Cyber Crime Effecting E-commerce Technology

Tarunim Sharma*, Vinita Tomar**

Abstract: ***In today's world market perception has gone a drastic change. Thanks to internet and security protocols that are making physical market trends to obsolete as everybody is adopting and shifting to digital marketplace. The biggest reason behind this is accessibility to global markets and increase in effectiveness of businesses. But nothing comes without any flaws so is our E-Commerce. It is also having some infirmities. Cyber Crime is the biggest problem for the ecommerce world. Cybercrime act as a barrier in the success of online business industry. It is also called Computer Crime because doing online transactions using computer is used as an instrument for executing illegal tasks such as committing frauds, trafficking in intellectual property, stealing identities or privacy being violated. This paper draws out awareness to various causes of Cyber Crimes, problems faced and prevention for the same. Paper also studies how cybercrime perception affect the user's interest to go for online commerce.***

Keywords: Cyber Crime, E-commerce, E-Business

1. INTRODUCTION

E-commerce or Electronic Commerce also known as Internet Commerce refers to buying or selling of goods and services with the help of Internet, not only this but transfer of money or data to accomplish number of transactions. No offs, no time limits, no distance barriers in today world commerce is getting its new definition. It has been now transforming from physical market to electronic and mobile commerce. It is providing an easy way for doing not only shopping but number of other transactions in a very easy and suited way, anywhere anytime i.e.24*7 by just a one click away. All bank and financial institutions are moving towards setting up their setups and mobile formats to mitigate the online transactions. Number of immense players in e-shopping like Amazon, Flipkart, eBay, Myntra have established new blueprints for doing shopping. E-commerce comes in different types based on the transactional relations between customers and businesses like retail, wholesale, Drop shipping, Crowd funding, Subscription, digital products and services etc. As of now E-Commerce is said to be one of the fastest growing industry in global economy. Though ecommerce has become part and parcel of today's everyone individual life's, but it is proving to be one of the dangerous aspect of one's life as there are more chances of security breach and cybercrimes.

As we are doing number of transactions online, it has become the source of crime because lots of confidential information being shared, bank related and monetary transfers are being done which attracts the cyber criminals for violating the security. All firms are going online there by increasing their technical base without inspecting the huge risk associated with the same [1]. Cybercriminals can exploit these most important data and can do so much damage for an organization that e-commerce can end up by shutting down.

Internet Uprising

India being ranked the second largest online market in the world after China with 560 million internet users. With Revolution came in smart phones has uplifted the internet use and e-commerce vogue in India. This is because e-commerce offers number of unique advantages as it gives number of opportunities to different kinds of businesses to expand their business exponentially. It has a global reach which will otherwise be not possible with physical markets. It has other advantages to business that is freeing them from the office space, investment and travelling time also. Internet is a boon and acting as a connecting link between the supply sources and demand. This rapid growth is mainly because of huge advancements in technology and high-speed wireless networks availability.

TABLE 1

©MEDIANAMA

Statewise subscribers of narrowband and broadband connections

Telecom Service Area	Narrowband		Broadband	
	Rural	Urban	Rural	Urban
Andhra Pradesh	2.33	2.25	19.21	30.01
Assam	0.67	0.61	5.9	5.85
Bihar	3.69	1.56	21.68	16.96
Delhi	0.2	2.61	0.54	35.18
Gujarat	1.18	1.43	10.86	29.13
Haryana	0.55	0.61	5.61	9.26
Himachal Pradesh	0.26	0.19	3.16	2
Jammu and Kashmir	0.01	0.03	1.69	3.14
Karnataka	1.45	1.86	12.87	27.5
Kerala	0.79	1	9.48	14.7
Kolkata	0.18	1.38	1.34	13.94
Madhya Pradesh	2.48	2.15	14.58	25.23
Maharashtra	2.51	2.62	19.65	32.82
Mumbai	0.1	2.39	1.27	25.21
North East	0.3	0.34	2.66	4.06
Orissa	1.42	0.47	9.09	6.63
Punjab	0.7	0.97	6.68	16.34
Rajasthan	2.07	1.56	15.16	20.42
Tamil Nadu	1.54	2.54	11.94	32.44
Uttar Pradesh (East)	3.77	2.19	20.14	23.4
Uttar Pradesh (West)	1.96	1.64	11.27	19.75
West Bengal	2.46	1.18	12.23	14.44
Total	**30.62**	**31.58**	**217.01**	**408.41**

** Assistant Professor, Maharaja Surajmal Institute; tarunimsharma@msi-ggsip.org*
*** Assistant Professor, Maharaja Surajmal Institute; vinitatomar@msi-ggsip.org*

TABLE 2: Internet Subscribers in India

At the End of March	Total	Urban	Rural
2013	13.47	-	-
2014	20.28	-	-
2015	24.07	49.07	12.89
2016	26.97	58.28	12.80
2017	32.85	70.83	15.49
2018	38.01	84.74	16.41

The above data shows the digital buyers becomes almost doubles in 2018 and estimates that the number of users will be reaching almost 623 million by the end of this year which is a huge number. The data shows that almost 97 percent of users are going for mobile phones to access the internet and various e-commerce activities. Increasing bandwidth availability, flexible and variety of data plans and number of awareness programs by government has bridged the digital gap among rural and urban India that can be seen in the table above. But it comes with the problem of security of online transactions.

