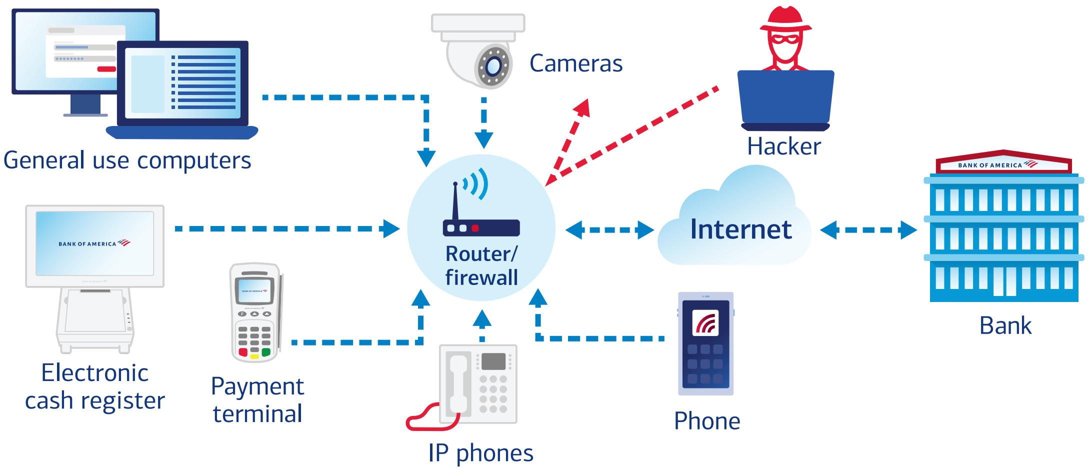
# What are the risks and benefits of different payment systems?

The risk of a data breach greatly depends on the complexity of your payment system(s).

Complex systems offer hackers more entry or access points to break in and steal data.

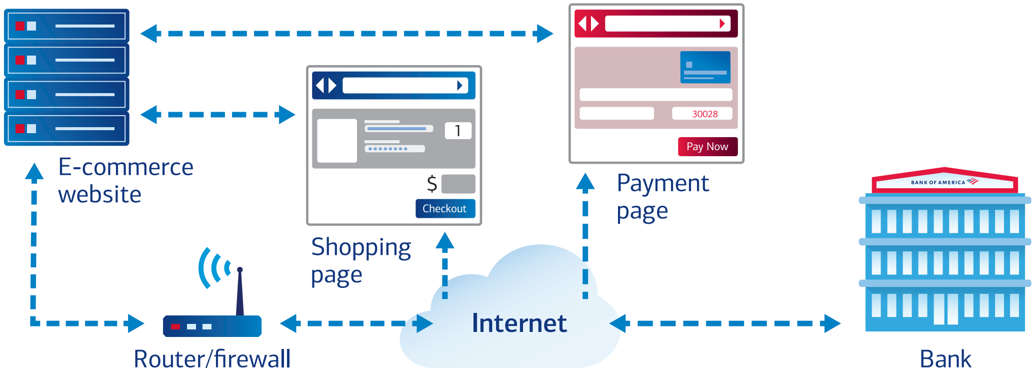
## High risk

Complex payment systems for in-person transactions are difficult to make secure and offer multiple entry points for hackers.



## High risk

Complex eCommerce payment systems for online purchases, where merchants manage their own website and payment page, are also very risky.

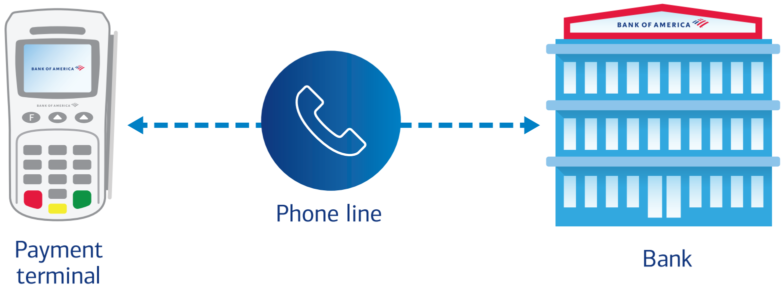


# What are the risks and benefits of different payment systems?

The risk of a data breach greatly depends on the complexity of your payment system(s).

