Received: 03-03-2024
Accepted: 13-04-2024

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

E-Commerce Security in Vietnam, Current Situation and Solutions

[1] Pham Thi Thu Thuy, [2] Pham Thuy Duong
[1] Department of Business Administration, University of Labour and Social Affairs, Vietnam
[2] Foreign Trade University, Vietnam

Corresponding Author: **Pham Thi Thu Thuy**

Abstract

The digital technology age has helped e-commerce grow stronger, which means that issues of security and network security for e-commerce platforms need to be given special attention. According to data from Juniper Research, in the period 2021-2025, the total losses that businesses will suffer from online payment fraud will reach 206 billion USD. This is just one of many ways that hackers frequently use to attack networks in the e-commerce industry. To minimize risks and prevent cyber attack methods, within the scope of this article, the authors have introduced the concept of e-commerce security, clarifying the threats to e-commerce, analyzing Analyze the current state of e-commerce security in Vietnam, thereby suggesting solutions to ensure e-commerce security.

Keywords: E-Commerce, E-Commerce Security, Security

1. Introduction

In Vietnam, the concept of e-commerce just appeared not long ago. The legal basis regulating e-commerce activities in Vietnam was born quite late compared to many countries in the world. At the end of 2005, Vietnam had the "Electronic Transaction Law" and in 2006, a Decree was issued guiding the implementation of this law. The Internet is increasingly popular in the world along with the advent of many modern technologies, causing e-commerce to grow strongly and be increasingly widely applied. Not only that, but e-commerce also helps us solve essential and urgent needs in areas such as electronic transaction systems and electronic payments, but its actual operations also create benefits. Benefits and efficiency that traditional commerce cannot bring such as saving on travel and advertising costs (through online buying and selling or online bidding through websites such as ebay, amazon, chodientu.com). Because of these huge potentials, e-commerce is playing an increasingly important role in the world economy.

In our country, although e-commerce is only in its early stages, it really brings significant benefits to the economy. This is also one of the means to help us integrate into the world economy. However, along with those benefits come risks when doing e-commerce business. According to Associate Professor, Dr. Dinh Trong Thinh - Economic expert at the Academy of Finance, when the application of digital technology in businesses develops rapidly and the number of electronic transactions increases rapidly each year, the issue of ensuring Security in electronic transactions and data security have become increasingly urgent to protect system safety and customer data [1]. Therefore, e-commerce security is an important issue that needs to be studied.

2. General issues of e-commerce security

2.1 Concept

E-commerce is a form of buying and selling goods and services online global computer. E-commerce is becoming a business method that brings many benefits to humanity based on the rapid development of technology industries, first of all information technology. E-commerce, therefore, becomes a representative business method for the knowledge economy.

E-commerce security is the process by which businesses minimize and limit risks that may occur in their e-commerce activities. Security in business e-commerce involves issues such as: Procedures, policies, laws and especially technology.

2.2 Threats to e-commerce security

+ Hackers and Crackers: Hackers is a term used to refer to programmers who seek unauthorized access to computers and computer networks. Crackers are people who find ways to crack passwords to gain unauthorized access to computers or programs.

+ Credit card fraud: In traditional commerce, credit card fraud can occur such as: Lost or stolen credit card, card number information, PIN code, customer information disclosed and used illegally. In e-commerce, fraud acts are more complex such as card-related information or transaction information being stolen.

+ Fraud: Fraud in e-commerce is when hackers use fake email addresses or impersonate someone to commit illegal actions. Phishing may also involve changing or redirecting web links to a fake web address.

+ Types of cyber attacks:

Technical attacks are software attacks performed by experts with good system knowledge.

Social engineering is the practice of trying to trick people into obtaining sensitive information.

Denial-of-service (DoS attack) is the use of special software that is continuously sent to the target computer, causing it to become overloaded and unable to be served.

Distributed denial of service (DDoS attack) is a denial of service attack in which the attacker has illegal access to multiple machines on the network to send data. dummy to target.

Man in The Middle Attack. This is an attack where hackers secretly relay and alter communication between two parties. For example, hackers eavesdrop on information taking place between customers and a company's online store to take advantage of customer data and sabotage business operations. Hackers will easily take advantage of users connecting to unsafe wifi networks to attack.

Spam (junk mail): Every day you can receive dozens or hundreds of spam emails.

A virus is a computer program that can self-replicate and spread: Takes up resources, slows down computer processing speed, can delete files, reformat hard drives, etc.

Worms: Computer worms differ from viruses in that worms do not penetrate files but penetrate the system.

Bots: Some hackers will attack and develop bots with the purpose of scanning our websites and stealing information about inventory and prices. Usually, unfair competitors in the market will use this method of security attack in e-commerce to edit displayed goods with lower prices to lower the victim's revenue level.

