

MTC TECH TALK

*For Humans
Not Geeks!*

Your resource for the latest technology updates and opportunities for your success.



Navigating the New PCI Compliance 4.0:

Keeping Payment Data Safe and Sound


What's In This Issue?

Your Monthly
Technology Update

How To Safely Share Passwords
With Employees

The Future of Fraud

Planning Digital
Transformation? Don't
Forget Your People

Meeting Tree Computer
 (845) 237-2117

Did you know that if your business accepts, handles, stores, or transmits credit/debit card payments, you must adhere to security standards outlined by the Payment Card Industry Security Standards Council (PCI SSC)? And that it isn't only big companies that must adhere to these rules?

The moment your customer hands over their payment information, you become responsible for keeping this data secure.

This, unfortunately, is easier said than done.

So let's dive in and explore PCI compliance, its everyday relevance, the fallout from not following the rules, and some strategies to stay in the compliance game.

What is PCI Compliance?

Created in 2004 by Visa, MasterCard, American Express, and Discover, the Payment Card Industry Data Security Standard (PCI DSS) has worked together for years to ensure that all organizations that handle credit/debit card payments have systems and processes to prevent data breaches.

Although the foundational framework of PCI-DSS has remained the same since its inception, numerous incremental changes and improvements have occurred over time. The most recent version is PCI DSS 4.0. Version 4.0 was released in March 2022 and has an implementation deadline of March 31st, 2024.

Every company that accepts credit and debit cards must follow PCI DSS, no matter the volume of transactions it processes or the business size (although the PCI SSC does help small businesses). However, there are four levels of compliance, depending on the number of transactions a business processes annually. These levels determine what actions it must take to be compliant; the more transactions, the more actions are necessary.



PCI v4.0 lists 14 requirements that must be considered if your goal is to be compliant.

Getting Started With PCI Compliance

Preparing for a PCI audit and ensuring your company meets credit card compliance standards can be daunting. Use these five steps to help guide your business through the process:

Determine your business's relevant PCI compliance level by performing an audit to identify the cardholder data you are responsible for. This will help determine what actions you must take to become compliant.

Take stock of your IT assets and evaluate your processes for securing payment data. Scrutinize these aspects of your business operations for potential vulnerabilities that malicious actors could exploit to purloin cardholder data and note any compliance gaps. Any system that connects to the cardholder data environment is within the scope of compliance and, therefore, must meet PCI requirements.

Take steps to fill in gaps and eliminate vulnerabilities in your system.

Once you have a well-documented system that adequately addresses all 14 PCI DSS standards, you can complete a Self-Assessment Questionnaire (SAQ).

Ensure your compliance reports are submitted to the relevant banks or card brands you engage with (e.g., Visa, MasterCard, American Express, or Discover). This proactive step will prevent the accumulation of penalties or fees that could arise from failing to maintain PCI compliance.

It is important to note that only Level 1 merchants and service providers (processing more than 6 million transactions annually) must have their PCI compliance validated by a Qualified Security Assessor (QSA). All others can confirm compliance by performing a Self-Assessment Questionnaire (SAQ) before requesting an Attestation of Compliance (AOC).

What Are The Consequences Of Non-Compliance?

Although implementing PCI DSS compliance can be a hassle and maintaining compliance is an ongoing process, compliance gives peace of mind and protects your business

from data breaches and violations.

Consider these potential consequences:

Dealing with a data compromise is a time-consuming and expensive hassle from both a consumer's and a business owner's perspective.

Monthly penalties imposed by payment processors for non-compliance ranging from \$5,000 per month to \$100,000.

Banks can terminate your merchant account for coming short of PCI DSS, preventing you from taking card payments.

Regulatory bodies, payment card brands, and acquiring banks can impose substantial fines on non-compliant organizations.

Non-compliance and consequential data breaches can also lead to legal, financial, and reputational repercussions, as the fallout from a breach can damage customer trust, lead to customer attrition, and harm your brand's reputation.

PCI DSS Compliance Takes Work

Assessing the PCI components, documenting procedures, conducting ongoing risk assessments, addressing gaps, and performing SAQs is a massive undertaking. However, protecting cardholder data from fraud and building trust so your customers feel comfortable using their credit cards when doing business with you are worth the work it takes to be(come) compliant.

Thankfully, there is an alternative to the Do-It-Yourself (DIY) path – an option that keeps you safer while taking your compliance and data security problems off your plate. With PCI 4.0 knocking on the door, outsourcing PCI compliance to a compliance-savvy MSP like Meeting Tree Computer is a smart move. With our one-stop-shop data compliance management services, we take care of everything for you. You won't have to worry about securing, updating, and maintaining anything, and performing a self-assessment questionnaire or hiring a security assessor will all be part of the plan allowing you to focus your time on developing your core business and growing your customer base.

Technology Update



Introducing 'People view' in OneDrive

Microsoft is at it again with more innovative features. This time it's releasing 'People view' in OneDrive Web. It's designed to make it easier to access shared files, and is integrated directly into OneDrive. This is perfect if you regularly receive files from different people and need an easier way to locate them.

The best part? Using People view is a breeze - just select a file or folder like you would with any other item in OneDrive. It's designed to keep you organized by grouping shared files. We believe it's both user-friendly and intuitive.

How To Safely Share Passwords With Employees



If you ask a security professional, you get by-the-book advice about sharing passwords: “Don’t share passwords.” But we know, in reality, that doesn’t work. Your office might be sharing a single

password for apps like SurveyMonkey right now to save cash on buying additional users, and some social media accounts don’t even give you the option to have multiple log-ins.

