Journal of Academic Research and Trends in Educational Sciences
Journal home page:
http://ijournal.uz/index.php/jartes

THE IMPACT OF CYBER THREATS ON E-COMMERCE SITES

Rakhmonov Gayrat Ismatulloyevich[1]

Tashkent University of Information Technologies named after Muhammad ibn Musa al-Khwarizmi

KEYWORDS

Ecommerce, Cyber Threats, Hacking. Encryption, Firewalls, Digital Signatures, DDOS Attacks, digital economy, Phishing, electronic, internet, network, Password, technology, innovation, Security, resource, communication, demand, information, communication, platform, process, services, activity, infrastructure, dynamics, segment, classic, analysis, indicator, telecommunication, parameters, skills, statistics, mobile communication, base, station, content.

ABSTRACT

Today, the Internet has penetrated almost every corner of the world and has become a popular means of communication and information search. Various organizations and companies are using the internet to introduce and promote their products and services, which has introduced the concept of E-commerce. E-commerce is basically the purchase or sale of goods and services by consumers and e-commerce organizations over the Internet. E-commerce provides an economical and efficient way to do business on the Internet. This article discusses e-commerce, cyber threats to e-commerce sites, and the impact of these threats on e-commerce sites.

2181-2675/© 2022 in XALQARO TADQIQOT LLC.
DOI: 10.5281/zenodo.7220788

[1] Faculty of Economics and management, Tashkent University of Information Technologies named after Muhammad ibn Musa al-Khwarizmi, Uzbekistan (raxmonovgayrat82@mail.com)

iJOURNAL Journal of Academic Research and Trends in Educational Sciences (JARTES)
VOLUME 1, ISSUE 10 / ISSN 2181-2675

KIBER TAHDILARNING ELEKTRON TIJORAT SAYTLARIGA TA'SIRI

KALIT SO‘ZLAR:
elektron tijorat, kiber tahdidlar, xakerlik. Shifrlash, xavfsizlik devorlari, raqamli imzolar, DDOS hujumlari, raqamli iqtisodiyot, fishing, elektron, internet, tarmoq, parol, texnologiya, innovatsiya, Xavfsizlik, resurs, aloqa, talab, axborot, aloqa, platforma, jarayon, xizmatlar, faoliyat, infratuzilma, dinamika , segment, klassik, tahlil, indikator, telekommunikatsiya, parametrlar, malakalar, statistika, mobil aloqa, baza, stantsiya, kontent

ANNOTATSIYA

Hozirgi kunda Internet dunyoning deyarli barcha burchaklariga kirib borgan va mashhur aloqa va axborot qidirish vositasiga aylangan. Turli tashkilot va kompaniyalar o‘z mahsulot va xizmatlarini joriy etish va targ‘ib qilish uchun internetdan foydalanmoqda, bu esa E-tijorat tushunchasini joriy qildi. Elektron tijorat asosan iste’molchilar va elektron tijorat tashkilotlari tomonidan Internet orqali tovarlar va xizmatlarni sotib olish yoki sotishdir. Elektron tijorat Internetda biznes yuritishning iqtisodiy va samarali usulini taqdim etadi. Ushbu maqolada elektron tijorat, elektron tijorat saytlariga kiber tahdidlar va bu tahdidlarning elektron tijorat saytlariga ta’siri muhokama qilinadi.

INTRODUCTION

E-commerce websites help to facilitate business and provide a platform to spread the business to every corner of the world. With the help of e-commerce, an organization can expand its business to national and international markets with minimal investment. An organization can easily connect with more customers, suppliers and best business partners worldwide [1]. This tremendous growth in the popularity of e-commerce has led to a new generation of related cyber threats.

Cyber threats to E-Commerce sites

Now the Internet has become a tool to do several transactions online. Its continued availability and ease of use make it the most popular marketing and commercial tool. E-commerce website security is a dynamic process with new threats emerging every day. In today's competitive world, e-commerce systems must maintain customer trust, for which proper planning must be done to protect the system from potential security threats. A secure e-commerce application should have the following five security features:

- Authentication: Authentication establishes proof of identities. It helps in ensuring that the source of an electronic document or message is identified correctly
- Integrity: The integrity of message is lost, when the sender sends the message but its contents are modified before reaching the intended recipient. Integrity of message must be intact i.e. message must not be manipulated during transition [2].
- Non repudiation: It is a situation where the sender denies later on that the message was not sent by him/her. It does not allow the sender of a message to deny the sending of that message.

- Access control: Access control determines who has the access of what, because from the security perspective not just everybody can have the access of system [16].
- Availability: Availability ensures that the resources are available to authorized persons at all times [3].