According to Techopedia statistics, in 2022, the world will have a total of 493.33 million ransomware attacks, phishing is still the most common cyber attack with about 3.4 billion spam emails daily, the cost The average loss due to a data breach is $4.35 million, the average cost of damage due to stolen or compromised credentials is up to $4.5 million [4].

3. Current status of e-commerce security in Vietnam

E-commerce is growing proportionally with the increase in many cybersecurity threats, including those affecting private information, data ownership and management, location of data centers, data security and law. Thirty years ago, only 32% of market value was based on intangible assets, mainly intellectual property. To date, this number is 80%, requiring businesses to carefully protect digital assets against the risk of being stolen by criminals. According to data from Juniper Research, in the period 2021-2025, the total losses that businesses will suffer from online payment fraud will reach 206 billion USD.

Vietnam's e-commerce market is currently dominated by foreign businesses. Notably, some businesses start out as Vietnamese businesses, but when successful, they are acquired by foreign countries or controlled by foreign legal entities. Typically, Tiki floor is a native Vietnamese floor. By the end of 2020, foreign capital on this floor accounted for nearly 55%, by 2021 this floor will transfer 90.5% of its shares to the Singaporean legal entity Tiki Global. Thus, Tiki has become a Singaporean enterprise. Similarly, Sendo started as a Vietnamese enterprise, but by the end of 2020, foreign capital on this floor had reached more than 65%. Thus, among the four largest e-commerce trading floors in the Vietnamese market today, there are up to 03 e-commerce trading floors with foreign investment. The market dominance of foreign e-commerce platforms is reflected in the number of visits. According to February 2022 data, the total number of visits on Shopee is 78.5 million, on Lazada is 14.8 million, on Tiki is 14.1 million and Cho Tot (Vietnam) is 12.7 million times. In the ranking of mobile applications (Android, iOS) for shopping in Vietnam, Shopee is also the most used application, followed by Lazada and Tiki [2]. Besides, popular social networking platforms are also gradually encroaching on e-commerce activities and online transactions. Typically Facebook, Google, Netflix, Youtube, Amazon, TikTok. These platforms allow displaying ads to buy and sell goods and products, and can be bought and sold through links with e-commerce platforms, or integrated Directly post product purchases and sales on these platforms. Thus, with a large percentage of dominating the e-commerce market, foreign-owned e-commerce platforms not only have large revenues in the Vietnamese market, but also hold a large amount of data of Vietnamese people, from information markets. Basic information such as name, age, address, phone number related to information about shopping behavior, preferences, habits and living standards of Vietnamese people. This is a huge risk to network safety and security.

In fact, many businesses are not aware of safety and security issues in e-commerce. A survey and assessment of the information security situation of e-commerce websites with high brand recognition and a large number of visitors has shown that in Vietnam, there are still about 1/3 of The e-commerce website system currently operating in the market has a serious error. This rate corresponds to millions of users who are at risk of losing their information security. This is causing many customers to gradually feel worried and lose confidence when performing e-commerce transactions. The cause of this loss of trust comes from the fact that the world's major electronic websites are constantly being attacked, causing customer accounts to be stolen. EBay's e-commerce security story is an example. This online shopping site with hundreds of millions of users globally suffered a major data breach affecting 145 million registered members around the world, after the website's database was attacked [3].

In Vietnam, along with the strong growth in the number of Internet users, especially online shopping, cyber attacks are increasing, both in number and scale; more sophisticated forms of attack. According to a report published by the Ministry of Public Security, in Vietnam many websites and network systems have not been built according to a unified standard, lacking verification of information security and network security; software and hardware devices that have security vulnerabilities but have not been promptly resolved; The use of unlicensed software is still common. Many organizations do not have a complete cybersecurity policy;

There is no or specialized department responsible for ensuring network information security and safety, but it does not meet the requirements in the current situation. The Vietnam Computer Emergency Response Center has recorded and handled nearly 10,000 website attacks. Of these, nearly 50% of incidents come from spreading malicious code through security holes.

Vietnam aims to have 55% of the population participate in online shopping by 2030, with the value of online purchases of goods and services reaching an average of 600 USD/person/year; B2C e-commerce sales increased by 25%/year, reaching 35 billion USD, accounting for 10% of total retail sales of goods and consumer service revenue nationwide; strive to reach over 40 - 45% of small and medium-sized enterprises operating in the commercial sector participating in major domestic and foreign e-commerce platforms [1].

For e-commerce businesses, they need to protect themselves by ensuring the security of computer systems, data related to products, warehouses, customers, servers and client data encryption. Businesses need to take the following steps: (1) Assess the level of risk; (2) Develop e-commerce security policies; (3) Set up security monitoring points; (4) Security check; (5) Maintain an emergency reporting system.

4. Solutions for e-commerce security

Along with e-commerce activities, the issue of e-commerce security is also a problem for all businesses doing business on online platforms because hackers can attack at any time and cause damage. Many losses are unpredictable. Therefore, businesses must be clearly aware of the problem and implement solutions to protect e-commerce security, specifically.

