PUNE RESEARCH SCHOLAR ISSN 2455-314X
AN INTERNATIONAL MULTIDISCIPLINARY JOURNAL VOL 4, ISSUE 4

CYBER CRIME AND E-COMMERCE

DR. PRAMOD R. BOTRE
Associate Professor,
Department of Commerce
Mahatma Phule Mahavidyalay
Pimpri, Pune- 411017. **(MS) INDIA**

ABSTRACT

In this techno savvy world nearly every person is having his own smart phone with internet attachment. India is the fastest growing market for Internet providing company. Expenses on internet done by general people in India is growing every year. India is one of the top most countries using personal internet connection with smart phones. Indians not only use internet for information exchange but also for doing business, online purchase and sales of goods and services. As technology is upgrading every now and then the proportion of e-commerce to traditional commerce in the country is also increasing. The main reason behind increasing love for e-commerce in the people is that it saves time of people. People don't have time for tradition shopping as it covers time required for travelling to reach the shopping centre, traffic jams, parking problems etc. On the contrary there are more varieties available online by seating at home 24 by 7. The mode of payment for such transactions is either cash on delivery or direct online payments through banks. Here comes the other side of transaction, the threat connected with e-commerce i.e. cyber crime. This paper focuses on various types of cyber crimes and precautions to be taken to overcome such crimes.

Key words- *E-commerce, Cyber Crime, Threats*

INTRODUCTION

Highly equipped technology with various facilities have attracted commerce sector to spread business all over the world. E-commerce is the result of this attraction. E-commerce is nothing but trading with the help of internet using computer or smart phones. This takes place between two traders known as business to business transaction (B2B), between traders and consumers known as business to consumer transaction (B2C) or consumer to consumer transaction (C2C). The scope of e-commerce is wide spread all over the world. All type of big and small industries are registered online to capture the market in the country and outside

the country. This has became the most easiest way of transaction so banks have also provided its customers with various online services making payment systems more convenient for the people.

India has the second largest number of smart phone users in the world and internet acts as a catalyst in driving the growth of smart phone users in India. As white collar businesses are growing on the other hand cybercrime has became more rapidly growing business build by criminals. These criminals buy and sell valuable stolen financial information in online black market. They also damage businesses by hacking the sites of the business. Sometimes they also affect business so badly that it has to shut down. So it is very important for our nation to have strong cyber laws to fight such crimes.

Literature review-

1. Sourabh Munjal, Anooja A, "Cyber Crimes Threat for the E-Commerce", SSRN Electronic Journal, 2016

The article briefs us about various aspects of e-commerce and cyber threats associated with e-commerce. Authors have given information about the codes of IT Act and Indian Penal Code (IPC) related to cyber crimes. They analyse cases registered under different crime heads. The ways in which cyber crimes have taken place has been explained by them with the help of related cases. At the end they have suggested different steps to be taken by people to avoid cyber crime.

2. N. Leena, "Cyber Crime Effecting E-commerce Technology", Oriental Journal of Computer Science and Technology, Vol. 4(1), 2011

As the article is written by an author related to computer science department, it mainly focuses on different types of cyber threats related to e-commerce. All types of threats are explained in brief in the article. Readers can understand the ways in which they will come across cyber crime while dealing online.

3. Mayur Patel, Neha Patel, Amit Ganatra, Yegesh Kosta, "E-Commerce and Attached E-Risk with Cyber Crime"

This article is a combination of different aspects related to e-commerce and cyber crime. Article contains meaning of concepts of like e-commerce, virtual business, e-risk etc. It also explains different types of cyber crimes and their effects.

E-Commerce-

E-commerce is the buying and selling of goods and services or the transmitting of funds or data, over an electronic network, primarily the internet. This type of commerce emerged in the early 1990. There are different types of e-commerce,

- Most popular out of them is **business to consumer (B2C)**. In this type businessman directly sells goods and services to its ultimate consumer. The chain of middle man is omitted in this type of business. Consumers get a chance to choose from wide variety available with different businessmen at comparatively low prices. This type of transactions saves time of the consumers. Being economical and time saving this type of transactions is becoming more favourite among the consumers.
- **Business to business (B2B)** – In this type of transaction one company transact with other company over the internet. Exchange of goods and services along with their payments take place online. This helps the companies to transact faster, to reduce time required for decision making, to cover large market area. It helps companies to share huge information with each other online. Example of such e-commerce is Go Daddy- it deals in selling domain name, hosting services to other business.
- **Consumer to business (C2B)** – whenever consumer deals with business it is consumer to business transaction. In this form consumer sells information to business. Generally businessman asks questions to consumer related to the products. Through survey method such information is collected by the business with the help of questionnaire and for sharing the information customers are being paid by the company.
- **Consumer to consumer (C2C)** – In recent years this type of transactions became popular over the internet. In this type consumer sells his commodities directly to other consumer over the internet site. Due to such transaction consumer save lot of money to be paid to middleman. Examples of such type of sites are eBay, OLX

