Original Research Paper

Volume - 12 | Issue - 06 | June - 2022 | PRINT ISSN No. 2249 - 555X | DOI : 10.36106/ijar

Commerce

CYBER SECURITY- A CONCERN ON E COMMERCE

Shivani Rajendran PhD Scholar, Department Of Corporate Secretaryship PSG College of Arts & Science , Civil Aerodrome, Avinashi Rd, Coimbatore - 641014 ,Tamil Nadu ,India

ABSTRACT Internet security is one of the major growing concerns among the users of Ecommerce websites and payment portals. Though the usage of E-Commerce sites is convenient, Feasible and time saving, some questions that arise among the users are –"Is online transactions safe?" "Are my credentials secure?" Where there is money in circulation, theft and threat follows. This is where Cyber Security plays its role. The main objective of this article is to create awareness about various cyber security schemes and how E-Commerce transactions can be made safe and how to protect our credentials from unauthorized users and threat creators. Cyber security refers to the protection provided to data, information, Media, Personal photographs and monetary details stored electronically. In simple terms the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks is called the Cyber security. The scope of threat, theft and attacks are huge in online platform that has created the importance for security. The people across the globe operate everything under one roof in a single click of a button. Social media facilitate integration of culture by connecting different people from various geographical locations. Internet has brought the world together and close to each other with the platform called the social media. Though this is a development at large, it is still a question of safety and security. India is digitalizing phase by phase but the awareness about cyber attacks and its solutions seems to be near to null among the users .In this paper, I have unlocked the possible ways through which our data can be maintained safe and how these threats and attacks can be handled and protected from hackers and cyber thieves

KEYWORDS : Ecommerce, Cyber Security ,Cyber Attacks, Electronic Payments portal, Online Threats, Digitalization.

Introduction

What is E-Commerce Security?

E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. E-Commerce sites are exposed to threats and attacks to a far extent and it is now being the top prioritized platform for purchase and sale of commodities and services .It offers B2B ,B2C, C2C ,C2B, C2G and G2C transaction features ,therefore the quantity of data stored and accessed via internet is large . When consumers make purchases online, they entrust their financial and personal information to the business they indulge on. India stands on 3rd position among the countries which are highly affected by wannacry 2.0 cyber attack though India is not yet completely digitalized as compared to UK, Germany & Russia. E Commerce sites are vulnerable to threats and attacks as it contains personal and financial information such as credit card details, personal home addresses, details of bank account, Phone number etc that are sensitive in nature . Cyber criminals engage in stealing these credentials to duplicate and access credit cards, debit cards and other personal financial information identity theft and fraud. These Sensitive data could also be held for ransom by hackers. Various threats that attack Ecommerce websites and payment portals are Phishing, Distributed Denial of Service attack(DDSA),Man in the middle attack, Malware, Spyware, Ransomware , Adware .Managing the risk of facing such threats and protecting customer credentials is a highly challenging task for users, operators and developers of Ecommerce and payment portals. These threats and attacks and the ways to protect data are explained in brief in this article. In nutshell, the process through which Ecommerce websites are protected and controlled in order to avoid unauthorized access and theft of sensitive information is called Ecommerce Security.

WHAT DOES THE STUDY SAY?

According to business and consumer data company Statistics ,over 3.8 thousand government services in India were provided over the internet in the financial year 2021. A CLSA report says that the value of digital payments in India will grow three-times near to 1 trillion dollars in FY26 from 300 billion dollars in FY21. India had 448 million social media users in FY21 . The reports shows shocking results that indicates the vastness of the cyberspace that India needs to secure. The government's digital initiatives and RBI's Central bank digital currency may stay vulnerable as well. The war in Ukraine indicates that India needs to review and repair its cyber-defense policies and be prepared for attacks. The country has to balance its attention to build a deterrent cyber-offensive capability. National Cyber Security Strategy should be formulated and finalized as soon as possible.

Dimensions of E-Commerce Security

- Integrity : Prohibiting unauthorized data access and modification
- Non Repudiation: Preventing any one party from reneging on an agreement
- Authenticity: Authenticating the data source.
- Confidentiality: Protecting sensitive and personal data from threats and attacks.
- Availability: Avoidance of data delays or removals
- Privacy: Creating a trust among the users regarding the data privacy

Threat to E-Commerce

Buying and selling of products and services through Internet and made available for the entire world is called Ecommerce and the payments for purchase and sale is made through online payment portals where transactions takes place from one bank account to another in easy ,fast and convenient manner. These transactions are vulnerable for modification and destructions. These threats and attacks are caused by cyber criminals who indulge in theft and activities that promote unauthorized access to personal and financial information online. E-commerce can be done through many technologies such as mobile commerce, Internet marketing, online transaction processing, electronic funds transfer, supply chain management, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Some threats are accidental, some are purposeful, and some of them are due to human error. The most common security threats are an electronic payments system, e-cash, data misuse, credit/debit card frauds, etcSome of the Major threat and risks are explained below

E-Cash Threats

Payment through online portals are simply termed as E-Cash . It can be Wallet payment, UPI Application transactions etc. The most common examples of e-cash system are transit card, PayPal, GooglePay, Paytm Some of the major E-Cash Threats are:

BACKDOOR ATTACKS

Backdoor attacks gives authorization to access personal and financial data over internet. This works in the background when the user works on the system .These attacks are done in the hidden mode ,therefore the user or operator cannot identify the attack.

