**8 Ways for Businesses to Keep Online Transactions Secure**

Online shopping has become increasingly popular in the past few years. But as more people go online to conveniently shop from home, it gives cybercriminals all the more advantage to attack them and use their information to their advantage. This is why ecommerce companies work hard to secure their transactions and build their customer’s trust as the looming threats of cybercrimes can give a reasonable blow to their marketing efforts. Scammers are now targeting both merchants and customers. Once they gain your financial information, they may use it to buy goods and services for themselves, or sell your information to someone else and make a profit.

So what can businesses do to ensure safe online transactions for their consumers? The answer: stay aware and take safety precautions. If you want your customers to get the best out of their online shopping experience – without being a target of internet scams and cyber criminals – you as a business need to take ensure their safety by considering some important steps.

As a business owner, you are liable for any type of online data breach. Any problem of this nature can mean fees and penalty, damaged reputation and business loss.

Here are eight security steps that can help ensure businesses to keep their online transactions secure.

1. **Protect Your Customer’s Financial Information**

According to the Fair and Accurate Credit Transaction Act 2003 (FACTA), it is illegal to store a customer’s financial information. So, whatever you do, do not keep a customer’s financial data with you after a transaction. Not only will it save you from any legal liabilities, but will keep your business away from online security risks. If you don’t keep the information, the risk is gone.

However, if you need to store the information for genuine business operational purpose, you can use a private network for storing it to make it safe from online intruders. As a business owner with a merchant account, you are contractually liable to protect the customer’s financial information. Firstly, your transaction hardware and software should be PCI compliant, whether you use a Point of Sale terminal or a swiper linked to a computer running a payment software. This is because many card readers and software applications have security vulnerabilities that make them unreliable for use. Even if you are storing credit card information, do not store the security code or track data of the card saved in its magnetic stripe on the card’s back. Whether you store the information on paper or electronically, make sure it is stored in a secure place and encrypted respectively.

1. **Ensure Compliance to PCI-DSS**

This is probably one of the most important and comprehensive ways of ensuring safety of online transactions for a B2B business. The Payment Card Industry Data Security Standard is a set of compliance regulations for businesses involving payment cards. It provides steps for merchants to securely process, store and transmit credit or debit card payments to reduce the risk of loss of financial data.

PCI DSS provides comprehensive guidelines on how data breaches can be detected, prevented or what can be the course of action in case a breach occurs. They include 12 requirements for payment processors and merchants which are grouped into six main areas which include 1) Build and maintain a secure network and system 2) Protect cardholder data 3)Maintain a vulnerability management program 4) Implement strong access and control measures 5) Regularly monitor and test networks 6) Maintain an information security policy.

While it may seem cumbersome to implement the standards, you may want to seek help from a compliance specialist for this. Consider hiring a security consultant who can assist you with an annual assessment to point out vulnerable areas and provide solutions to comply with the PCI DSS regulations.

1. **Partner with a Secure Payment Processor and Ecommerce Platform**

Do your research and see which out of the hundred ecommerce platforms and processors are reputable and have good ratings, especially in implementing updated security measures. Once you partner up with a reliable payment processor and ecommerce provider, you can get advantage of all the security features that come along with the partnership.

For instance, e-commerce platforms like WooCommerce or Shopify come with added security features where you don’t have to be solely accountable for detecting threats or providing security. You can have a third party to keep your business safe and help you out.

1. **Verify all Your Transactions**

Always be vigilant towards transactions occurring from your business customers for any abnormal or out of routine transactions taking place, or an order that asks for delivery to an address other than the one mentioned on the record. You can contact the customer directly by phone and get confirmation from them about the larger-than normal transaction. Always seek the credit card security code in your online payment forms. Once you start to recognize fraudulent patterns, keep a note and train your new employees to watch out for such fraudulent transactions.

1. **Get an SSL Certificate for your Website**

When it comes to credit card breaches, all businesses can be a target. Getting an SSL certificate will help to safeguard your website and protect your customer’s sensitive information. SSL, which stands for Secure Sockets Layer, is the technology encrypting a connection with a website. When a merchant installs SSL certificate to their website, it works in the background to ensure that any sensitive information entered into your site is safeguarded automatically. When running an ecommerce website, getting an SSL certificate is not only a good idea but also necessary to comply with PCI DSS.

Technically speaking, SSL helps encrypt data which is hard to read by malicious outsiders as it can be only deciphered by three keys. One key is with the website and the other is with the browser. When a connection is made between the browser and the website, a third temporary key is created, called the session key. It organizes the exchange for the entire session until the user logs out and all three keys work together to create a unique encrypted communication.

1. **Use Personal Verification System**

For items that cost more, it is always a good step to get some sort of personal verification from the customer. For instance, Airbnb uses personal verification technology to verify users by asking them to submit their passport or ID. Verified users can then book rooms at once without waiting in confirmation lines.

You can also verify the customer’s address before authorizing a [credit card transaction](http://www.cardzgroup.com/ContactSmartCard.html). The merchant will receive a response code from the payment card processor which shows whether the transaction should be rejected or accepted. This is called the Address Verification System (AVS), which is a numeric verification system that matches a customer’s information with their information on files at the time of card issuance.

Let’s suppose a situation where AVS can help prevent fraud. For instance, a customer forgets their credit card on a store counter while checking out. Someone else comes and picks it up with the intention to use it for online shopping. Though the thief now has a real credit card with a CVV security code on the back, they don’t know the address of the cardholder. If the online ecommerce site asks for address verification for a transaction, it will stop a fraudulent purchase from going through.

1. **Buy an Insurance for Cyber Liability**

Even if you don’t store customer’s private data, there is still a chance of breach of data and leakage of personal information. This can have legal consequences for you as a business and this is why, in addition to good security practices, it’s a good idea to invest in cyber liability insurance. It can help you reduce the financial impact on the company and bear resulting legal costs.

Cyber liability insurance is a policy which is designed for malicious attacks, data breaches and all other threats related to cybersecurity. It primarily aims to protect the merchants but can also provide assistance to clients interacting with the merchant. Generally cyber liability insurance provides first party coverage and third-party coverage. The former covers loss suffered by the business whereas the latter covers loss incurred by people directly affected by the incident.

Some insurance policies also include services of risk mitigation for preventing cyber-attacks. The insurance service provider assists in evaluating policies and hardware/software for vulnerabilities. Other insurance policies can also cover fraud prevention or credit monitoring before or after an incident and extend their services to providing helpline for customers in effect of a breach.

1. **Educate Your Customers to Keep them Informed**

Even with all the online security measures in place on your part, it is highly likely that a careless customer compromises your business’s security. In fighting against cyber-crimes, experts believe that for business the consumers are often the weakest link in a security system. It is actually true that the online behavior of many consumers puts them at risk of being victim of a cyber fraud. However, in most cases consumers are not even aware of what is a risky online behavior. Therefore, it is very important to keep your customers well-informed about the possibilities and prevention. This can be shared with customers using a monthly newsletter or posting it on the website.

But even if businesses provide useful information to customers regarding safe usage of their credit cards, a mere list of tips lacking concrete solutions is not of much help. To truly engage a customer in the process, the need to create interactive and interesting content which takes them through step-wise experience and makes it easy for them to understand and implement secure online purchasing.

**Final Thoughts**

Businesses need to put in a lot of effort and energy to ensure smooth and safe online payments. Still then, you need to monitor the data to look out for any loopholes. Watch very closely for potential threats or any suspicious activity and react promptly should such a situation arise. Also work with reputable companies that ensure safe payment processing.