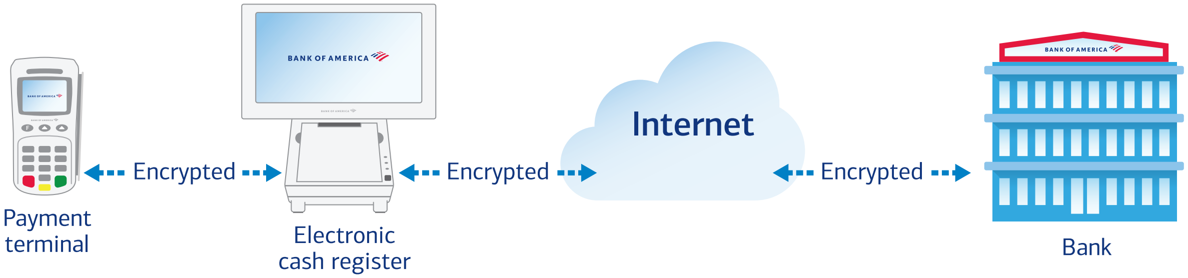
## Less risky

Simple payment systems for in-person transactions are less risky because there are fewer points of entry.



## Most protection

End-to-end encrypted payment systems provide the most protection because if card data is stolen, it can't be used.



# What's the risk for your customers?

When a customer's card information is stolen, they may not learn about it until their bank contacts them. Even though card issuers are required to reimburse customers for fraudulent charges, the customer still has to worry about:

- Overdrafts and bounced checks if debit card information was stolen — thieves can empty the cardholder's checking account.
- Canceling and replacing stolen cards — it's sometimes difficult for cardholders to remember all the accounts and services they use for recurring payments. Out-of-date card information can cause missed payments that may negatively affect their credit score.
- Opening new accounts because of a credit freeze — cardholders who have frozen their credit with credit reporting agencies may need to remove the freeze before they can get a new card.

# How can I reduce risk and protect my business?

Here are some ways you can help protect your business and your customers' information. Details on each of these techniques are provided in the following pages.

| Techniques you can start using now | Ease | Benefit |
|---|---|---|
| 1. Use our secure terminals and systems. | 🟥⬜⬜ | 🟦🟦🟦 |
| 2. Create strong passwords and change default passwords. | 🟥⬜⬜ | 🟦🟦🟦 |
| 3. Inspect payment terminals for tampering. | 🟥⬜⬜ | 🟦🟦⬜ |
| 4. Install patches and updates from vendors. | 🟥⬜⬜ | 🟦🟦🟦 |
| 5. Use up-to-date anti-virus/anti-malware software. | 🟥🟥⬜ | 🟦🟦⬜ |
| 6. Limit remote access to systems on your network. | 🟥🟥⬜ | 🟦🟦🟦 |
| 7. If you're an eCommerce merchant, use a fully outsourced payment page. | 🟥🟥⬜ | 🟦🟦🟦 |
| 8. Use a firewall to protect your systems from internet-based attacks. | 🟥🟥🟥 | 🟦🟦🟦 |
| 9. Protect payments on Wi-Fi. | 🟥🟥🟥 | 🟦🟦🟦 |

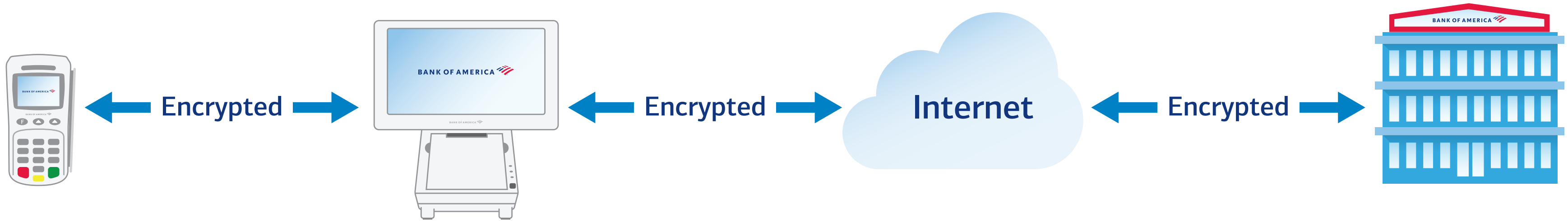
Ease 🟥⬜⬜ Benefit 🟦🟦🟦

# 1. Use our secure terminals and systems.

Each payment system we offer uses end-to-end encryption that protects card data from the point of sale to the card brand. You can upgrade any older systems you may have to our secure equipment to help create a safe payment environment.