DENIAL OF SERVICE ATTACKS

A denial-of-service attack (DoS attack) is a cyber attack through which the attack prevents the legitimate (correct) users from accessing the electronic devices. It makes a network resource unavailable to its intended users by temporarily disrupting services of a host connected to the Internet.

DIRECT ACCESS ATTACKS

Direct access attack is an attack in which an intruder gains physical access to the computer to perform an unauthorized activity and

installing various types of software to compromise security. These types of software are loaded with worms and download a huge amount of sensitive data from the target victims.

EAVESDROPPING

This is an unauthorized way of listening to private communication over the network. It does not interfere with the normal operations of the targeting system so that the sender and the recipient of the messages are not aware that their conversation is tracking.

CREDIT/DEBIT CARD FRAUD

A credit card allows us to borrow money from a recipient bank to make purchases for an amount more than the account balance. The issuer of the credit card has the condition that the cardholder should pay back the borrowed money with an additional agreed-upon charge.

A debit card is of a plastic card which is issued by the financial organization to account holder who has a savings deposit account that can be used instead of cash to make purchases. The debit card can be used only when the fund is available in the account.

SKIMMING-

It is the process of attaching a data-skimming device in the card reader of the ATM. When the customer swipes their card in the ATM card reader, the information is copied from the magnetic strip to the device. By doing this, the criminals get to know the details of the Card number, name, CVV number, expiry date of the card and other details.

UNWANTED PRESENCE-

It is a rule that not more than one user should use the ATM at a time. If we find more than one people lurking around together, the intention behind this is to overlook our card details while we were making our transaction.

VISHING/PHISHING

Phishing is an activity in which an intruder obtained the sensitive information of a user such as password, usernames, and credit card details, often for malicious reasons, etc.

Vishing is an activity in which an intruder obtained the sensitive information of a user via sending SMS on mobiles. These SMS and Call appears to be from a reliable source,say a bank but in real they are fake. The main objective of vishing and phishing is to get the customer's PIN, account details, and passwords.

ONLINE TRANSACTION

Online transaction can be made by the customer to do shopping and pay their bills over the internet. It is as easy as for the customer, also easy for the customer to hack into our system and steal our sensitive information. Some important ways to steal our confidential information during an online transaction are-

- Reading and scanning our keystroke and steals our password and card details
- By redirecting a customer to a fake website which looks like original and steals our sensitive information.
- By accessing public Wi-Fi

POINT OF SERVICE (POS) THEFT

The Point of Service is the service available in large stores, super and hyper market, restaurants where payment can be done by swiping the debit card. It is commonly done at merchant stores at the time of POS transaction. In this, the salesperson takes the customer card for processing payment and illegally copies the card details for later use.

THE ELECTRONIC PAYMENT SYSTEMS

The electronic payment systems have gained a fast paced growth in a very short period. UPI Transaction features are available at the payment doorstep of every vendors say from large enterprises to small roadside vendors. It plays very important role in e-commerce. E-commerce has led to paperless economy. It is one of the major revolutionary effort of banking sector and payment business managements that has made processing of fund and payment easy and time saving by reducing paperwork, transaction costs, and labour cost. Electronic commerce helps a business organization expand its market.

WHY E- COMMERCE SECURITY MATTERS?

Cyber attack leads to revenue loss and overall viability of business. Cyber criminals are well equipped and technically skilled to steal and attack on sensitive information from business. Breach of cyber security could mean the loss of customer information and thus could cost the business the trust and reputation of business

THREAT CAUSES

1. Intellectual property threats : To possess and usage of copyrighted materials and data without prior permission from author.

2. **Client computer threats**
- Trojan horse
- Active contents
- Viruses

3. **Communication channel threats**
- Sniffer progra
- Backdoor
- Spoofing
- Denial-of-service

HOW TO MINIMIZE SECURITY THREATS ?

1. Perform a risk assessment
2. Develop a security policy
3. Develop an implementation plan
4. Create a security organization
5. Perform a security audit

1**. Secure Electronic Transaction (SET) protocol**: Developed jointly by MasterCard and Visa with the goal of providing a secure payment environment for the transmission of credit card data.

2**. Disposable Credit Numbers:** One-time-use credit card numbers (private payment number) are transmitted to the merchant.

CONCLUSION

As the technological advancements increase, fear of attack and threat increase hand in hand.

There is a greater need for concern about the security of information Cyber security and privacy consideration has become predestined and unavoidable as India is growing and getting advanced in technology and global integration .Investments on Artificial Intelligence and cryptography has been a constant effort by organization inspite of pandemic and national emergencies. Threats are expected to be advanced when the platforms are getting highly technical such as cloud native, Digital native and Artificial Intelligence platform. Cyber security has not become a successful practice among the people. Theft through ATMs, stolen debit cards, unauthorized messages and phone calls to gather information, OTP sharing , fake bank calls to hack bank accounts have become very common nowadays but the awareness about the same is less than minimum compared to the number of Ecommerce users. The knowledge on Cyber crime, The cyber protection laws, ways and methods to protect data online need to be understood by all the citizen. In a country with 8 thousand government services being handled online and over 300 billion digital transactions held in year, the security must be made strict and efficient to handle attacks and cyber war. Protection is not a question, It is the solution.

REFERENCE:

1. https://www.cloudways.com/blog/ecommerce-security-tips/
2. https://economictimes.indiatimes.com/industry/services/education/cybersecurity-how-is-india-faring
3. http://www.ijser.org/researchpaper/Cyber-security
4. Amit Ghosh K(2012), E-Commerce Security and Privacy ,India , Springer Publishers.