Shodhak : A Journal of Historical Research
ISSN : 0302-9832
Volume: **53**, Issue: **02**, No: **06**, May - August : **2023**

CYBER SECURITY - A PREDOMINANT KEY FOR E-COMMERCE BUSINESS

Mrs. S.Suruthi M.com.,Research scholar , **Dr.R.R.Vishnupriya,** Assistant Professor and Research supervisor, Department of commerce and Research Centre,Sourashtra college,Madurai-625004

ABSTRACT

Nowadays, Global business has changed their phase from physical markets to online businesses. E-commerce has grown significantly during the past few years and regarded as a powerful tool for business transformation. The Business concerns have modernised their supply chain processes, expanded their network to global level, and offer better services to both suppliers as well as customers. Under these circumstances, huge data are generated and stored in Internet service. Security issues are the most important issue for everyone during Electronic business process. This massive increase in e-commerce has created a new generation of related security solutions. Cyber-attack is stealing data from online using advanced methods. In e-commerce, businesses or firms should be cautious while handling his customer's personal information and their own. This study briefs importance of cyber security to detect, prevent, and predict cyber-attacks on virtual machines.

KEYWORDS: E-Commerce, Cyber-attack, Cyber security, suppliers, customers

INTRODUCTION

Online purchasing replaces traditional method of shopping across the world. E- commerce sites like Amazon, Flipkart, eBay, Alibaba, Indiamart and others are paving theway for these technological changes. The most determined innovation currently being made to business is online shopping. E-commerce is well known as a powerful tool for business transformation that gives organisations the chance to modernise their supply chain processes, expand their network to global level, and offer better services to both suppliers as well as customers. Without a well-organized working of E-commerce security, it is not possible to apply the methods of online purchasing that produce such benefits. The prominent website's concern is to find a secure way to use computer to purchase and sell items or move money beA secure, efficient, and fast online payment system was designed to ease e-commerce. E- commerce use wide networks to carry out a number of crucial transactions. Cybercrime brings risks to e-commerce transactions, which result in theft of huge data and financial losses.The possibility of crimes may be performed without the victim's knowledge or consent makes the future even more disturbing. Future cybercrime prevention will involve strong digital security rather than simple human care. Due to different technological assaults of people's privacy, the role, function, and effectiveness of law in reducing cybercrimes havebeen questioned in recent years.

OBJECTIVES:

- To study the nature of cyber-attack in E-commerce businesses
- To understand E-commerce operation and need for cyber security in current trend
- To determine the prevention of Cybercrime on E-commerce business

RESEARCH METHODOLOGY:

The study focused on secondary data and gathered from various published resources, journals, economic reviews, books and websites about cyber security in E-Commerce businesses.

CYBER ATTACKS IN E-COMMERCE BUSINESSES – AN OVERVIEW:

Cyber-attack is referred as an attempt to snatch of systems, illegal access, misuse of network that has been seized to launch further attacks. The various techniques used by cybercriminals to execute a cyber-attack include are Malware attack, Phishing attack, Man- in-the-middle (MITM) attacks, & others.

VARIOUS TECHNIQUES OF CYBER-CRIMES:

1. MALWARE ATTACK

Malware attack invades a server by making use of vulnerability, frequently when the user clicks any suspicious link or email notification that frequently stimulates the installing of hazardous software.

2. PHISHING ATTACK

Phishing is referred as redirecting misleading notifications from a reliable source, usually through email. The purpose of sending is to glide or gather user information, such as details of login & Credit/Debit card details, or attacking the user system with malicious software. Phishing is one of the increasing cybercrime

3. MAN IN THE MIDDLE ATTACK (MITM)

Attacks known as Man-in-the-middle (MITM) or Eavesdropping take place when attackers intervene with something like a transaction between two parties. By jamming the traffic,the attackers can steal and hack data.

These are the two most general points for (MITM) attacks:

- Hackers may position them between a victim's device and the network when using Wireless local area network (WLAN) that's not secure. By this method victim gives the hacker complete data access without even knowing it.
- An attacker makes an attempt for installing spam in victim's device in order to hack their information immediately after malware have infected the device.

4. DISTRIBUTED DENIAL OF SERVICE ATTACK (DDoS)

A denial of-service attack (DDoS) over-burdens system, or the organizations with jamming, using network & other connectivity. Along with these, the system can't satisfy genuinerequest. This assault is likewise carried out by attackers using various hacked gadgets. This is often referred as a denial of service attack.

5. SQL INJECTION

At the point when a cybercriminals embeds suspicious code into a connection that utilizesSQL, and constrains the network to expose data that it will usually don't, this is often referred as aSQL injection. By entering suspicious code into a network on an unprotected site, a cybercriminalscould undoubtedly play out a SQL injection.