**Your security is our priority — here are some details about our terminals and systems:**

- We provide PCI-approved PIN Transaction Security (PTS) devices and PCI-validated payment applications.
- By using our secure terminals and systems, you can reduce a hacker's ability to use stolen card data even if they're able to breach your network. On our systems, your data is secured by means of encryption and tokenization.
- Using our secure terminals and systems also simplifies the process to verify your compliance with Payment Card Industry Data Security Standards (PCI DSS).



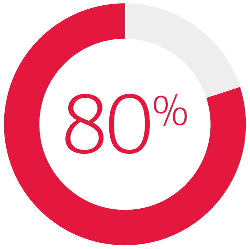
Ease 🟥⬜⬜ Benefit 🟦🟦🟦

# 2. Create strong passwords and change default passwords.

The passwords you use for your computer or network systems are critical for protecting your business and customer data — here are some best practices:

- **Change default passwords.** Most computer equipment and software comes with default passwords such as *password* or *admin*, which are frequently used by hackers to break into networks and systems. Be sure to change the default password on your computer to prevent this.
- **Change your passwords regularly.** By creating new passwords every three months, you significantly reduce the chance of being hacked. Don't use similar versions of the same password like *MyS1llyPa$$word1* and *MyS1llyPa$$word2* — hackers will use a known password and change the numbers until they find the latest version.
- **Make your passwords difficult to guess.** The two most commonly used passwords are *password* and *123456*. Hackers are able to guess more than half of all passwords in a dozen or so attempts. For the most protection, use a phrase as your password. An example would be ItWa$TheBe$tOfT1me$. If you don't use a phrase, create passwords with more than eight characters that include a combination of upper and lower case letters, numbers and symbols.
- **Never share your passwords with anyone.** Each user with access to your computer or network system should create their own user ID and unique password.

Click this link to see an infographic about why you should change your password to something strong



80% of data breaches involve guessed or stolen passwords.[4]

Ease 🟥□□ Benefit 🟦🟦□

# 3. Inspect payment terminals for tampering.

Thieves can steal card data at the point of interaction using a *skimming device*, even if you have end-to-end encryption on your payment system. Such a device can be difficult to notice because they're designed to look like part of the payment device.

Skimming is most common on unattended devices like gas pumps and ATMs, but skimming devices can be attached quickly and easily anywhere. Take these steps to help avoid card data theft from these devices:

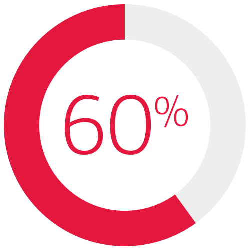
- **Examine all terminals on a regular basis.** Look for obvious signs of tampering such as broken seals over access cover plates, changes in the wiring and new features you don't recognize.
- **Keep an updated list of all payment terminals.** Take pictures of each terminal from all angles so you know what they're supposed to look like.
- **Keep terminals out of reach** when not in use and block their screens from public view. Lock up your terminals when you close for the day.
- **Don't allow unauthorized repairs or replacements.** Make sure all employees verify the identity of anyone claiming to be an authorized repair person.
- **Train all staff** to be vigilant and watchful.

Click this link to see a report outlining best practices to prevent skimming

Ease 🟥□□ Benefit 🟦🟦🟦

# 4. Install patches and updates from vendors.

Hackers can exploit bugs and vulnerabilities that naturally occur in any system. The best way to protect yourself is to install patches and updates provided by vendors as soon as they're available.



60% of breaches were linked to a vulnerability where a patch was available but not applied.[5]

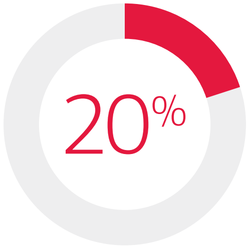
✓ All of your systems should be patched and updated, including:

- Payment terminals
- Payment applications
- Computers
- Cash registers
- Operating systems
- Browsers

Keep in mind, you may have other devices and systems not listed here.

**Additional precautions for eCommerce merchants:**

- It's very important you install patches and updates as soon as they're available.
- Make sure your vendor installs them if you outsource your website or payment page.
- Ensure your hosting provider regularly installs all patches and updates.



