Public Awareness on Cyber Crime with Special Reference to Chennai

Samrin Sulaiman, Sreeya B

Abstract With the rapid advancements in technology, our lives have become completely digitalised. We sit in the comfort of our home, and carry out our day-to-day activities like grocery shopping, education, banking, through the Internet. However, this has given rise to several threats to our security, called the cyber-crime which has become a global concern. Cybercrimes affect the lives of millions of people all around the world, including businesses, organisations and governments of different nations. This paper aims to determine the association between cybercrime awareness and the age, and to identify the difference between main cause of cybercrime and the gender. Descriptive research has been carried out which helps us to understand the characteristics of an individual or a group. The sampling method used here is convenient sampling where the samples have been chosen based on ease of access of availability. The sample size is 1540. Age, Gender and Occupation are the independent variables. Cyber-crime awareness, the main cause of cybercrime and the most popular cyber-crime are the dependent variables used here. The tools used here are Chi-Square, Independent Sample t test and ANOVA. It was found that there is a significant association between the cyber-crime awareness and the age of the respondent and that there is no significant difference between the main cause of cyber-crime and gender. With the rapid rise in the rate of cyber-crimes, it is imperative that the government provide the people with more effective ways of cyber security in order to protect the society.

Keywords: Cyber-crime, Cyber terrorism, Cyber Security, Cyber Laws, Public awareness.

I. INTRODUCTION

The term crime is defined as an unlawful act which is punishable by the state, which harms not only an individual but also the community or the state. The internet has definitely made our lives easier but at the same time it has also increased our risk and threats to safety. Cybercrimes refer to the criminal or fraudulent activities which are committed using the computer or the internet or both. This includes cyber bullying, phishing, email spoofing, cyber pornography, cyber stalking, etc. Cyber-crimes take place due to the greed for money, personal vengeance, and also as a hobby. The cyber criminals generally tend to target the regions where the cyber laws are weak and vulnerable. These cyber-crimes are carried out through computer systems and other electronic devices using viruses, as a weapon to carry out crimes or as an accessory to store illegal information. It affects several businesses every year, leading to substantial loss of money and reputation. India, the largest market for internet users, is no exception to this menace. In a report published by the National Crime Records Bureau report (NCRB 2011), the incidence of cyber-crimes under the IT Act has increased by 85.4% in the year 2011 as compared to 2010 in India, whereas the increase in incidence of the crime under IPC is by 18.5% as compared to the year 2010. Maharashtra has emerged as the centre of cyber-crime with maximum number of incidences of registered cases under cyber-crimes. Bangalore, being India's 'Silicon Valley' registered a whopping 5035 FIRs at the city's lone cybercrime police station which is a lot more than in the other major cities in 2018 as per the National Crime Records Bureau. Thus, it is imperative that the government increases the number of cybercrime police stations in the country and also enforces the law strictly to reduce cybercrime rates in India.

II. OBJECTIVES

- To understand about the cyber-crimes.
- To determine the association between cyber-crime awareness and the age.
- To identify the difference between main cause of cyber-crime and the gender.
- To find the level of agreeability towards the most popular cyber-crime among the occupational groups.

III. LITERATURE REVIEW

Hannarae Lee, et al. (2019) has explored the study with the objective of understanding whether public awareness matters to fight against cyber crimes and cyber criminals. It is an exploratory research where the data has been collected from secondary sources like journals, documents, etc. The author has found that the government and public awareness is mandatory to fight against cyber crimes. Navneet Kaur (2018) has determined the types of cyber crimes like crimes against individuals, crimes against property, and crimes against organisations. It is a conceptual paper where the researcher has given a theoretical framework regarding the types of cyber crimes. The researcher has concluded that international laws and regulations combined with reliance on technologies are crucial to help fight against cyber crimes. Muhammad Dharma, et al. (2018) has examined the effect of cyber crimes on the financial status of a country and on the consumer confidence of online shoppers due to fraud victimisation in online stores. The data has been collected from previous research findings and journals. They have found out that cyber crime can be eradicated only under three categories which are Cyber Laws, Policy-

Revised Manuscript Received on 14, October 2019.

Samrin Sulaiman, Author, BBA LLB (Hons.), Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, Tamilnadu, India.

Dr. Sreeya B, Co Author, Associate Professor, Department of Management Studies, Saveetha School of Law, Saveetha Institute of Medical and Technical Sciences (SIMATS), Chennai, Tamilnadu, India. (email: sreeyab.ssl@saveetha.com)

