A Study on Fear of Cybercrime Victimization In E-Commerce

DEVAYANE. B
Assistant Professor, Department of Criminology and police administration, Sri Kanyaka Parameswari Arts & Science College for Women, Chennai, Tamil Nadu

***Abstract*— Online shopping has grown in popularity in recent years, particularly during this pandemic. In the twenty-first century, e-commerce has gained popularity. Despite its growth, it has certain negative consequences, such as cybercrime. The purpose of this study is to determine the extent of victimization fear and how it affects e-commerce purchases. Primary data is gathered via an online questionnaire, while secondary data is gathered through journals, publications, and studies. The analysis is carried out using statistical techniques in order to determine how the fear of crime affects the e-commerce platform, as well as the level of awareness of various cybercrime actions among Chennai residents. According to the study, the fear of cybercrime influences online shopping behavior.**

***Indexed Terms*— cybercrime, victimization, e-commerce**

I. INTRODUCTION

We are now in the twenty-first century, and all transactions are conducted through internet platforms. E- Commerce is a rapidly expanding field in the twenty-first century. E-commerce is a platform that allows us to buy and sell items from around the world. It brings people from all around the world together. The rise of e- commerce has accelerated in the last two years as a result of the epidemic. Since the pandemic, everyone has found it more convenient to shop online. E-commerce refers to the buying, selling, and marketing of goods over the internet. Every coin has two sides, and e-commerce has certain disadvantages as well. The result is a cybercrime threat. For online transactions, e-commerce platforms generate a large amount of data. Those detailsare at risk of being used by the government.

The National Crime Records Bureau (NCRB) is an Indian government body tasked with collecting and analyzing crime statistics in accordance with the Indian penal code. According to the NCRB data, Bengaluru (Karnataka) has the highest number of cybercrime instances when compared to all other states. The total number of cases reported in Chennai in 2018 was 73, rising to 118 in 2019, and rising to 186 in 2020. In comparison to Karnataka, the number of cases reported in Chennai is lower. According to statistics, observing cybercrime in Chennai is not a concerning scenario. However, the NCRB only keeps track of reported cases; there are many unreported cases, i.e., those cases that aren't mentioned in the media. Even though the city of Chennai is not in a dangerous scenario, we cannot deny that cybercrime rates have risen. Given the ominous data, it is critical to investigate criminality on e-commerce platforms.

II. E-COMMERCE

E-commerce, also known as electronic commerce, refers to online purchases, sales, marketing, and other types of transactions conducted over the internet. Amazon, Flipkart, eBay, Myntra, and other online stores are examples. Business to business (Shopify), business to consumer (Amazon), and consumer to consumer (Amazon) are the three types of e-commerce (ebay). The lack of security and privacy is the most serious flaw ine-commerce.

III. VICTIMIZATION

A victim is a person who has been harmed or lost their fundamental rights, either psychologically or physically, as a result of acts or omissions. The process of being victimized or being a victim is known as victimization. The process of victimizing someone over the internet is known as "cyber victimization."

The term "cyber victimization" is used to describe victimization caused by cyber criminals.

IV. CYBERCRIME

Cybercrime is defined as any crime that involves computer networks or the use of computers to commit an offence. In other circumstances, the computer may have been used as a target for cybercrime. It may have an impact on a person's security and financial well-being.

V. CYBER ATTACKS ON E-COMMERCE

Cybercriminals are currently focusing their efforts on e-commerce. For them, it's like a honey pot. By breaking into a website's database, hackers can obtain a large amount of data. E-commerce cyber security is becoming increasingly dangerous. The following are some examples of cyber-attacks on e-commerce sites.