Every electronic system that supports e-commerce is largely vulnerable to abuse and threats:

Fraud

Direct financial loss associated with fraudulent activity. Financial records may simply be destroyed or funds may be transferred from one account to another [4]. Fraud isn't just about credit card payments, criminals are using malware to manipulate online transactions via computers, phones and tablets. They steal bank account information to make fraudulent payments.

Identity theft. This is the most common type of fraud that concerns businesses. This is where credit cards are targeted by fraudsters because it doesn't take much for a criminal to complete a "card not available" transaction. Traditionally, in identity theft, fraudsters conduct transactions using a different identity. Instead of inventing an entirely new identity, they spoof someone's existing identity [5]. It's much easier and faster. Fraudsters use someone's personal information, such as names, email addresses and addresses, as well as account or credit card information, to identify or steal someone's identity. Using this information, they place orders online using a fake name and make payments by debiting someone else's account or using someone else's credit card information. A stolen password is usually all that is needed to spoof someone's identity. This information is used to manage the existing account in the online store, where the information required to make payments is already available on the account. Criminal attacks on e-commerce organizations and theft of customer information fall under the category of fraud.

Friendly fraud. The term is actually a misnomer: consider a scenario where a customer orders goods or services and pays for them directly by debit or credit card. However, he knowingly initiates cashbacks and claims that his credit card or account information has been stolen. He gets a refund - but orders the product. This type of fraud is usually found in services such as adult environments or gambling. Friendly scams are also combined with reshipping. Here, a fraudster who pays for their purchases using stolen payment information uses the middleman's address for shipping, which then ships the goods.

Clean fraud. The idea behind pure fraud is that credit card information is stolen and used to make payments, but the transaction is manipulated to bypass the fraud detection mechanism. There is more to gathering information than a friendly scam. In pure fraud, criminals delve into fraud detection systems and large amounts of information about the rightful owner of stolen cards. This correct information is then provided during the checkout process to bypass the fraud detection mechanism. Card verification is usually done before fraud occurs. The fraudster makes test purchases to see if the stolen credit card information works [13].

Affiliate fraud. There are two types of affiliate scams, and both have the same goal: to get more money from an affiliate program by manipulating signups or traffic statistics. This is done by forcing real people to log into merchant sites using fake accounts or using a fully automated process. This type of fraud is payment method neutral but common.

Triangulation fraud. Triangulation fraud is done through three points. The first is a fake online store that is used to offer highly sought-after goods at very low prices. Often, additional bait is added, for example, if the goods are paid for, then only the goods are sent immediately after the information using a credit card. This fake store collects credit card information and shipping address - that is the only purpose. The second point of the fraud triangle is that the fraudster then uses the stolen name and credit card information to order goods at the real store and then ship them to the original customer. The third point of the fraud triangle is that the fraudster uses the stolen credit card information to make subsequent purchases. This fraud usually goes undetected for a long time because it is very difficult to connect credit card information and order information, which leads to great losses.

Merchant fraud. It is the simplest: fake online stores offer goods at very low prices, but the buyer never ships them. Payments are obviously stored in this fake online store. Such fraud is also found in wholesale trade. It is not exclusive to any payment method, but it is certainly where cashless payment methods are unique.

More international fraud. The difficulty of maintaining international labels for each customer, as well as language barriers, create additional challenges in fraud detection and prevention. The main problem of fraud prevention is the lack of an integrated system that provides a unified view of their transactions across all markets.

Phishing

The term "phishing" first appeared in the hacking tool "AOHell", which included the functionality of trying to steal the financial information and passwords of American Online users [6]. The term is derived from the word "fishing", spelled "phishing", similar to "phreaking", a mechanism for hacking a telephone network. Phishing appeared a few years ago, so it is a relatively recent phenomenon. Now it has become an effective tool with cyber criminals. **Fig. 1.**

Several characteristics of phishing:

- Criminals get Trojan horses installed on targeted machines to collect details.
- Hackers “generate” login details and distribute them to cyber criminals.
- User’s computers are compromised to collect information without their knowledge.
- Vulnerable software cannot prevent user computers from downloading malicious code.

To make the phishing successful, an attacker uses various methods. Some of the common methods are:

- Link manipulation: In this method of phishing, the attacker inserts a link in an email to some website.
- Graphical Substitution: As the user logon to the phishing website, it manipulates the users screen with the help of Java Scripts that alters the address bar by adding the image of requested URL instead of the attacker's actual URL.
- DNS Cache Poisoning: Normal traffic is interrupted by using DNS Cache Poisoning. It makes the Domain Name Server to direct traffic from specified IP address to the fraudster's server IP address [8].
- Filter evasion: In this method of phishing, images are used as links instead if text that makes difficult for the phishing filters to detect.