making and Education. Kyung-shick Choi, et al. (2018) has analysed the inter connectivity between cyber crime, cyber terrorism and cyber security. The paper is based on the data from news report, journals, etc published previously. They have observed that cyber crime and cyber security are ubiquitous and are rapidly developing with new techniques and skills. K. Jaishankar (2018) in his paper has focused on the history, contribution and impact of cyber Criminology in today's era, which is based on the information acquired from other journals and papers. The author has put forth that there has been a surge of cyber crime in the past decade or so because of the advancements in the field of technology. Juneed Iqbal et al. (2017) has identified the challenges faced by the people due to cyber crimes and the remedies available with special reference to the population of India. They believe that India must sign the Budapest Convention in order to combat cyber crimes and to reduce its rates. Dambo Itari, et al. (2017) has given a detailed explanation regarding the causes and effects of cyber crime and the importance of cyber security with special reference to the country of Nigeria. The data has been collected from secondary sources like journals, books and newspapers. They have concluded the paper with some recommendations to the Nigerian government on how to reduce the rate of cyber crimes. Johannes Xingan Li (2017) has reviewed the historical development of cyber crime and the legal countermeasures. It is a conceptual paper which thoroughly talks about the origin and development of cyber crimes. The author has concluded that the criminal phenomena will be saturated at an equilibrium point only when there is a balance between criminal and judicial resources. Animesh Sarmah et al. (2017) has conducted a brief study of the cyber crimes and cyber laws prevailing in India, where the data has been derived from previous research findings and journals. They have put forth numerous suggestions to the general public on how to protect themselves from cyber criminals. Michael L. Gross, et al. (2017) has analysed the effects of cyber terrorism on psychological well- being, public confidence and political attitude. It was an empirical research where an online survey experiment was conducted on 522 Israeli adults were assigned to three treatments after which they answered a series of psychological and political questions. They found out that cyber terrorism aggravates anxiety and personal insecurity and that many people were willing to support strong government policies against it.

IV. METHODOLOGY & RESULTS

Descriptive research has been carried out which helps us to understand the characteristics of an individual or a group. The sampling method used here is convenient sampling where the samples have been chosen based on ease of access of availability. The sample size is 1540. Age, Gender and Occupation are the independent variables. Cyber-crime awareness, the main cause of cyber-crime and the most popular cyber-crime are the dependent variables used in this study. The tools used here are Chi-Square, Independent Sample t test and ANOVA.

V. ANALYSIS AND DISCUSSION

Null Hypothesis: There is no significant association between the cyber-crime awareness and the age of the respondents.

Alternate Hypothesis: There is a significant association between the cyber-crime awareness and the age of the respondents.

Table 1: Crosstabulation – Awareness of Cyber Crime and Age

Age	Awareness of Cyber Crime		Total
	Yes	No	
Less than 25 years	399	212	611
26-35 years	211	172	383
36-45 years	207	115	322
46-60 years	104	71	175
Above 60 years	34	15	49
Total	955	585	1540

Table 2: Chi-Square Tests - Awareness of Cyber Crime and Age

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	12.930	4	0.012

Interpretation:

Since p value (0.012) is less than 0.05, the null hypothesis is rejected. Therefore, there is a significant association between the cyber-crime awareness and the age of the respondent. It shows that the awareness of cyber-crimes depends upon the age of the respondent.

Null Hypothesis: There is no significant difference between the main cause of cyber-crime and the gender.

Alternate Hypothesis: There is a significant difference between the main cause of cyber-crime and the gender.

Table 3: Main Cause of Cyber Crime and Gender

Gender	N	Mean	Std. Deviation	Std. Error Mean
Male	803	2.41	1.147	.040
Female	737	2.41	1.226	.045

Table 4: Independent Samples Test - Main Cause of Cyber Crime and Gender

	t	df	Sig. (2-tailed)
Independent Sample t test	0.087	1538	0.931

Interpretation:

Since p value (0.931) is more than 0.05, the null hypothesis is accepted. Therefore, there is no significant difference between the main cause of cyber-crime and gender. It shows that the opinion regarding the main cause of cyber-crime does not differ with gender.

Null Hypothesis: There is no significant difference in the mean scores of level of agreeability towards the most popular cyber-crime among the occupational groups.

Alternate Hypothesis: There is a significant difference in the mean scores of level of agreeability towards the most popular cyber-crime among the occupational groups.

Table 5: ANOVA - Most Popular Cyber Crime and Occupation

		Sum of Squares	df	Mean Square	F	Sig.
Cyberbullying	Between Groups	32.992	2	16.496	18.081	.000
	Within Groups	1402.294	1537	.912		
	Total	1435.286	1539			
Identity theft	Between Groups	15.345	2	7.673	10.435	.000
	Within Groups	1130.158	1537	.735		
	Total	1145.504	1539			
Piracy	Between Groups	34.420	2	17.210	17.587	.000
	Within Groups	1504.070	1537	.979		
	Total	1538.490	1539			
Transaction fraud	Between Groups	69.283	2	34.641	33.448	.000
	Within Groups	1591.857	1537	1.036		
	Total	1661.140	1539			
Hacking	Between Groups	164.496	2	82.248	59.236	.000
	Within Groups	2134.088	1537	1.388		
	Total	2298.584	1539			

Interpretation

Since p value (0.000) is less than 0.01, the null hypothesis is rejected. Therefore, there is a significant difference in the mean scores of level of agreeability towards the most popular cyber-crime among the occupational groups. It was found that opinion regarding the most popular cyber-crime differs depending upon the occupation of the respondent.