Cyber Crime and Criminals

Cyber Crime is a crime which uses computer and internet as an object to enact illegal tasks. While most of the cyber-crimes are performed by criminals to gain benefits but some of them are executed mainly to disable and damage computer or network of computers with some infectious programs know as viruses. Not only this they gain access to confidential organization information, personal information, government important information, credit card or other payment related data and use them for unfair means and sell them for their profits. In today's world of digital age our identity information is the most essential part of our day to day life. So, cybercrime is generally related to digital data and the persons performing these activities are said to be Hackers. These hackers are using very modern and innovative ideas to perform cyber-attacks while on the contrary avoiding their detection and arrest. Hackers uses well equipped software for achieving their goals, but social engineering is said to be their important component [4]. Cybercrimes are basically categorized as follows:

1. Data Offence

- ***Data Alteration***

Privacy while establishing connection between the two parties is important to make sure that the data being transmitted is not get tampered in transit. Connecting through internet brings the chances of computer crime being conducted by the third party when the data is exchanged. In this attack unauthorized user modify the data being transmitted by gaining access to it illegally.

- ***Data Stealing***

As the name says data is stealed by unauthorized users which includes confidential data, personal data, government information, credit card information, passwords, organization secret information. In this information is being copied in an illegal way without the knowledge of user which comes under a big crime. Phishing named as Email spoofing which include links to number of admissible looking websites which steals your confidential and secret information.

- ***Data ambushing***

In this the attacker detects the torrent of data being transmitted from one end to other to gather information which can be used later. Data collection is the main objective of this attack.

2. NETWORK MISDEEDS

In this network is being tempered like deleting, damaging, altering, suppressing, defacing the data being exchanged. Botnets are the computer networks that are managed by remote hackers. Remote hackers take these botnets as the medium to attack on other computers in networking.

3. GAINING CRIME

In this attack hackers gains unauthorized access to confidential data with the help of number of exploit kits which are the ready-made tools bought by hackers online. In this attack we also discuss viruses which are computer programs that attaches themselves to system files to corrupt or replicate themselves to transmit to other computers on networks to disrupt the operation going on and damage data stored.

4. EMAIL BOMBING AND SPAMMING

In this large number of emails are send to target address which results in crashing of its account. The mails are too big to handle and consumes a large amount of network resources resulting in denial of service attack.

5. WEB JACKING

In this hacker takes control on others website illegally. The owner lost the control on his website and attacker use the unauthorized accesses website for its own profit gains. They not only change the content of genuine website but redirects the user to the fake website which is now owned by the attacker.

CYBER Criminals

They are the persons that attacks our computer system and crash them by adopting any of the above methods. They include an individual or a group of people who perform these attacks for their financial and personal gains[8]. They are of the following types:

- Hackers: It refers to an individual who uses their technical knowledge to have an unauthorized access to network of systems or data.
- Stalkers: They are the people who intentionally observe the activities of their victim to get hold of their private data. These types of crimes are generally conducted through social media daises.
- Discontented Employees: Employees of an organization can also become hackers if they are unsatisfied with their job. They perform cybercrime by attacking their organizations system.
- Script Kiddies: These attackers use the already made hacking programs and go through them thoroughly so that they can reuse them by making slight changes according to their convenience.
- Phishes: They are the cyber criminals whose main motive is to steal the personal or sensitive information related to an individual. They create the copy of the original website and users fall prey to such activities and share their important information. Such sites also spoil the reputation of organization which leads to decrease in revenues.
- Commercial Groups, Insiders, Advanced Persistent Threat Agents etc.

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 e-commerce 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.

Causes of Cyber Crime

Number of factors are there that motivates cyber criminals to execute the attacks. The number of causes include:

- Sometimes attackers have grudges against an organization because either they have taken away his market or job, never appreciated the hard work, incentives or promotion due not given.
- Other factor can be low cost for implementing these crimes, inadequate rules and regulation, chances for being caught are low.
- Poverty, corruption and unemployment also attracts being hackers.
- Easy accessibility to internet makes it serene to execute such attacks.
- Peer group influence and defective socialization are the other factors for motivating these criminals.