6. ZERO-DAY EXPLOIT ATTACK

Later a network exposure is disclosed but prior to a reinforcement or solution is being implemented; a Zero-day exploits attacks. Throughout the process, hackers concentrate on the widely exposed information. Hazard Warning from zero-day helplessness requires continuous observation

7. DNS TUNNELING ATTACK

DNS tunneling refers to abusing of primary DNS protocol. DNS is used to transfer HTTPand other protocol jamming. There are different, acceptable reasons in order to implement the DNS tunneling. They will be used to hide data that is usually shared via an online by masking outward traffic as DNS. DNS requests are changed for malicious purposes to unencrypt data fromvictim computer to network of the hacker. It is also used for calls from the network of the hackerto a victim computer for commanding and controlling.

IMPACT OF CYBER-ATTACK IN E-COMMERCE

When cybercriminals attempt to attain unauthorized access or hacking of online data heldon a computer or network, it is called a cyber-attack. The intention could be to cause harm to a person or business's reputation or steal data for other purposes. Governments, organizations, groups, and individuals may all be the targets of cyber-attacks. Cyber-attacks lead to loss of data,revenue and overall business viability, which makes cyber security essential tool for e-commerce. Cyber-attack is stealing data from online using advanced methods. In e- commerce, businesses or firms should be cautious while handling his information and customer's personal information.

NEED FOR CYBER SECURITY:

Online business usually indulges with huge data transfers and exchange of information in wide, online payments, fund transfers, supply chain management, online marketing and order processing. Therefore, money is transferred and exchanged through online platforms in billions.Cyber security is the important tool need to manage, control and safeguard the information from harmful attacks.

Technical cybercrimes are the most alarming types of cyber-attacks in e-commerce. The purchase section includes selection tabs, shipping details, payment options, and signature verification. So, business should be more cautious on providing a trustable platform for customers while purchasing online. It includesnetwork security, card payment security, application authentication, user provisioning system and mobile security. Securing these services and processes ensures customer confidence when sending money and delivering orders. Strong cyber security protection prevents such attacks.

PREVENTIVE MEASURES ON CYBERCRIME FOR E-COMMERCE BUSINESS:

Organisation should work on taking necessary measures to control cybercrime. Both the Government and Businessesshould offer surety and technical assistance to stop cybercrime activities. Customer should practice only buying in trusted websites in order to avoid being a prey to this electronic scammer. The impact of cyber security on E-commerce can be fully enhanced only when

- Use proper antivirus
- Keep OS software's updated
- Use secured networks
- Secured passwords and login details
- Shop only through trusted websites
- Do not open spam emails sent.
- Do not save card or bank details on websites.
- Change passwords and pin numbers for credit/debit cards frequently.

GOVERNMENT INITIATIVES FOR CYBER SECURITY

Cyber-crimes in India are registered under Information technology (IT ACT) act, 2000 by the Government. The Government of India has enacted current legislations regarding cyber security. The various laws enforcing cyber security are:

I. The Information Technology Act(IT ACT), 2000
II. The Information Technology (Amendment) Act, 2008
III. Information Technology (IT) Rules, 2011
IV. Indian SPDI Rules, 2011 For Reasonable Security Practices
V. National Cyber Security Policy, 2013
VI. IT Rules, 2021
VII. National Cyber Security Strategy, 2020

These are laws being initiated by government in providing safety and security against data theft in E-commerce business. Government law and practise has aided e-commerce businesses in preventing illegal activity and has improved the efficient operation of businesses. This improves the digitalization in India without scam and other malware practices

CONCLUSION:

E-commerce has advanced from traditional marketing patterns to a virtual presence. Many people, especially those involved with e-commerce technology because of its fame on the World Wide Web, have begun to identify cybercrime with fear in recent times. Companies operating in competitive economies are adopting various service methods. With the emergence of e-commerce platforms, data security has become an high cost business, with enormous budgets pouring into securing its operations and databases. Consumer needsand security are top priorities when it comes to e-commerce investments. A endurablee- commerce platform can therefore be attained through solid security framework and effective law. Government law should be made stronger in order to protect India from cybercrime that affects the growing digital economy.

REFERENCE:

https://www.getcybersafe.gc.ca/en/blogs/e-commerce-cyber-security-introduction-online- merchants

https://studycorgi.com/cybersecurity-in-amazon-business-and-its-industry/

https://www.globalsign.com/en/blog/cybersecurity-analysis-why-its-important-your-e- commerce-business

https://zenodo.org/record/3697886#.ZB3KnHZBzIW

https://www.emerald.com/insight/content/doi/10.1108/10662249910297778/full/html

https://infosecawareness.in/cyber-laws-of-india

https://www.ibef.org/industry/ecommerce-presentation

https://www.unisys.com/glossary/what-is-cyber-attack/