VI. CONCLUSION

Cyber-crime is the use of computer and Internet by criminals to conduct fraud and scams against many organisations, companies or the general public. For example, email phishing, credit card scams, child pornography, identity theft, etc. With advancements and developments in technology, cyber criminals are discovering new methods and techniques to commit crimes through the Internet. It was found that there is a significant association between the cyber-crime awareness and the age of the respondent, there is no significant difference between the main cause of cyber-crime and gender and that there is a significant difference in the mean scores of level of agreeability towards the most popular cybercrime among the occupational groups. Since cybercrime is increasing day-by-day, it's imperative that the general public is aware of protecting themselves against these cybercrimes. Some of the measures are using a reliable security software, strong passwords, keeping certain information private, and preventing cybercrime with hotspot shield. Each person needs to be aware and vigilant of their virtual reality, in order to protect themselves against any form of cybercrime.

REFERENCES

1. Hannarae Lee, Hyeyoung Lim, Awareness and Perception of Cyber Crimes and Cyber Criminals, International Journal of Cybersecurity Intelligence & Cybercrime, 2019, Vol 2, Issue 1, Page 1-3 (Hannarae Lee 2019)
2. Er. Navneet Kaur, Introduction of Cyber Crime and its Type, International Research Journal of Computer Science, ISSN: 2393- 9842, 2018, Vol 5, Issue 8, Page 435- 439(Kaur 2018)
3. Muhammad Dharma Tuah Putra Nasution, Andysah Putera Utama Siahann, Yossie Rossanty, Solly Aryza, The Phenomenon of Cyber Crime and Fraud Victimisation In Online Shop, International Journal of Civil Engineering and Technology, ISSN: 0976- 6316, 2018, Vol 9, Issue 6, Page 1583- 1592 (Siahaan and Muhammad Dharma Tuah, n.d.)
4. Kyung-Shick Choi, Claire Seunguen Lee, The Present and Future of Cybercrime, Cyberterrorism and Cybersecurity, International Journal of Cybersecurity Intelligence & Cybercrime, 2018, Vol 1, Issue 1, Page 1-4(Kyung-Shick Choi 2018)
5. K. Jaishankar, Cyber Criminology as an Academic Discipline: History, Contribution and Impact, International Journal of Cyber Criminology, ISSN: 0973-5089, 2018, Vol 12, Issue 1, Page 1-8(Jahankhani 2018)
6. Juneed Iqbal, Bilal Maqbool Beigh, Cybercrime in India: Trends and Challenges, International Journal of Innovation & Advancement in Computer Science, ISSN: 2347-8616, 2017, Vol 6, Issue 12, Page 187- 196(Juneed Iqbal 2018)
7. Dambo Itari, Ezimora Okezie Anthony, Nwanyanwu Mercy, Cyber Space Technology: Cyber Crime, Cyber Security and Models of Cyber Solution, a Case Study of Nigeria, International Journal of Computer Science and Mobile Computing, ISSN: 2320- 088X, 2017, Vol 6, Issue 11, Page 94- 113(Dambo Itari, Ezimora Okezie Anthony, Nwanyanwu Mercy 2017)
8. Johannes Xingan Li, Cyber Crime and Legal Countermeasures: A Historical Analysis, Official Journal of the South Asian Society of Criminology and Victimology, ISSN: 0973- 5089, 2017, Vol 12, Issue 2, Page 196- 207(Li 2017)
9. Animesh Sarmah, Roshmi Sarmah, Amlan Jyothi Baruah, A brief study on Cyber Crime and Cyber Laws of India, International Research Journal of Engineering and Technology, ISSN: 2395- 0056, 2017, Vol 4, Issue 6, Page 1633- 1641(Animesh Sarmah, Roshmi Sarmah, Amlan Jyothi Baruah 2017)
10. Michael L. Gross, Daphna Canetti, Dana R. Vashdi, Cyber Terrorism: It's Effects on Psychological Well-Being, Public Confidence and Political Attitude, Journal of Cyber Security, DOI: 10.1093, 2017, Vol 3, Issue 1, Page 49-58(Gross, n.d.)
11. Aparna Srivastava, Analyzing Cyber Crime & Cyber Laws in India, VSRD International Journal of Technical & Non- Technical Research, ISSN: 0976- 7967, 2017, Vol 3, Issue 2, Page 44- 46(Srivastava 2017)
12. Anuraj Singh, Studies Report on Cyber Law in India & Cybercrime Security, International Journal of Innovative Research in Computer and Communication Engineering, ISSN: 2320- 9801, 2017, Vol 5, Issue 6, Page 11273-11279(Singh 2017)
13. Jitender Kumar, Cyber Crime in India: An Overview, Imperial Journal of Interdisciplinary Research, ISSN: 2454? 1362, 2017, Vol 3, Issue 4, Page a963-967(Kumar 2017).