International Journal of Advanced Research in Commerce, Management &Social Science (IJARCMSS)
ISSN :2581-7930, Impact Factor : 6.809, Volume 06, No. 01(III), January-March, 2023, pp 79-82

CYBER SECURITY CONCERN IN E-COMMERCE

Dr. Nupur Saboo*

ABSTRACT

Cyber Security is a crucial aspect of modern society that aims to protect computer system, networks, and sensitive data from unauthorized access, theft, damage, or disruption. With the increasing reliance on technology and the internet, cybersecurity has become an essential component of virtually all industries, including, government, finance, healthcare, and transportation. Cyber Security involve the use of various techniques, tools, and practices to identify potential threats, assess risks, and prevent or mitigate the impact of cyber-attacks. These strategies include firewalls, encryption, intrusion detection and prevention, malware detection, and vulnerability scanning, among others. As cyber threats continue to evolve and become more sophisticated, cyber security experts must stay up-to-date with the latest trends and innovations to safeguard against potential attacks. The importance of cyber security is only set to grow as the world becomes increasingly connected, and businesses and individuals rely more heavily on technology for everyday activities.

Keywords: *PCI DSS, IAM, Phishing, Encryption.*

Introduction

E-commerce has grown exponentially over the year, and so has cybercrime. Cyber security is essential to safeguarding the integrity, privacy, and safety of customers and e-commerce businesses. In this research paper, we will explore the cyber security challenges faced by e-commerce businesses and discuss some of the best practices and measures that can be adopted to mitigate them. Cyber security is the practice of protecting computer systems, networks, and sensitive information from theft, damage, or unauthorized access. With the widespread use of digital technology and the internet, cyber security has become a critical issue for individuals, businesses, and government around the world.

Cyber threats come in many forms, including viruses, malware, phishing scams, hacking, and denial-of-service attacks. These threats can cause significant damage to computer systems and networks, resulting in data breaches, financial losses, and reputational damage. To mitigate the risk associated with cyber threats, organizations and individuals need to implement a range of security measures, including firewalls, antivirus software, encryption, and strong passwords. It is also important to stay informed about the latest threats and to regularly update software and system to protect against new vulnerability. Overall, cyber security is a constantly evolving field that requires ongoing attention and vigilance to stay ahead of the latest threats and protect against them effectively.

Cyber Security Challenges in E-commerce

- Payment fraud: Payment fraud is one of the most significant cybersecurity challenges faced by e-commerce businesses. Fraudsters use stolen credit card details to make unauthorized purchases. Payment fraud can be divided into two categories: account takeover fraud and card-not-present fraud.
- Phishing attacks: Phishing attacks are common in e-commerce, and they involve tricking customers into divulging their personal information, such as login credentials, payment card details, and other sensitive information. Phishing attacks are usually carried out via email, social media, or SMS.

* Assistant Professor, Department of Commerce, Ram Lal Anand College, University of Delhi, New Delhi, India.

- Data breaches: Data breaches can occur when an e-commerce business's network or systems are compromised, resulting in the loss of customer data. In the event of a data breach, customer data can be sold on the dark web, and the e-commerce business can face legal and financial repercussions.
- Malware attacks: Malware is malicious software that can be used to steal customer data, including payment card details, login credentials, and other sensitive information. Malware can be delivered via email, social media, or through malicious websites.

How Cyber Security makes E-commerce Works so Easy

Cybersecurity plays a crucial role in making e-commerce work smoothly and securely. Here are some ways in which cybersecurity helps e-commerce:

- **Protecting customer information:** Cybersecurity measures such as encryption and secure data storage help to protect sensitive customer information, such as credit card numbers, addresses, and other personal details, from cyber-attacks and fraud.
- **Ensuring secure transactions:** Cybersecurity measures such as two-factor authentication and fraud detection systems help to ensure that transactions are secure and legitimate, preventing fraudulent purchases and chargebacks.
- **Maintaining website availability:** Cybersecurity measures such as DDoS protection help to ensure that e-commerce websites are available and accessible to customers, even in the face of cyber-attacks that aim to disrupt or take down the website.
- **Preventing malware and cyber-attacks:** Cybersecurity measures such as anti-virus software and firewalls help to prevent malware and cyber-attacks that can compromise e-commerce websites, steal customer data, and cause other damage.