S.No	Cyber Attacks	Explanation			
1	POS Cyber attacks	A POS (point of scale) attack occurs when a customer's personal information is maintained at a specific location. To attack or access the information, the hackers utilize malware.			
2	Web application attacks	Web jacking is another method of gaining access to client information (technique used). Hackers acquire access to and control over another's website.			
3	Phishing & spear phishing	Phishing is a type of social engineering assault used to Obtain financial information from clients. Impersonation is similar to spear phishing.			
4	Spoofing	It is also a type of social engineering attack in which the hackers duplicate the website so that the information we provide is directly stored and Accessible to the hackers.			
5	E-skimming	By hacking the website's payment page, the hackers have direct access to the credit card information			

		of the clients.			

VI. LAWS RELATING TO CYBERCRIME IN INDIA

We must all remember that cyberspace is a common tradition that we have inherited from the benefits of emerging technologies. It is our responsibility to keep cyberspace free of problems. The government enacted cyber laws to prevent crimes in cyberspace. Cyber law refers to legal issues that arise as a result of using the internet. The significance of cyber law is that it touches on every aspect of cyberspace issues. Cybercrime is covered by the Information Technology Act of 2000 and the IPC. The IT Act was later amended in 2008. In addition to the IT Act and the IPC, there are two other acts that address cyberspace security, namely the Copyrights Act and the Consumer Protection Act.

VII. OBJECTIVES

- Determine whether or not the fear of being a victim of cybercrime influences online shopping.
- To discover the significant relationship between gender and cybercrime victimization.
- Determine the level of familiarity with various cybercrime laws.

VIII. LITERATURE REVIEW

The internet is undergoing a revolution in the twenty-first century. E-commerce platforms are one such thing that is expanding in tandem with the internet. The positive impact of the revolution is accompanied by a negative impact, namely cybercrime fraud. People nowadays are well aware of the dangers of online shopping. A large number of people are concerned about becoming victims. The perceived risk of victimization is not the only barrier to using e-commerce platforms. The two most important predictors of fear of cybercrime victimization are perceived risks of victimization and cybercrime victimization (Billy Henson, 2011). Aside from being a victim of cybercrime, expressing concern and raising awareness has nearly twice the negative impact on online behavior. Similarly, those who have never heard of cybercrime are more likely to shop online (Rainer Bohme & Tyler Moore,2012). Analyzing the relationship between three predictors of cybercrime fear: prior victimization, perceived risk of victimization, and perceived seriousness of cybercrime. We discovered that not all predictors of cybercrime are the same (Szde Yu,2014). Cybercrime is regarded as a roadblock in the path of e-commerce. The only way to combat cybercrime threats is to enforce existing laws. A major issue for administrators is a lack of skills and a training programme (Debendra Shaw,2016). Another wayto effectively enforce cyber law is to make the law adaptable to changing circumstances, and to establish more and morecyber cells (Yougal Joshi &Anand Singh , 2013). Cyber laws should be reviewed on a regular basis in order to protect India from cybercriminals (N.Leena,2011). Every netizen, businessman, company, organization, and government must be aware of these threats and collaborate to combat this societal evil. A little awareness will help us avoid cybercrime (Dr.Pramod.R.Borse, 2018).

IX. RESEARCH METHODOLOGY

The research methodology is a methodical approach to solving any research problem. It is an important step in any research study because the research is done scientifically. The methodology for the study is divided into several categories, including questionnaires, data collection, and statistical tools and techniques.

- Sources of Data

Primary data is gathered using an online questionnaire, while secondary data is gathered using journals, articles, and research.

- Area of the Study

The study is restricted to some places of Chennai city.

- Target Population

People who live in Chennai city were the target population.

- Questionnaire Design

There were five sections to the questionnaire. The first section contains demographic information about the respondents, such as their age, gender, occupation, and educational status. The second section is about the preference for online shopping, the third section is about the fear of victimization, the fourth section is about the impact of cybercrime victimization in e-commerce platforms, and the last section is about prior victimization and awareness.

- Sample size

Out of 200 samples, only 142 samples are suitable for the analysis. The remaining 58 samples are illogicalto the study.