All these types of e-commerce cover a huge market area. It connects the whole world together. Consumers get N number of varieties for a single commodity. Businessman also earns handsome profits. Though e-commerce is having lots of benefits it also has the threat of online theft by the hackers. This type of online crime is known as cyber crime. **Very common cyber crimes are** -

- **Phishing** – A fictitious email is sent by the perpetrator to individuals. This mail contains a fraudulent link which appears official and it makes the receiver to share his personal information on this website which is misused by the perpetrator.
- **Botnet** – Under this fraud hacker controls remote computers by transmitting controlling instructions to other computers. Then such computers are used for fraudulent work by the hacker.
- **Netspionage** – When confidential information of an individual is obtained by the hacker by hacking online system or individual's computers then it is known as Netspionage. Generally this information is sold to other parties for misuse by the hacker.
- **Online banking theft**- For transferring money from one account to criminal's account criminal hacker hacks banking system. In today's world where most of the people transact online, India is suffering with crucial online thefts by the hackers. Recently Cosmos Bank, Bank of Maharashtra and some other bank's websites were hacked by the hackers
- **Online credit card fraud**- Hackers make illegal online acquisition of credit card number and use it for unauthorised purposes and fraudulent purchases.

Cyber crime and Cyber Law-

Every unlawful act is punishable by the law. Cyber theft, fraud, forgery, hacking and every such act done by the criminals is punishable by two main acts in India. First is Information Technology Act, 2000 and second is Indian Penal Code. The cyber crime is governed by section 65 to 74 of Information Technology Act, 2000 and more than 20 sections of IPC. Both these act safeguard trading activities over internet. With the help of these acts people have registered cases against these cyber crimes. Every year thousands of cases are being registered against such fraud. This shows that with increasing number of internet users the number of complainants for cyber crime is also increasing rapidly. Most of these cases include online financial fraud. Interesting part of these cases is that not only individuals but big and small companies are also victims of such cyber crimes.

Ways to deal with Cyber Crimes

A single person, one company or government alone cannot fight against increasing cyber crime. Joint efforts from all the sides are required to control cyber crime. Some basic safety majors which can be followed are as follows

- First and for most important is **use of secured network.** Try to avoid public Wi-Fi as they can be easily hacked.
- Always keep your **operating system updated** because it helps in monitoring software of the device.
- Good quality, licensed **antivirus to be used** to prevent device from cyber attacks.
- Always **keep on changing password.** Using single password for longer period can be dangerous so keep on changing password for all online activities. Such as banking, email, credit debit cards etc.
- **Use different password** for different online activities. If you have habit of keeping same password for all transactions and if hacker cracks one of your passwords he can easily access to all your accounts so to safeguard your transactions keep all your passwords different from each other.
- Shopping online is today's worlds need. While fulfilling this need one has to be very careful as most of the cyber crimes take place through unsafe shopping websites. So keeps habit of **shopping through authentic websites** having full proof cyber security for the transactions.
- Keep the habit of **not opening mails from unknown sources.** Phishing is a type of tracking in which criminal trap their victims by sending spam mail asking for personal information so don't open unknown source mails.
- **Banks should develop their own cyber security system** instead of hiring it from it companies. This will help the bank in maintaining the privacy of the financial information of the bank.
- Criminals know how to mould the law from their side. It is the duty of government to frame strong laws with minimum loop holes. This will create fear in the criminals about the law and crimes will be reduced to some extend at the initial stage.

CONCLUSION

E-commerce, e-governance, paperless transactions, online banking are needs of today's hi-tech world. With good and developing concepts comes the treat of its misuse. Cyber crime is nothing but a dark side of advance technology. As technology will keep on developing cyber treat will also increase. So it is the duty of consumers, bankers, businessmen and government to be always aware of these treat and should help each other for fighting with this evil in the society. Little awareness will help all of us to stay away from cyber crime.

REFERENCES

1. Sourabh Munjal, Anooja A, "Cyber Crimes Threat for the E-Commerce", SSRN Electronic Journal, 2016
2. N. Leena, "Cyber Crime Effecting E-commerce Technology", Oriental Journal of Computer Science and Technology, Vol. 4(1), 2011
3. Mayur Patel, Neha Patel, Amit Ganatra, Yegesh Kosta, "E-Commerce and Attached E-Risk with Cyber Crime"
4. Mehta S., and Singh V., "A study of Awareness About Cyber Laws in the Indian Society", International Journal of Computing and Business Research, Vol. 4(1), Jan. 2013.
5. Nappinai N. "Cyber Crime Law in India: Has Law Kept Pace With Emerging Trends?"
6. Kandpal V., Singh R., "Latest Face of Cyber Crime and Its Prevention in India", International Journal of Basic and Applied Sciences, Vol. 2(4), 2013.