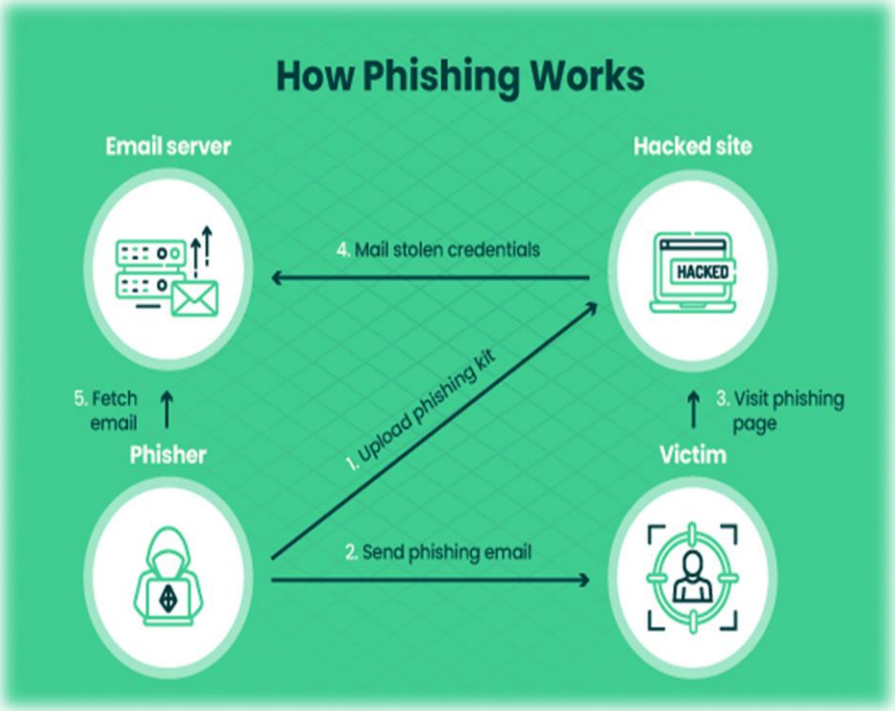

Fig. 1. Phishing and Pharming

Server Threats

The server plays the third connection point in the Client-Internet-Server trio. This trio embodies the E-commerce path between the e-commerce server and the user. Servers are vulnerable and these vulnerabilities can be misused by anyone to cause great harm or someone can collect information illegally.

Database Threats. Every e-commerce system maintains a database that stores user information, and product information is retrieved from this database that is connected to web servers. In addition to product data, databases store valuable and informative data that can cause significant business damage if stolen or compromised. Some databases do not provide great security when storing usernames and passwords. Anyone can log in as an authorized user, or the user can impersonate someone after receiving authentication

information.

Web Server Threats. Web server software serves web pages in response to HTTP requests. As software grows in complexity, so does the likelihood that it will have coding and security holes—security issues that provide doors through which hackers or attackers can gain access to the system.

Common Gateway Interface Threat. CGI transfers data from a web server to another application, such as a database. A common gateway interface and the software they transmit information to provide web pages with active content. If misused, CGI has a high potential to pose a security threat, for example, CGI scripts on web servers can be configured to run with unrestricted privileges. CGIs that contain some bugs or malicious code can access system resources, freeze or crash the system. These malicious codes or flaws invoke privileged core system programs that can then delete or modify files or view sensitive user information, including usernames and passwords.

Password Hacking

Password cracking is the simplest attack against a password-based system and involves guessing passwords. Guessing passwords requires access to three attributes:

- Complement.
- The complementation functions.
- The authentication functions.

If none of these attributes are changed before password guessing is complete, a hacker can use the password to gain access to the system [9].

Cyber Crime and Ecommerce

In the past few years, the definition of how we do business activities has changed a lot. Market has changed their faces to online business using internet which further attracts number of cyber criminals there by. Organization are very comfortable adopting e-commerce but on same side worried about security and number of risks involved. As we all know e-commerce works differently as of traditional commerce, so chances of frauds are more in this as physical presence is not there. Though number of businesses are attracting towards ecommerce rate of cyber crimes are also increasing proportionally to that and percentage is large in India specially. Government should take serious initiatives to overcome the challenges being faced by cyber crimes otherwise it will extremely affect our online business trends. Chances of frauds are more in India because e-retailing is in first stage buyers are new they lack awareness and get easily fooled. Cyber cheaters are using the fake websites like the original ones to fool the buyers. Cases are also registered in which buyers getting the wrong, false, damage delivery of products in comparison to what they have shown and described on their websites. In some cases, sellers are also involved in such bad activities by making the false complaints and gaining benefits out of that. Amazon, Flipkart are the big giants in e-commerce industry has registered such kind of cases. Table 1.

