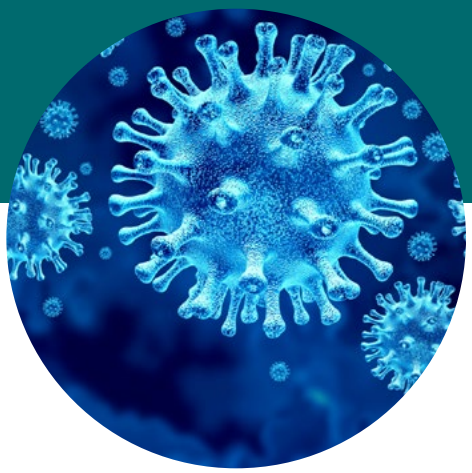
8 Tips to Help Small Merchants Protect Payment Card Data During COVID-19



The COVID-19 pandemic is quickly changing how many small merchants accept payments. Merchants that previously only had brick-and-mortar locations are moving to accept e-commerce and over-the-phone transactions. PCI Security Standards Council shares key considerations to help small merchants keep their customers' payment data secure in this rapidly changing environment.

UNDERSTANDING THE RISK

Cybercriminals are moving quickly to take advantage of rapid changes to payment card data environments.

475% increase in malicious reports related to Coronavirus in March.[1]

41% of small businesses that suffered a data breach paid more than $50,000 to recover.[2]

29% of consumers surveyed said they would never again use a small business that suffered a data breach.[3]

1: Source: BitDefender 2, 3: Source: Bank of America Small Business Payments Spotlight

TIPS FOR SMALL MERCHANTS

These resources and more can be found on the PCI SSC Small Merchant webpage and on the PCI Perspectives Blog.

TIP #1: REDUCE WHERE PAYMENT CARD DATA CAN BE FOUND

The best way to protect against data breaches is not store card data at all. Many small merchants are offering curbside pickup now and are accepting telephone payments in lieu of former face-to-face transactions. Avoid writing payment card details down and instead enter them directly into your secure terminal.

More Information: PCI SSC Special Interest Group Paper: Accepting Telephone Payments Securely

TIP #2: USE STRONG PASSWORDS

The use of weak and default passwords is one of the leading causes of payment data breaches for businesses. To be effective, passwords must be strong and updated regularly. Weak and vendor default passwords are a frequent source of small merchant breaches.

More Information: Strong Passwords Infographic

TIP #3: KEEP SOFTWARE PATCHED AND UP TO DATE

Criminals look for outdated software to exploit flaws in unpatched systems. Timely installation of security patches is crucial to minimize the risk of being breached. One way to keep up with all the necessary changes is by ensuring vulnerability scans are performed regularly to identify security issues. PCI Approved Scanning Vendors (ASVs) can help you identify vulnerabilities and misconfigurations in your Internet-facing payment systems, e-commerce website, and other systems, providing a report of your vulnerabilities and how to address them—for example, what patches to apply. Be sure to act upon the results of ASV vulnerability scans and keep your software up to date.

More Information: Patching Infographic

PCI Security Standards Council

TIP #4: USE STRONG ENCRYPTION

Encryption makes payment card data unreadable to people without a specific key, and can be used to protect stored data and data transmitted over a network. Ask your vendor whether your payment terminal encryption is done via a Point-to-Point Encryption solution and is on the PCI SSC's List of PCI P2PE Validated Solutions. If you are setting up a new website, confirm the shopping cart provider is using proper encryption, such as TLS v1.2, to protect your customers' data.

More Information: Information Supplements on Use of SSL/Early TLS

TIP #5: USE SECURE REMOTE ACCESS

To minimize the risk of being breached, it's important that you take part in managing how and when your vendors can access your systems. Criminals can gain access to your systems that store, process, or transmit payment data through weak remote access controls. You should limit use of remote access and disable it when not needed. If you must allow remote access, ask your vendors to use multi-factor authentication and strong remote access credentials that are unique to your business and not the same as those used for other customers.

More Information: PCI SSC Secure Remote Access Infographic

TIP #6: ENSURE FIREWALLS ARE CONFIGURED PROPERLY

A firewall is a device or software that sits between your network and the Internet. It acts as a barrier to keep traffic out of your network and systems that you don't want and didn't authorize. Firewall rules can seem complex, but configuring them properly is vital to security. If you require additional assistance to properly configure your firewall, seek help from a network professional.

More Information: Resource for Small Merchants: Firewall Basics

TIP #7: THINK BEFORE YOU CLICK

Hackers use phishing and other social engineering methods to target organizations with legitimate-looking emails and social media messages that trick users into providing confidential data, such as payment card number, merchant account number or password. Small merchants should be extra vigilant and be on the look out for common phishing and social engineering hacks.

More Information: Beware of COVID-19 Online Scams and Threats

TIP #8: CHOOSE TRUSTED PARTNERS

It's critical you know who your service providers are and what security questions to ask them. Is your service provider adhering to PCI DSS requirements? For e-commerce merchants (and those of you that recently started accepting e-commerce payments in lieu of face-to-face payments), it is important that your payment service providers are PCI DSS compliant, including the service provider that manages your payment process (your "payment service provider" or PSP).

More Information: Questions to Ask Your Vendors

PCI SSC IN-DEPTH BACKGROUND MATERIALS

Best Practices for Securing E-commerce

Protecting Telephone-Based Payment Card Data

Protecting Payments While Working Remotely

Guide to Safe Payments

Questions to Ask your Vendors

Common Payment Systems

The Council has established resources for COVID-19 updates, so please be sure to check our COVID-19 webpage and our blog regularly as this is a constantly evolving situation. You can also subscribe to our blog to receive email alerts.

PCI Security Standards Council