**5 Ways to Secure your Ecommerce Website**

If we consider how common hacking and data breaches have become today, it is not unusual for ecommerce websites to face security challenges from cybercriminals. Though ecommerce startups are mostly technically knowledgeable, they still lack the expertise to strengthen the security of their website. More than any other business, ecommerce businesses are at a high risk of cyber attacks and losing their reputation as well as customers in case of a data breach. If the issue is not dealt with, along with disgruntled customers, they can also lose their website and customer’s data. But fortunately, there are several ways in which an ecommerce business can secure its website from cyber threats. This article elaborates five such ways.

1. **Choose a Better Ecommerce Platform and Hosting Service**

When choosing an ecommerce platform, a business must account for different factors such as performance, support, and features. But because financial transactions are involved in an ecommerce business, security must be at the forefront – thus a platform that prioritizes it should be chosen. A platform that uses secure payment gateways, includes shipping method extensions and releases regular security patches. There are many secure Ecommerce platforms available, such as Prestashop, Shopify and WooCommerce.

Similarly, chose a web hosting service that has a good backup service for easy restoration of the website in case of a security breach. Also ensure that it is operational at all times with maximum uptime. A good hosting service must also have a RAID data protection to make backup copies of your site on multiple disks so that your website performs faster. For security, it is always recommended to choose a managed cloud-hosting platform. Not only is security handled professionally in a managed platform, you can also add further security layers to your website from the admin panel.

1. **Always use HTTPS**

Instead of using simple HTTP, it is always recommended to use HTTPS, which secures the transmission of data across the website by encrypting the information between the customer’s browser and your servers. This helps avoid online frauds and prevents cybercriminals from stealing user data. Before moving your website to HTTP, you must install Secure Socket Layer (SSL) certificate to your website.

HTTPS advantages go further beyond security. In fact, Google ranks websites with HTTPS at a higher search ranking, which attracts more visitors. Contrary to that, Google also marks an unencrypted website as “non secure”, which makes a website appear unsafe to the user.

1. **Don’t Store Customer’s Sensitive Data**

A customer’s personal information and privacy is of utmost importance, especially for websites that take financial details. Though businesses require this data for improving their product offerings and communication with customers or to make purchase returns easier, the danger of saving confidential user data is that it can be easily targeted by hackers through phishing or cyber attacks.

Ensure that no sensitive data such as credit card details are stored on your website. If your system gets compromised, not only will you face reputational and financial loss, you will also lose your customers – which takes a lot of time and marketing efforts to attract in the first place. You can also prevent this by using Tokenization, a process that generates token or random number instead of customer information. It greatly helps to prevent credit card frauds.

As a first rule, only collect the data that is required for completing the transaction. To ensure easy handling, avoid getting more data than what is required. This rule is particularly relevant to storing [credit card](http://www.cardzgroup.com/logistics.html) information of customers. Not only is it unnecessary after a transaction completes, it also violates Payment Card Industry - Data Security Standard (PCI-DSS), which is discussed in the next paragraph.

1. **Ensure that Your Website is PCI DSS Compliant**

As an ecommerce business owner, you must ensure that your website is in compliance with the PCI DSS, which is a security standard for the payment card industry. Among many other best practices, the standard also ensures that you as an administrator have control over your customer’s cardholder data in order to prevent online frauds. By complying with PCI DSS, your website can proactively prevent and detect potential breaches. Also, it regulates you to perform regular vulnerability scans on your website to allow very little opportunity for hacking attempts. Every ecommerce platform has its different tools for vulnerability scanning. Also, always update your website to ensure that you have latest patches installed for all software programs.

1. **Always Monitor Your Website**

Even deploying all the security measures stated above does not completely ensure that your website will remain safe from cyber criminals. It is always a good idea to invest in a robust third-party monitoring tool for your website. Such tools are specifically designed with advanced features to not only help your website to run reliably but also more securely. You can build your personal dashboard and use features like performance benchmarking and application health monitoring for smooth running of your website, which is a mandatory requirement for seamless customer shopping experience. Even if you are not an IT professional, you can still use features like audit rail for modifications or a root cause analysis engine – which can help track down security problems while they happen or even before a potential problem arises.

**To put it short,** the actual challenge for ecommerce businesses lies in effective implementation of security and authentication measures in a frictionless manner so as to not impact the customer’s experience – while staying on top of ever emerging threats without compromising on security budget. Only by putting security at the core of your business model, you can offer your customers a safe online shopping experience.