20% of all vulnerabilities discovered are High Risk or Critical Risk.[6]

Click this link to see an infographic about the importance of installing patches

Ease 🟥🟥□ Benefit 🟦🟦□

# 5. Use up-to-date anti-virus/ anti-malware software.

Anti-virus/anti-malware software is an important part of your system security. To make sure your systems are protected, you should:

**Make sure you install and continuously run the software on all devices and systems that require it,** including any computer systems or mobile devices on your network.

**Configure your anti-virus/anti-malware software to automatically update** to ensure that you have the most current protection.

**Run anti-virus/anti-malware scans on your system(s) regularly** and consider completing them daily to detect threats faster.

Globally, 56% of organizations identify a security breach at some point.[7]

Nearly 90% of security breaches are financially motivated.[8]

57% of customers say they are not confident that companies follow their own privacy policies with personal data.[9]

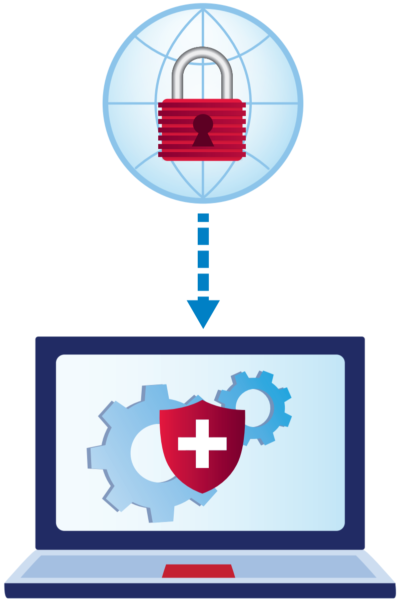
Ease 🟥🟥⬜ Benefit 🟦🟦🟦

# 6. Limit remote access to systems on your network.

Vendors can connect to systems on your network from locations other than your business using remote access software. However, remote access is also one of the most common ways hackers can get into your network — often, they remotely access a computer that isn't related to your payment systems and use it to gain access.

You can take these steps to make your network more secure:

- Know which vendors need and use remote access to systems on your network, not just payment terminals.
- Ensure that any vendors using remote access don't have shared or common credentials.
- If a vendor needs remote access to troubleshoot issues or install updates, enable the access **only at the time they need it** and disable it as soon as they complete the work.
- When possible, ensure vendors use multi-factor authentication (MFA) to remotely access your system(s). MFA requires individuals logging in to a system to use at least two of these: a username and password or passphrase, a token or smartcard, and a biometric such as a fingerprint scan or facial recognition.



74% of organizations breached within the last 12 months said the exposure originated from third parties.[10]

Examples of remote or non-console access software include VNC and LogMeIn.

Click this link to see an infographic about securing remote access

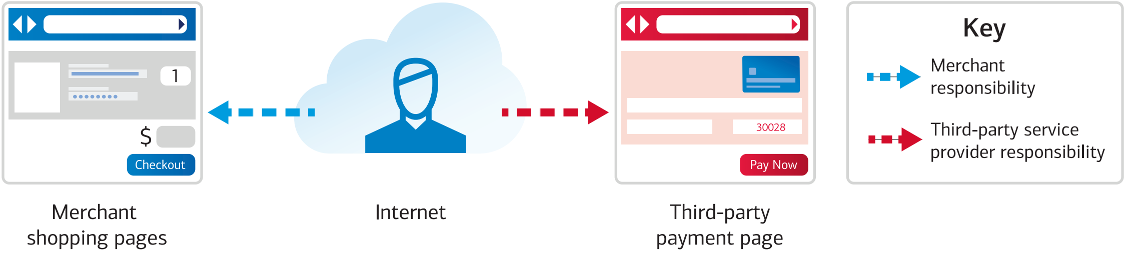
Ease 🟥🟥⬜ Benefit 🟦🟦🟦

# 7. If you’re an eCommerce merchant, use a fully outsourced payment page.

If your customers make purchases or donations on your website or payment page, it’s important you use a fully outsourced payment page from a PCI-compliant third-party vendor because:

- eCommerce is one of the fastest growing targets for hackers — chip cards have made it more difficult for hackers to steal card data from payment terminals, so they’re focusing on web and payment pages.
- Building your own payment page is complex and it can be difficult to keep secure, up-to-date and patched.
- It can significantly reduce the risks to your business and your customers.
- Validating your PCI compliance is much easier.