- Data analysis & interpretation

The collected data is analyzed using statistical tools such as the Independent t test and chi-square test. Cronbach's Alpha equals .715.

- Technique of analysis

To ensure the accuracy of the data obtained, the primary data collected from respondents is categorized, edited, and analyzed using a statistical tool called SPSS.

- Limitations

The study's scope is limited to residents of Chennai, and the sample size is so small that it may not represent the entire Chennai population.

X. DATA ANALYSIS

Table 1: Demographic profile of the respondents

Demographic profile		Frequency	Percentage	Total
Gender	Male	26	36.6	142
	Female	43	60.6	
	Prefer not to say	2	2.8	
Age	Below 20	29	40.8	142
	20-29	39	54.9	
	30-39	2	2.8	
	40-49	1	1.4	
	50 & above	-	-	
Educational Qualification	SSLC	3	4.2	142
	HSC	9	12.7	
	UG Graduate	29	40.8	
	PG Graduate	26	36.6	
	Professionals	3	4.2	
	Others	1	1.4	
Occupational Status	Private Employee	17	23.9	142
	Government Employee	2	2.8	
	Business	1	1.4	
	Home Maker	5	7.0	
	Student	38	53.5	
	Others	8	11.3	

(Source computed data)

According to table 1, the majority of respondents are females (60.6%), aged 20–29 years (54.9%), undergraduates (40.8%), and students (53.5%).

Table 2: Reporting behavior of the respondents

Reporting Behavior		Frequency	Percentage	Total
Have you been victimizedof any cybercrime fraud?	Yes	16	22.5	142
	No	55	77.5	
Have you ever reportedany cybercrime fraud?	Yes	16	22.5	142
	No	55	77.5	
If no, What are the reasons?	Not knowing where to report	12	16.9	142
	Not considering it as a big fraud	10	14.1	
	Others	44	62.0	
If yes, where will you report?	Police Station	18	25.4	142
	Register complaints online	10	14.1	

	Raising complaints inthe E-commerce platforms	17	23.9	
	Others	15	21.1	

(Source computed data)

Table 2 shows that the majority of respondents (77.5%) have not been victims of cybercrime fraud; the majority of respondents (77.5%) have never reported any crime; and the majority of respondents who report crimes in police stations (25.4%).

Table 3: Awareness on legal provisions

Awareness on legal provisions		Frequency	Percentage	Total
Have you been aware of theInformation Technology Act?	Yes	35	49.3	142
	No	16	22.5	
	Maybe	20	28.2	
Are you aware of the Copy Rights Act?	Yes	40	56.3	142
	No	12	16.9	
	Maybe	19	26.8	
Have you been aware of theconsumer Protection Act?	Yes	45	63.4	142
	No	10	14.1	
	Maybe	16	22.5	

(Source computed data)

Table 3 shows that the majority of respondents are aware of cyber laws such as the IT Act (49.3 percent), the Copy Rights Act (56.3 percent), and the Consumer Protection Act (63.4%).

Table 4: Fear of Cybercrime victimization influences online shopping

Independent T test					
	N	Mean	Std. Deviation	T	Sig.(2-tailed)
Data that we have entered on e- commerce sites are used for committing most of the cybercrimes	142	3.79	.754	36.736	
I trust those websites for confidentiality.	142	3.30	.991	23.764	.000
My Fear of victimization made me to avoid online shopping.	142	3.54	.892	28.681	.000
My fear of victimization does not influence my shopping behaviour	142	3.44	.937	26.407	.000

(Source computed data)

According to table 4, the mean values of respondents' views on the influence of fear on e-commerce platforms range from 3.30 to 3.79. The standard deviation of the majority of the variables ranges from.754 to.991. The significant value reveals that fear has an impact on e-commerce platforms.