By implementing strong cybersecurity measures, e-commerce businesses can create a secure and trustworthy online shopping environment, which helps to build customer trust, reduce the risk of fraud, and increase sales.

Type of Cyber Security

There are many different types of cybersecurity, each of which focuses on protecting different aspects of computer systems and networks. Here are some of the most common types of cybersecurity:

- **Network Security:** This type of cybersecurity focuses on protecting computer networks from unauthorized access or attacks, such as viruses, malware, and denial-of-service attacks.
- **Application Security:** This type of cybersecurity focuses on protecting software applications from vulnerabilities that could be exploited by hackers. This includes things like SQL injection attacks and buffer overflow attacks.
- **Cloud Security:** This type of cybersecurity focuses on protecting data and applications that are hosted in the cloud from unauthorized access or attacks.
- **Mobile Security:** This type of cybersecurity focuses on protecting mobile devices and their data from security threats, such as malware, data breaches, and hacking.
- **Internet of Things (IoT) Security:** This type of cybersecurity focuses on protecting the growing number of connected devices that make up the Internet of Things, such as smart home devices, medical devices, and industrial control systems.
- **Identity and Access Management (IAM) Security:** This type of cybersecurity focuses on ensuring that only authorized users have access to a company's systems and data, and that their identities are properly authenticated and verified.
- **Cryptography:** This type of cybersecurity focuses on protecting data by using encryption techniques to prevent unauthorized access or interception of sensitive information.
- **Incident Response:** This type of cybersecurity focuses on responding to security incidents, such as data breaches or cyber-attacks, in a timely and effective manner to minimize the impact on the organization.
- **Social Engineering:** This type of cybersecurity focuses on protecting against attacks that exploit human vulnerabilities, such as phishing scams or pretexting.

Goals of Cyber Security in E-commerce

The primary goals of cyber security in e-commerce are to protect the confidentiality, integrity, and availability of sensitive information, such as personal and financial data, as well as to ensure the safe and secure functioning of e-commerce systems. Some specific goals of cyber security in e-commerce include:

- **Preventing unauthorized access:** Cybersecurity measures such as access controls and authentication mechanisms are implemented to prevent unauthorized access to e-commerce systems and data.
- **Protecting sensitive information:** Encryption techniques and secure communication protocols are used to protect sensitive information, such as credit card details, from being intercepted or stolen.
- **Maintaining system availability:** Cybersecurity measures such as firewalls and intrusion detection systems are implemented to ensure that e-commerce systems remain available and functional, even in the face of cyber-attacks.
- **Preventing fraud:** Cybersecurity measures such as fraud detection algorithms and transaction monitoring systems are implemented to prevent fraudulent activities, such as identity theft and payment fraud.
- **Ensuring compliance:** E-commerce businesses must comply with various regulations and standards, such as the Payment Card Industry Data Security Standard (PCI DSS), which outlines the minimum-security requirements for handling credit card information. Cyber security measures are implemented to ensure compliance with these regulations and standards.

