Cultural Daily

Independent Voices, New Perspectives

Detecting fraud in your online business before it happens

Our Friends · Tuesday, January 18th, 2022

As a business owner, you will do anything you can to grow your business and make it as successful as you know it can be. You will hire the employees that are a perfect match for it, and you will do the market research to find out who your targeted customers are and how to reach them. Of course, you won't forget about your competition, so you will research who your competitors are and how to get the upper hand. Surprisingly, while most businesses consider this a standard practice, they don't consider including cybersecurity efforts in their everyday business operations.

Most of them still believe they won't become victims of cyber fraud as they are not big enough to get noticed by the cybercriminals. Sadly, that might've been true in the past, but no longer. Cybercriminals will attack any business regardless of the size if it can make them a profit, and they can find profit just about anywhere. For example, in addition to exploiting the business and stealing its money, they can also access confidential details about the business and customers to use for their benefit. There is profit to be made from selling that data on the black market or using it for account takeover fraud, or even applying for a loan. The fraudster will keep getting more creative and sophisticated and find new ways to exploit business. Luckily, if you follow tips by SEON on eCommerce fraud, you will be able not only to detect fraud but also prevent it from damaging your business.

What is eCommerce fraud?

Ecommerce fraud covers various types of fraud whose aim is to target e-commerce stores and their customers and exploit them for their financial gain. The most common types of eCommerce fraud are:

- Transaction Fraud
- Friendly Fraud
- Triangulation Fraud
- Chargeback Guarantee Fraud
- Return Fraud

Other than the return fraud, all other types of fraud ultimately end with the chargeback request from a card owner. A chargeback can be highly damaging to the business as merchants will lose the item while needing to pay a chargeback fee in addition to reversal of payment. It can even result in merchants' account providers increasing their fees or closing their accounts altogether as they consider them high risk.

How to detect fraud?

Fraud is an ever-present threat all businesses need to deal with. By keeping an eye on the following red flags, you will be able to detect fraud before it can cause any significant damage and take necessary action.

- Differences in order data
- Order larger or smaller than usual
- Unexpected user location
- Several declined transactions on the same account
- Multiple failed login attempts
- Multiple shipping addresses
- Several shipping addresses used
- Using several different cards on one account
- Various transactions made in a short timeframe through one account
- Multiple orders from a country you don't usually receive orders from.

How can you protect your business from eCommerce fraud?

Now when you know the red flags you need to be on the lookout for, you are already one step closer to protecting your business from fraud. By implementing the following advice, you will minimize the risk and avoid becoming a victim.

1. **Security audits.**

They need to be performed regularly to ensure you discover any flaws or vulnerabilities in your network. These issues can be fixed as soon as you discover them, preventing the fraudsters from exploiting them.

2. **Educate your employees**

Employees are one of the most significant risk factors any company can have, which is why it is essential to educate them about the dangers they might be facing and effective ways of dealing with them. From dangers of oversharing on social media, to the importance of good password hygiene or knowing how to recognize suspicious emails, well-informed employees are vital in protecting the business.

3. **Ask for a CVV with every transaction**

While fraudsters can get access to your card details in various ways, CVV or Card Verification Value number is a bit harder to get. This is why asking for it gives you a unique opportunity to increase the chances of dealing with an actual card owner with a physical card present.

4.Update your cybersecurity protocols

By implementing cybersecurity protocols and keeping them up to date, you will reduce the risk of fraud significantly. Tools such as device fingerprinting, data enrichment, or email lookout tools help you minimize the risk of fraud as they can detect it before it even happens.

Photo by mohamed_hassan on Pixabay

This entry was posted on Tuesday, January 18th, 2022 at 4:55 am and is filed under Check This Out
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.