Table 5: Relationship between Gender and prior victimization

Association between gender and prior victimization					
			Have you been victimized of any cybercrime fraud?		Total
			Yes	No	
Gender	Male	Count	8	18	26
		% within Gender	30.8%	69.2%	100.0%
		% within Have you been victimized of any cybercrime fraud?	50.0%	32.7%	36.6%
		% of Total	11.3%	25.4%	36.6%
	Female	Count	8	35	43
		% within Gender	18.6%	81.4%	100.0%
		% within Have you been victimized of any cybercrime fraud?	50.0%	63.6%	60.6%
		% of Total	11.3%	49.3%	60.6

					%
	Prefer Not to say	Count	0	2	2
		% within Gender	0.0%	100.0%	100.0%
		% within Have you been victimizedof any cybercrime fraud?	0.0%	3.6%	2.8%
		% of Total	0.0%	2.8%	2.8%
Total		Count	16	55	71
		% within Gender	22.5%	77.5%	100.0%
		% within Have you been victimized of any cybercrime fraud?	100.0%	100.0%	100.0%
		% of Total	22.5%	77.5%	100.0%

Chi-square test		
Pearson Chi-Square	Degrees of Freedom	Significance (2-tailed)
1.972^{a}	2	.373

(Source computed data)

The Chi-square test on the summarized cross tabulation is shown in Table 5. The Pearson Chi-Square value is 1.972a, and the significant value is.373, both of which are statistically insignificant, implying that there is no association between gender and prior victimization. This implies that everyone is vulnerable, regardless of gender.

XI. FINDINGS

- According to the study, the majority of respondents (60.6 %) was women between the ages of20 and29 (54.9 %) and enrolled in a UG program (40.8 %).
- 77.5 percent of those polled were unaffected and chose not to report it. Respondents' first priority when filing a complaint is the police station (25.4 %).
- Respondents are familiar with cybercrime laws such as the IT Act (49.3%), the Copyright Act (56.3%), and the Consumer Protection Act (63.4 %).
- According to research, the fear of being a victim of cybercrime influences online shopping behavior.
- The study also revealed that everyone is vulnerable, regardless of gender.

CONCLUSION

According to the study, the fear of being a victim of cybercrime influences online shopping behavior. This significant effect suggests that respondents experience fear when shopping on e-commerce platforms, which reduces their online shopping behavior. To summarize, everyone is vulnerable, regardless of gender, so itis necessary to raise public awareness.

BIBILOGRAPHY

[1] Debendra Shaw, cybercrime in India – A challenge to the growth of E-commerce, RAY: International Journal of Multidisciplinary Studies, E-ISSN: 2456-3064 Volume I, No. 2, October, 2016, pp. 75-83.

[2] Joshi, Yougal., & Singh, Anand. (2013). A study on cybercrime and security scenario in India. InternationalJournal of Engineering and Management Research (IJEMR), 3(3), 13-18.

[3] Houssam Saleh, Amira Rezk, Sherif Barakat ,THE IMPACT OF CYBER CRIME ON E-COMMERCE, International Journal of Intelligent computing and information science, IJICIS, Vol.17 No. 3 July 2017

[4] Billy Henson, "Fear of Crime Online: Examining the Effects of Online Victimization and Perceived Risk on Fear of Cyber stalking Victimization", PhD Thesis, School of Criminal Justice of the University of Cincinnati, 2011.

[5] Rainer Bohme and Tyler Moore, "How Do Consumers React to Cybercrime?", The 7th APWG e-Crime Researchers, Las Croabas, Puerto Rico, 2012.

[6] Szde Yu, "Fear of Cyber Crime among College Students in the United States: An Exploratory Study", International Journal of Cyber

Criminology (IJCC), Vol. 8, No. 1, 2014, pp. 36–46.

[7] N. LEENA, Cyber Crime Effecting E-commerce Technology, Oriental Journal of Computer Science &Technology Vol. 4(1), 209-212 (2011).

[8] Dr.Pramod R. Borse, Cybercrime and E-commerce, An International Multidisciplinary Journal, ISSN 2455- 314X Vol.4 Issue