Cyber Security Techniques in E-commerce

As e-commerce has become increasingly popular, it has also become an attractive target for cyber criminals. To ensure the security of e-commerce transactions, various techniques can be employed, including:

- **Encryption:** Encryption is the process of converting plain text into a secret code to protect sensitive information from being accessed by unauthorized parties. E-commerce websites use encryption techniques, such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols, to secure sensitive data during transmission.
- **Two-factor authentication (2FA):** Two-factor authentication adds an extra layer of security to the login process by requiring users to provide a second form of authentication, such as a fingerprint scan, in addition to their password. This makes it more difficult for cyber criminals to gain access to sensitive information.
- **Firewall:** A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls are used to protect e-commerce websites from unauthorized access and to prevent malicious traffic from entering the network.
- **Regular security updates:** E-commerce websites must keep their software up-to-date to ensure that vulnerabilities are addressed as soon as possible. Regular security updates to the website's software, including the operating system, web server, and database management system, can help prevent cyber attacks.
- **Strong passwords:** Passwords are the first line of defense against cyber attacks. E-commerce websites should encourage their users to choose strong passwords that are difficult to guess or crack. Passwords should also be changed regularly to prevent unauthorized access.
- **Anti-malware and anti-virus software:** E-commerce websites should use anti-malware and anti-virus software to prevent malware and viruses from infecting their systems. This software can also detect and remove any malware that has already infected the system.
- **Regular backups:** Regular backups of the website's data can help ensure that the website can be restored in the event of a cyber-attack or data loss. Backups should be stored securely and offsite to prevent them from being compromised in the event of a cyber-attack.

Overall, e-commerce websites must adopt a multi-layered approach to cyber security, combining the above techniques with regular security audits and risk assessments to ensure the safety of their users' information.

Cyber Security Ethics

Cyber security ethics refers to the moral principles and values that guide the actions of individuals and organizations involved in the protection of computer systems and networks from unauthorized access, attacks, and other forms of digital threats. The following are some of the key ethical considerations in cyber security:

- **Privacy:** Cyber security professionals must respect individuals' right to privacy and ensure that personal information is kept confidential and secure. They should also be transparent about their data collection practices and obtain consent from users before collecting or using their personal information.
- **Confidentiality:** Cyber security professionals must maintain the confidentiality of sensitive information and protect it from unauthorized access or disclosure. This includes protecting trade secrets, confidential business information, and other forms of proprietary information.
- **Integrity:** Cyber security professionals must ensure the integrity of computer systems and networks by preventing unauthorized modifications or alterations to data, code, or other digital assets. They should also ensure that data is accurate and reliable and that users can trust the systems they are using.
- **Availability:** Cyber security professionals must ensure that computer systems and networks are available to authorized users and that disruptions and downtime are minimized. This includes protecting against denial-of-service attacks and other forms of disruption.
- **Responsibility:** Cyber security professionals must take responsibility for their actions and ensure that they comply with relevant laws, regulations, and ethical standards. They should also report any suspected security breaches or other incidents to appropriate authorities.
- **Continuous Learning:** Cyber security professionals must engage in continuous learning and stay up-to-date with the latest threats and technologies. They should also educate others on cyber security best practices and encourage a culture of security awareness within their organizations.

Overall, cyber security professionals must balance the need for security with respect for individual rights and freedoms. By adhering to ethical principles and values, they can help ensure that the digital world remains a safe and secure place for everyone.

Conclusion

Cybersecurity is an essential aspect of our digital lives. It involves protecting computer systems, networks, and sensitive information from unauthorized access, theft, and damage. With the increasing reliance on technology and the internet, the risks and threats associated with cyber-attacks have also increased. These attacks can take various forms, such as malware, phishing, hacking, and ransomware, and can cause significant damage to individuals, businesses, and even governments.

Effective cybersecurity measures involve a combination of technological tools, policies, and procedures. Some examples include firewalls, antivirus software, encryption, strong passwords, regular backups, and employee training. It is also essential to stay up-to-date with the latest threats and vulnerabilities and continuously monitor and evaluate the effectiveness of security measures. Overall, cybersecurity is a critical issue that requires constant attention and proactive measures to ensure the safety and security of our digital world.

References

1. https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security
2. https://www.researchgate.net/publication/260126665_A_Study_Of_Cyber_Security_Challenges_And_Its_Emerging_Trends_On_Latest_Technologies
3. https://www.ijert.org/a-review-paper-on-cyber-security
4. Ecommerce- Dr Sushila Madan.