Visit the Visa Global Registry of Service Providers to see if your eCommerce Service Provider meets the PCI Council’s security requirement.



Click this link to read a report about securing eCommerce transactions

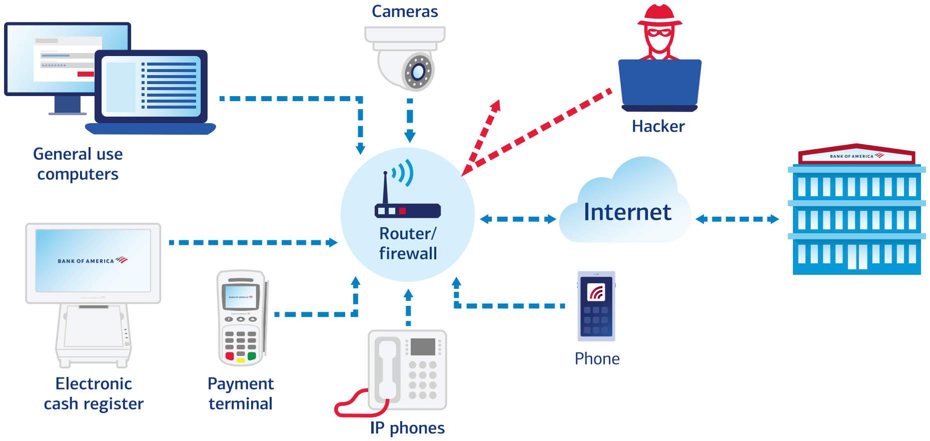
Ease 🟥🟥🟥 Benefit 🟦🟦🟦

# 8. Use a firewall to protect your systems from internet-based attacks.

If you use the Internet (either Wi-Fi or ethernet) to connect your payment terminals, it's critical that you use a firewall to protect payments and other systems from the Internet.

Here's what you need to know:

- A properly configured firewall is a network security device that blocks unauthorized access, including hackers and bots, and prevents them from gaining access to your computers and systems.
- Routers pass traffic back and forth from the internet, but many of the newer broadband routers also have built-in firewalls. If you're not sure whether or not your router has a built-in firewall, ask your broadband or internet service provider.
- If you use the internet for anything other than your payment terminals, use your firewall to segment your network to completely isolate your payment terminals from the rest of your network. You can then lock down the payment terminal network segment to ensure only traffic to and from your payment processor is allowed.
- Limit physical access to your firewall so that no one can connect any equipment you haven't authorized.
- If you only accept payments using a computer that's connected over public Wi-Fi, install a software firewall to ensure your card data environment is safe.



The firewall acts like a filter between your systems and the Internet to protect your business from hackers.

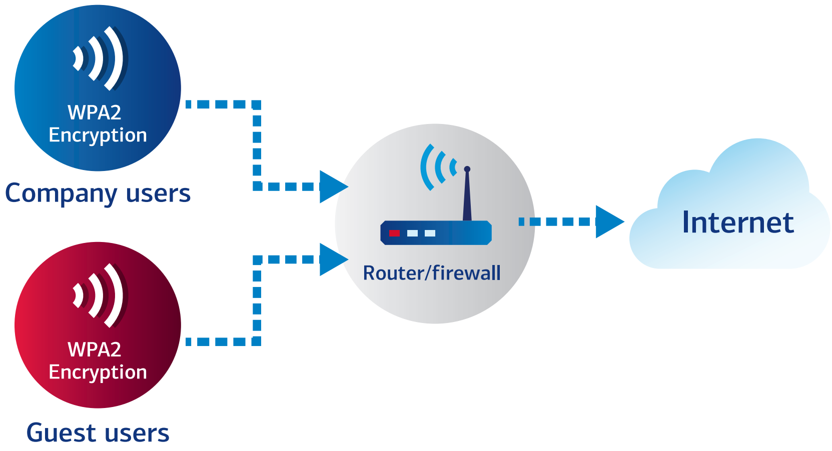
Click this link to see an infographic about firewall basics