+ Set up HTTPS and SSL certificates for websites, especially websites that handle sensitive information like payments or contact numbers. The HTTPS protocol is an extension of HTTP, better known as HTTP over SSL. HTTPS helps identify the website users visit, protecting data privacy and security. At the same time, the method also helps increase website rankings on Google search pages. Compared to HTTP, HTTPS will help websites face less risk of cyber attacks.

+ Anti-intrusion and DDOS service attacks: A DoS denial of service attack is an activity that brings down a server or network, making it impossible for other users to access that server or network. This solution helps businesses prevent and detect intrusions (IPS), preventing comprehensive attacks from DDOS. Through this solution, businesses detect early and quickly prevent DDOS attacks. Through the process of analyzing data streams, the system will detect unusual behaviors and immediately prevent the objects causing this problem.

+ Use firewalls: Firewalls create a comprehensive security layer for e-commerce website systems, helping businesses avoid XSS, SQL Injection and many other cyber attacks by hacker. Using a firewall also helps businesses control all traffic to their website, ensuring only trustworthy traffic can click through.

+ Use anti-malware software: This is a program that helps businesses detect, remove and prevent malicious code from infecting computers and network systems. Because malware is a general term, including viruses, worms, trojans, etc., using anti-malware software will help companies prevent many dangers from hackers.

+ Website and server security: Currently, we have many ways to secure websites and servers. One of the ways is that website administrators need to use complex passwords and change them regularly. In addition, businesses need to decentralize website administration according to the roles of each management and employee level to minimize the risk of data loss or leakage. In addition, we also need to set up alerts when any strange or suspicious IP is trying to access our e-commerce website.

Besides, businesses can also use third parties for security and network security management. Businesses can use the company SecurityBox. SecurityBox will act as a supervisor of the business's website. The solution helps ensure 24/7 safety for the website. The device paints an overall picture of the cybersecurity status of the business website; Helps businesses get a visual view of the strengths, weaknesses, vulnerabilities and cyber security risks that exist in that website. In addition, the device also offers solutions to help overcome existing vulnerabilities. Finally, there is the function of periodically reporting on the network security status of the website.

+ Online payment gateway security: Businesses should choose reputable third-party payment solution providers to process transactions from the website, avoid arbitrarily storing credit card-related data information. of cutomer. This ensures minimizing risks related to online payments and protecting customer information. Businesses can choose AppotaPay Payment Gateway, this is a comprehensive payment solution, helping businesses grow revenue and access international markets most easily, with the following advantages: Diversifying domestic payments and international; Convenient integration via website and mobile application; Processing 350,000 transactions/minute; Friendly and clear management system helps businesses easily operate and control; Support 24/7, timely support for technical problems. AppotaPay brings new technology solutions, leading the "cashless payment" trend, suitable for both B2B and B2C customers.

+ Data backup: This is a simple but effective solution against attacks or security risks for e-commerce. Whenever your website has problems that cannot be resolved with normal rescue measures, you can restore the backup to continue serving users. The difficult problem when backing up data is choosing a solution that is suitable for the scale of the business and can easily scale up when necessary. AmazonWeb Service's backup service will solve this problem for most businesses. Besides, it is also necessary to perform offline backup as a backup plan when the worst case scenario occurs.

+ Update hardware and software: Always update versions of technology components such as: Workstation-server operating system, browser, software, hardware, NAS, content management platform, website …This will help businesses avoid cyber attacks through third-party vulnerabilities.

+ Raise awareness related to e-commerce security for employees: Shark Pham Thanh Hung in the Shark Tank Vietnam program correctly pointed out the biggest security risk in technology in general and security in particular, which is people. Even when an e-commerce business is equipped with a solid defense system, just one mistake by an employee during operation can cause hackers to penetrate the organization and cause destruction. That is why organizing short-term training classes on security and internet usage knowledge is important in enhancing cybersecurity for organizations.

5. Conclusion

Strong technological innovation reminds businesses to pay more attention to e-commerce security, which is one of the burning issues for many businesses today. Hackers can attack using any method, causing a lot of loss to businesses. Preventing security threats will help businesses have a solid foundation and capture more development opportunities. Therefore, understanding clearly what security in e-commerce is and building a solid e-commerce website system from the beginning and regularly updating, upgrading, and maintaining is essential. every business should do to avoid e-commerce security risks.

6. References

1. Vu Le. Ensuring information security in e-commerce transactions, 2022.
2. Phong Lam. risk of losing network security in e-commerce, 2022. https://vietq.vn/nguy-co-mat-an-toan-an-ninh-mang-trong-thuong-mai-dien-tu-d200272.html
3. Current status of Vietnamese e-commerce website security. https://www.matbao.ws/blogs/ban-hang-hieu-qua/thuc-trang-bao-mat-cho-website-thuong-mai-dien-tu-tai-viet-nam.html
4. https://www.techopedia.com/cybersecurity- statistics