Sharing passwords in your office is sometimes necessary for collaboration and makes employees’ jobs a lot easier. . Medical leaves, turnover, vacations and “Bob isn’t coming in because he ate bad fish last night but has our Amazon log-in” are other reasons passwords get handed around like a plate of turkey at Thanksgiving dinner.

The Future of Fraud

To help fight cybercrime, it’s important to look

ahead and forecast what the future of fraud may look like. With this knowledge, it becomes easier to plan for future attacks face them head on.

Let’s explore some possible future cyber scams.

An emerging trend within the cybercrime sphere revolves around the incorporation of artificial intelligence (AI). Deepfake images, audio files and videos are gaining popularity because they’re easy to create and incredibly convincing when done right.

Expect to see a large uptick in attacks targeting IoT devices. You may think who would want to hack my smart refrigerator, but these events do

happen. Attacks on medical devices more than doubled worldwide during the pandemic. A compromised device could either put sensitive patient information at risk or can be configured to malfunction at the cybercriminals command. Imagine having your heartbeat regulating pacemaker held hostage by a villain.



Last but not least, all signs point to the dark web playing a huge role in the future of cybercrime. Insights into the dark web show cyber criminals working together, and in many cases

However, unsafe sharing habits will put your private passwords in the hands of greedy hackers, who can fetch a high price for your data in dark web markets. IBM Security reported that in 2022, 19% of all breaches were caused by stolen or compromised credentials.

So, how do you share passwords safely?

We recommend using reliable password managers because they have multiple layers of encryption so only those with a key (your master password) can see it, AND they include more robust security and sharing features like: Multifactor authentication, unique password generation, fake log-in page warnings, breach or weak password notification and simple, secure built-in password sharing (Some password managers let you choose which passwords your employees can see and keep others in a private vault. Others, like Keeper, let you share documents or records without exposing credentials).

Smart Businesses Use Password Managers

It’s a good idea to avoid sharing passwords as much as possible, but when you have to, use a reliable password manager to ensure you have control over exactly who sees your credentials. If you’re not sure which password manager to use, give us a call and we’ll get you set up with one.

helping each other for our demise. Scammers are enhancing their tools and streamlining attack methods, while also sharing their success stories and tips. Dastardly developers create new malware and injection methods then put their designs on the web available for purchase at affordable rates. Unfortunately, we expect to see more individuals flocking to this profession and the online black market known as the Dark Web as the demand grows.

These forecasts may seem a bit too grim, but we have to be proactive in protecting ourselves: watch for an increase in scam campaigns and, like the scammers, use the community approach to alert others in your circle about circulating scams. Call us if you see anything phishy and that you’re not sure how to handle!

Planning Digital Transformation? Don't Forget Your People.

Have you heard of the term “digital transformation”? It's where you introduce new technology across every part of your business, to help you sell more, deliver better customer service and be more efficient/profitable.

That word ‘transformation’ sounds impressive, doesn't it? It's like your business is a caterpillar, ready to emerge from its cocoon as a dazzling, tech-savvy butterfly.

But hold on a minute, let's not forget about the most important part of this metamorphosis – **your people**.

Yes, you read that right. It's not technology that should be at the heart of any digital transformation... it's people.

Businesses often make the mistake of getting caught up in the whirlwind of “cool new tech” and forget about the human element. How many times have you heard of a company rolling out a major new software system, only for their employees to struggle with the change?

The truth is, the success of any digital transformation hinges on your team's buy-in. You can have the most cutting-edge technology in the world, but if your people hate using it, it's going to fail.

So how do we put people first in digital transformation? It starts with communication. Your team needs to understand why change is happening and how it will benefit them. This isn't just a one-time announcement, but an ongoing two way conversation.

Next, you need champions. These are individuals at all levels of the business who are enthusiastic about the change and can help others get on board. Enthusiasm is contagious!

And finally, you need to break down silos. The digital world thrives on collaboration, and your business should too. If departments are working in isolation, you're not harnessing the full potential of your team or your technology.

Let's not forget about the role of AI in all this. Generative AI systems, such as ChatGPT, have been making waves in the media, highlighting the importance of the human element in the digital transformation debate. After all, technology should serve people, not the other way around.

The pace of technological advancement is dizzying, no doubt about that. But amidst all the change, one thing remains constant - the importance of putting people, processes and culture at the center of your digital transformation.

If we can help you with any kind of technology project, get in touch.



This is how you can get in touch with us:

call: 845-237-2117 | email: info@meetingtreecomputer.com
website: www.meetingtreecomputer.com

Q&A

How do I back up my data?

Backing up data can save your business from a catastrophe, so make sure you do it! Basic backup can be as simple as connecting an external drive and copying important files. However, you must then remember to do it. The most robust solution is using software that updates all your files securely to the cloud, all the time. We can suggest a service if you want.

Our network is slow... can we speed it up?

A slow network is frustrating and can halt productivity. To speed it up, you can upgrade your hardware, optimize router settings, limit bandwidth-hungry apps, and regularly update network drivers. Again... we can help!

Do my staff need USB cameras when working from home?

Most current laptops have great cameras built-in, so probably not. However, the better the image and sound, the better they can communicate. It might be worth investing in cameras, USB microphones and lighting for staff who speak to clients or prospects on video calls.

Submit Your Questions Here:
info@meetingtreecomputer.com



Follow Us

