Public Awareness on Cyber Crime with Special Reference to Chennai

Samrin Sulaiman, Sreeya B

Abstract

The rapid advancements in technology have completely digitalised our lives, making daily activities like grocery shopping, education, banking, and communication 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 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 the 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 to availability. The sample size is 1540. Age, Gender, and Occupation are the independent variables. Cybercrime awareness, the main cause of cybercrime, and the most popular cybercrime 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 cybercrime awareness and the age of the respondent and that there is no significant difference between the main cause of cybercrime 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 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. 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 (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 cybercrime 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 research 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-
PUBLIC AWARENESS ON CYBER CRIME WITH SPECIAL REFERENCE TO CHENNAI

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

<table>
<thead>
<tr>
<th>Age</th>
<th>Awareness of Cyber Crime</th>
<th>Yes</th>
<th>No</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 25 years</td>
<td>399</td>
<td>212</td>
<td></td>
<td>611</td>
</tr>
<tr>
<td>26-35 years</td>
<td>211</td>
<td>172</td>
<td></td>
<td>383</td>
</tr>
<tr>
<td>36-45 years</td>
<td>207</td>
<td>115</td>
<td></td>
<td>322</td>
</tr>
<tr>
<td>46-60 years</td>
<td>104</td>
<td>71</td>
<td></td>
<td>175</td>
</tr>
<tr>
<td>Above 60 years</td>
<td>34</td>
<td>15</td>
<td></td>
<td>49</td>
</tr>
<tr>
<td>Total</td>
<td>935</td>
<td>585</td>
<td></td>
<td>1540</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Pearson Chi-Square</th>
<th>df</th>
<th>Asymp. Sig. (2-sided)</th>
</tr>
</thead>
<tbody>
<tr>
<td>12.930</td>
<td>4</td>
<td>0.012</td>
</tr>
</tbody>
</table>

Table 3: Main Cause of Cyber Crime and Gender

<table>
<thead>
<tr>
<th>Gender</th>
<th>N</th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>Std. Error Mean</th>
</tr>
</thead>
<tbody>
<tr>
<td>Male</td>
<td>803</td>
<td>2.41</td>
<td>1.147</td>
<td>0.040</td>
</tr>
<tr>
<td>Female</td>
<td>737</td>
<td>2.41</td>
<td>1.226</td>
<td>0.045</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Independent Sample t test</th>
<th>t</th>
<th>df</th>
<th>Sig. (2-tailed)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0.087</td>
<td>1538</td>
<td>0.931</td>
</tr>
</tbody>
</table>

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.
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 agreeableness towards the most popular cybercrime 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 agreeableness 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