Ease 🟥🟥🟥 Benefit 🟦🟦🟦

# 9. Protect payments on Wi-Fi.

If your business uses or offers Wi-Fi, it’s critical you secure it because Wi-Fi is a very common entry point for hackers. Here’s what you need to do:

- If you offer guest Wi-Fi to your customers, make sure you use a separate network segment specifically for guest access. This will help ensure no one can access critical business systems or customer data through your Wi-Fi.
- If your payment terminals use Wi-Fi, make sure you set up a network segment specifically for your payment systems and nothing else.
- Use WPA2 encryption and a strong password for your Wi-Fi. Older encryption methods like WEP or WPA aren’t secure.
- Disable Wi-Fi Protected Setup (WPS) — this is the ability to connect Wi-Fi devices with the push of a button using a PIN.
- Ensure that physical access to your router/firewall or other Ethernet ports is locked down and there aren’t any unauthorized Wi-Fi access points connected to your network.
- When using public or guest Wi-Fi to take payments, here’s what to keep in mind based on the payment device you use:
  - **Payment terminal** — make sure it’s updated with latest software and firmware and used/stored in a secure location.
  - **Mobile device** — use a device that doesn’t allow unrestricted access (known as a jail-broken or rooted device) because it makes the device more vulnerable to hacking.
  - **Laptop** — if you use one with a virtual terminal or payment application, make sure the laptop is running up-to-date anti-virus/anti-malware software and has a correctly configured firewall.



# How can I comply with Payment Card Industry Data Security Standards (PCI DSS)?

The PCI Security Standards Council, founded by the major card brands, established security standards designed to reduce credit card fraud. The card brands require every business that accepts credit and debit payments to comply with PCI DSS and validate compliance.

If you process fewer than 1 million total card transactions or 20,000 eCommerce transactions each year, you can complete a self-assessment. There are two ways to complete it and validate your compliance:

## Use our simple PCI Assist portal.

**Set it up once — it's easy to revalidate your PCI compliance with just a few clicks, and you won't need to send us any documents.**

1. Go to the Merchant Help Center and click on the PCI Compliance link.
2. Follow the instructions to complete the Profile section. The system will then pre-fill many of the questions for you to validate your PCI compliance.
3. If you're required to pass a vulnerability scan every 90 days, you can schedule it through the portal. The scan will then run automatically for you.
4. If there haven't been any changes, with just a few clicks, you can quickly re-validate your compliance each year.

## Follow the council's steps.

**You have to download and fill out the SAQ in its entirety each year.**

1. Go to the PCI Council website.
2. Determine which Self-Assessment Questionnaire (SAQ) you should use.
3. Download and complete the SAQ.
4. Scan and upload the SAQ to our PCI Assist portal.
5. If you're required to pass a vulnerability scan every 90 days, you'll need to have the scans completed by an Approved Scanning Vendor. After each vulnerability scan, upload the results to our PCI Assist portal.
6. Re-validate your PCI compliance 12 months from the date of your last assessment, including the vulnerability scans every 90 days, if required.

# Resources

**Additional resources you may find helpful:**

- It’s Time to Change Your Password
- Best Practices for Skimming Prevention
- Patching and Updating Your Systems
- Secure Remote Access
- Visa Global Registry of Service Providers
- Firewall Basics
- PCI Guide to Safe Payments
- Common Payment Systems
- PCI Self-Assessment Questionnaires

# Sources

[1] Ponemon Institute, “2019 Global State of Cybersecurity in Small and Medium-Sized Businesses,” commissioned by Keeper Security, October 8, 2019.

[2] Salesforce Research, “Trends in Customer Trust,” September 6, 2018.

[3] Verizon, “2021 Data Breach Investigations Report,” May 13, 2021.

[4] Verizon, “2020 Data Breach Investigations Report,” May 19, 2020.

[5] Ponemon Institute, “Costs and Consequences of Gaps in Vulnerability Response,” commissioned by Service Now, October 2019.

[6] Edgescan, “2018 Vulnerability Statistics Report,” May 2018.

[7] Thales, “2021 Thales Data Threat Report,” February 2021.

[8] Verizon, “2020 Data Breach Investigations Report,” May 19, 2020.

[9] Pew Research Center, “Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information,” November 15, 2019.

[10] Ponemon Institute, “A Crisis in Third-party Remote Access Security,” sponsored by SecureLink, May 4, 2021.