Impact of Cyber Crime

i. Time wastage and decline financial growth: There is lot of time wastage as IT professionals spent most of their time rectifying and recovering from the harm caused by cyber criminals. That time can be utilized in gaining profit for the organization. Not only this but financial growth also get disturbed as people started losing trust on the companies because of the frauds and started moving to others for security.

ii. Decrease in productivity: Companies spent most of their time in inculcating security by applying number of passwords that consumes most of the organizations productive time. Companies also buys expensive software to stop the attack from viruses which add to the overhead cost.

iii. Fear in Teenagers: Today teenagers fear a lot from this because of cyber bullying. It has now become the situation of concern. It is affecting the girl teenagers mostly as they are the easy targets and they fear from bad comments, negative pictures and threatening messages.

iv. Identity theft: If you are the victim in hands of cyber criminals it leaves a long-lasting effect on your life as sharing personal information is a big loss.

v. Change in consumer behavior: Consumers will start avoiding the online shopping and they will take it as an alternative method. Because security is their main priority.

Controlling Cyber Crimes

Cybercrimes must be controlled by the joint effort of organizations and internet users. All the required precautions must be taken to prevent these attacks. Internet users should be smart enough to not to fall in trap of hackers. Everyone should know the basics of how to protect themselves from such attacks. Otherwise cybercrime will put our lives to harm.

In contrast to real life world cyber criminals works in unity instead of fighting for supremacy. They help each other to strengthen their power and increase their opportunities[7] . Hence instead of routine methods we should implement some advanced techniques to keep check on them.

I. Employ strong passwords: Don't use same passwords on different websites, change them regularly. Passwords should be complex including numbers, letters and special symbols.

II. Keep your system up to date: The most important thing you must keep in mind is to make your operating system, internet and security software updated. If there is any flaw in that attacker will take advantage of that you will their next target.

III. Directing your social media fixtures: Keep your personal and private information secure. Do not reveal detail information about yourself and your family because they give hints to attackers to crack into your protected data.

IV. Educate your children about the internet: Teaching your children about how to make proper use of internet. They must be knowing about the pros and cons about using that.

V. Keeping yourself aware on major security breaches. If your website is there on internet for e-commerce you should be aware of what information hackers usually

VI. Access so that they should protect and apply proper check on those and change passwords regularly.

Encrypt and back up your most important data. You should keep duplicate copies of your personal data either on hard disk attached to your primary memory or on remote such as cloud.

6. CONCLUSION

The use of internet has spread his roots globally for e-commerce. This paper shows how cyber crime is affecting e-commerce and different levels of society. This helps us in getting knowledge of various threats of using internet and how to save yourself from that. The ways to overcome these crimes is to study laws, policy and well educated about how to save yourself from such attacks. In addition to this we have adopt other measures to secure our self from cyber criminals. So that they does not take advantage of browser ignorance, laws inefficiency, legislative delays.

REFERENCES

[1] Dalla, H. S., & Geeta. (2013). Cyber Crime – A Threat to Persons, Property, Government and Societies. International Journal of Advanced Research in Computer Science and Software Engineering,

[2] Dhanoa, R. (n.d.). Cyber Crime Awareness. International Journal in Multidisciplinary and Academic Research (SSIJMAR), 2(2), 1-7.

[3] Saini, Hemraj, Rao, Yerra Shankar., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications (IJERA), 2(2), 202-209. Retrieved from http://www.ijera.com/ papers/Vol2_issue2/AG22202209.pdf.

[4] R. Boateng, R. Heeks, A. Molla, and R. Hinson, "Advancing e-commerce beyond readiness in a developing country: experiences of Ghanaian firms," Journal of Electronic Commerce in Organizations, vol. 9, pp. 1-16, 2011. Available at: https://doi.org/10.4018/jeco.2011010101.

[5] S. Hawkins, D. C. Yen, and D. C. Chou, "Awareness and challenges of Internet security," Information Management &Computer Security, vol.8, pp.131-143, 2000. https://doi.org/10.1108/09685220010372564.

[6] R. Smith, P. Grabosky, and G. Urbas, "Cyber criminals on trial," Criminal Justice Matters, vol. 58, pp. 22-23, 2004. Available at: https://doi.org/10.1080/09627250408553240.

[7] D. Gefen, I. Benbasat, and P. Pavlou, "A research agenda for trust in online environments," Journal of Management Information Systems, vol.24, pp. 275-286, 2008. Available at: https://doi.org/10.2753/mis0742-1222240411

[8] Turban, E., King, D., Lee, J. K., Liang, T.-P., & Turban, D. C. (2015). E-Commerce Security and Fraud Issues and Protections Electronic Commerce (pp. 459-520): Springer.

[9] O'Brien, J. A., & Marakas, G. (2011). Developing Business/IT Solutions. Management Information Systems, 488- 489.

[10] Kim, S.-S., Hong, J.-W., & You, Y.-Y. (2015). an Exploratory Study on E-Business Risks Due to the Sector Classification of Small and Medium-Sized Enterprises. Indian Journal of Science and Technology, 8(S8), 387-396.