



10 Myths of PCI Compliance

One of the most essential and vital possessions of any person in this era is their own personal information. Buying and selling on the Internet has introduced the hazards of exposing one's confidential information. Therefore, trust in the current security measures is vital nowadays, and the essential demand for stronger security and standardized tools and controls has become tremendous.

The Payment Card Industry Data Security Standard (PCI DSS) is a unique set of rules, aimed to ensure that all companies that process, store or transmit credit card information maintain a secure environment. Essentially, any merchant that takes credit cards, has to follow the PCI DSS, created by the Payment Card Industry Security Standards Council.

The five major credit card companies generated it as a guideline for the merchants and for other companies who are dealing with hardware, software and other effective procedures, to safeguard sensitive credit card and personal information. The rules of PCI compliance are stringent so as to ensure a secure environment, but also, PCI compliance has benefits that are rewarding for your business.

Most companies try to build long-lasting trust and hence acquire such services from the very beginning that can only be attained from a PCI compliant host. Merchants that meet PCI compliance are less likely to have a breach and can enjoy a safer harbor.

PCI compliant hosting for your web site, provides your customers a peace of mind, dwindles the risk of security breach, improves customer trust, helps protect you from fines, and guards your business' reputation.

There are a few myths about Payment Card Industry Data Security Standard that need to be resolved to remove fear and to maintain the trust in PCI, which we will now describe.

Myth: PCI compliance is too expensive

Fact: PCI compliance is affordable and worth it because it fulfils all the requirements of guarding personal information. In fact, it is the most reasonable and effective security measure within your means. Organizations spend millions on business infrastructure such as Human Resource, Equipment, Marketing, etc. PCI is much cheaper considering its effectiveness.



Myth: PCI compliance is for the U.S. only

Fact: Wherever there is a requirement for preservation or transmission of personal information you can find PCI compliance. PCI compliance is present worldwide. United States is the world's strongest economy and therefore PCI compliance is more common there, however it applies to all businesses that accept credit cards, no matter where in the world they are.

Myth: PCI compliance is too hard to achieve

Fact: People usually consider PCI compliance too hard, as they believe it is not cheap and time consuming, but this is not true. The cost of having a non-compliant business can be vast and devastating such as fines, legal fees and decrease in reputation. Implementation of PCI DSS can help save and protect from such disasters. And with your hosting company helping you out on this, it is not as hard as it seems.

Myth: PCI Compliance is only for large businesses

Fact: PCI is applicable to any size of business. If you take even 1 credit card a year, you need to be PCI compliant. Business can only flourish if proper infrastructure is established such as Human Resources, Marketing, Customer Service, etc. In the same way PCI Compliance is something that should be setup and considered as a key ingredient of your business infrastructure.

Myth: You only need to be complaint with the majority of the PCI DSS conditions

Fact: You need to comply with ALL the PCI standards that apply to you. If you are scanned by an ASV, and are found non-compliant for even 1 rule, then you lose your PCI compliant status.

Myth: PCI is optional, we can wait until there is an obligation or the bank advises to be PCI Compliant

Fact: You must be PCI compliant at all times, even if your merchant account provider or bank has not specifically said you need to be. Waiting for a bank to require you to become PCI compliant is not allowed, and by the time they tell you, it may already be too late, and your customer's data could have been compromised.

Myth: PCI Compliance means I am hack proof

Fact: If all standards of PCI are applied, then there is less risk of a problem, however no system or set of rules is perfect. PCI compliance gives better safeguard, and makes it a lot more difficult for a hacker to get to you, therefore he will likely move on to another target. But it is not a golden guarantee you will never get hacked.



Become PCI Compliant in 24 Hours
PenguinWebHosting.com

Myth: PCI Compliance prevents storing card holder data

Fact: PCI DSS strongly opposes the storage of card holder data by merchants and processors, but does allow it if there is a business reason to store card information, and you meet or exceed all of the PCI compliance rules. This only applies to some of the card information, for example the 3 or 4 digit CVV number is never allowed to be stored.

Myth: PCI Compliance is only applicable for online companies

Fact: PCI applies to every company that deals with card holder information, whether its a retail store, a restaurant or an online store. Because at most physical locations, the credit card numbers are transmitted through the Internet for charging, we can say that in this world of technological enhancements every single company is an E-Company.

Myth: Protection of only credit card data is required, and not ATM debit card data

Fact: Both types of data are required to be protected by PCI compliance. You should use the same methods to protect a debit card number, that you would for a credit card.