Table 1: The Summary of Cyber Crime categories according its target

Target	Cyber Crime	Method
Against individual	Email spoofing	Email
	Spamming	Ads
	Phishing	Fake emails
	Botnet	Sends the instructions to another computers
	Netspionage	Hack into individual PCs
	Cyber defamation	Websites or sending emails
	Harassment and cyber stalking	Emails, posting messages on bulletin boards, chat rooms, user net groups
Against property	Credit Card Fraud (CCF)	Unlawful online getting of a credit card number
	Intellectual property crimes	Software hacking, illicit programs copying, distribute of copies of software illegally
	Copyright infringement	Reproduce right or the copyrighted perform work
	Trademarks Violations	Attaching to a trademark with unauthorized of the trademark owner or any licensees
Against society	Forgery	Forged by usage the high-quality scanners and printers and computers
	Cyber Terrorism	Terrorists trigger virtual devastation in online computer systems.
	Web Jacking	Hacking
Against organization	E-bank theft	Hacks into the system of banking
	Unauthorized Accessing of Computer	Hacking
	Denial of Service (DoS)	Viruses, email barrages
	Computer Contamination	Virus attack and Worm attack
	Email Bombing	Emails
	Logic Bomb	Event dependent programs
	Trojan Horse	Unauthorized program and working from an inside authorized program

E-Commerce security tools

Following security features must be there for a secure e-commerce system (Figure 1):

- Public Key Infrastructure.
- Passwords.
- Encryption Software.

- Biometrics: Retinal scan, finger prints, Voice etc.
- Firewalls: Software and Hardware.
- Locks and Bars
- Digital Certificates
- Digital Signatures.

Fig. 2. Word cloud for security tools of e-commerce

Cybercrime is committed by fraudsters or intentional actions of internet users and takes advantage of the availability and ease of use of the internet. This poses serious threats to the integrity, quality and security of most organizational information systems, and therefore the development of effective security mechanisms becomes a priority. Cybercrime involves the use of computer resources to commit illegal or unauthorized acts [12]. Organizations that provide goods and services online can be severely affected if an E-commerce website is compromised. Fig. 2.

Significant business consequences of a security incident may include, but are not limited to, the following:

- Subsequent loss owing to adverse publicity.
- Criminal charges if that site is found to be in breach of the regulatory requirements or relevant personal data privacy laws.
- Internet fraud is costly and affects brand.
- Market share is lost if customer confidence is impacted.
- Direct financial loss as a result of fraud.

Payment Gateway Security

While it may make processing payments more convenient, having credit card numbers stored on your database is a liability. It's nothing less than an open invitation for hackers where you put your brand's reputation and your customer's sensitive information on the line.

If you fall victim to a security breach, and hackers get their hands on credit card data, all you can do is to say goodbye to your business because the heavy fines will force you into bankruptcy.

In order to save your business from this terrible fate, you should never store credit card information on your servers and ensure your payment gateways security is not at risk. Additionally, you can use third-party payment processing systems to carry out the process off-site. Popular ecommerce payment processing options include PayPal, Stripe, Skrill, and Wordplay.

When it comes to ecommerce recommendations, you must obtain a Payment Card Industry Data Security Standard (PCI DSS) accreditation.

Secure your website with SSL certificates

You can fortify your security by using various layers of security. You can use a wide-spread Content Delivery Network or CDN to protect your site against DDoS attacks and malevolent incoming traffic. They do so by utilizing machine learning to filter out the malicious traffic from regular traffic.

You can also use two-factor authentication to squeeze in an additional layer of security. Two-factor authorization requires a standard username and password combination as well as an extra code that is sent as an email to the user or as an SMS to their provided phone number. This ensures that only the user can access the service even if their username and password are at risk.

Educate Your Clients

Some lapses in security don't happen at your end but your client's. They might be using weak passwords or they might deliver sensitive information on phishing sites and in the hands of hackers.

You can solve these ecommerce security threats by educating your customers. Educate them about the risks associated with unsafe security practices. You can demand strong passwords and introduce them to how phishing works.

