**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 way of ensuring safety of online transactions for a B2B business. The Payment Card Industry Data Security Standards are a set of compliance regulations for businesses involving payment cards. 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 payment 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.

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.

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.

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.

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. 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.

**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.