Strong passwords require a good combination of characters, symbols, and numbers that are near-impossible to brute-force or guess. You can also keep users away from creating profiles with weak passwords. You can also adopt the two-factor authentication system in case they are using weak passwords. Or if the user submitted information is sensitive and susceptible to hacking.

Give these approaches due consideration because some customers might consider them a hassle and might just leave your website altogether. Do ensure that you aren't making your customers jump through unnecessary hoops.

Or you can bypass this whole process and simply let them sign up via Facebook or Google which offer world-class cyber security.

Ransomware and DDOS Attacks Against E-commerce

A recent Sophos report shows that 44% of retail organizations were hit by ransomware in the last year, and 54% of these attacks were successful, and customer data was encrypted. Almost one-third of the companies whose data was encrypted paid average

ransomware of $150K, but they only got back two-thirds of their data on average.

The average bill from recovering from a ransomware attack in the retail sector (downtime, people time, device cost, network cost, lost opportunity, ransom paid, and more) was US$1.97 million

Denial of Service is a cyber-attack allowing threat actors to render the website unusable for legit users by sending an overwhelming traffic volume. In the case of a distributed denial of service (DDoS) attack, multiple sources, multiple bots from untraceable IP addresses send constant traffic to the target server to crash.

As a result, it could cause business disruption, which could significantly bother during the peak business periods. Threat actors use DDoS attacks to put pressure on ransomware victims or as an extortion tactic.

In February 2020, Amazon Web Services defended against a DDoS attack with a peak traffic volume of 2.3 Tbps (Terabits per second), the largest ever recorded. Amazon said that the attack was mitigated by AWS Shield, a service designed to protect customers of Amazon.

CONCLUSION

The growth of the Internet and various technologies has made E-commerce functions faster and easier. Today, a huge number of transactions are carried out through e-commerce and a large amount of data is stored. Therefore, e-commerce security is a major concern and better security can only be ensured if we know more about threats and fraud.

REFERENCES

1. Arti, Sunita Choudhary, and G. N. Purohit. “Role of Web Mining in E-Commerce.”.

2. Kidane, Teklehaimanot Tadele, and R. R. K. Sharma. “Influence of culture on E-commerce and vice versa.”

3. Udo, Godwin J. “Privacy and security concerns as major barriers for e-commerce: a survey study.” Information Management

& Computer Security 9.4 (2001): 165-174.

4. KOHLI, GAUTAM. “E-COMMERCE: TRANSACTION SECURITY ISSUE AND CHALLENGES.” CLEAR International

Journal of Research in Commerce & Management 7.2 (2016).

5. Maurya, Santosh Kumar, and NagendraPratap Bharati. “Cyber Security; Issue and Challenges in E-Commerce.” PARIPEX- Indian Journal of Research 5.1 (2016).

6. Jarnail Singh- ‘Review of E-Commerce Security Challenges’. International Journal of innovative Research in Computer and

Communication Engineering, 2014.

7. Mathew, Alex Roney, Aayad Al Hajj, and Khalil Al Ruqeishi. “Cyber crimes: Threats and protection.” 2010 International

Conference on Networking and Information Technology. IEEE, 2010.

8. McCrohan, Kevin F. “Facing the threats to electronic commerce.” Journal of Business & Industrial Marketing 18.2 (2003):

133-145.

9. Lokhande, Prashant S. “E-Commerce Applications: Vulnerabilities, Attacks and

Countermeasures." (2013).

10. Niranjanamurthy, M., and DR Dharmendra Chahar. "The study of e-commerce security issues and solutions." International

Journal of Advanced Research in Computer and Communication Engineering 2.7 (2013).

11. Leena, N. "Cyber Crime Effecting E-commerce Technology." Oriental Journal of Computer Science & Technology 4.1 (2011).

12. Statistics, Cyber Attacks. "Hackmageddon." Avaialble online: http://hackmageddon. com/category/security/cyberattacks- statistics (2015).

13. Cashell, Brian, et al. "The economic impact of cyber-attacks." Congressional Research Service Documents, CRS RL32331 (Washington DC) (2004).

14. Ghosh, Anup K. E-commerce security: weak links, best defenses. Wiley, 1998.

15. Lallmahamood, Muniruddeen. "An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of this on their Intention to Use E-commerce: Using an Extension of the Technology Acceptance Model." Journal of Internet Banking and Commerce 12.3 (2007)

16. Kim, Dan J., Charles Steinfield, and Ying-Ju Lai. "Revisiting the role of web assurance seals in business-to-consumer electronic commerce." Decision Support Systems 44.4 (2008): 1000-1015.