Public opinion on cyber Crime

V.S.K.Suryan, Sreeya.B

Abstract Cybercrime, or computer orientated crime, is crime that involves a laptop and a community. Only 38 percent of worldwide agencies claim they're organized to deal with a sophisticated cyber assault. Cybercrimes can be defined as: "Offences which are committed towards individuals or groups of people with a crook motive to intentionally harm the popularity of the victim or reason bodily or mental damage, or loss, to the sufferer directly or circuitously, using current telecommunication networks along with Internet (networks together with however no longer restricted to Chat rooms, emails, word boards and organizations) and cell telephones (Bluetooth/SMS/MMS)" Descriptive analysis is used. Convenience sampling method is used for selecting sample size 1480 samples. Independent variable such as age, gender, and educational qualification are used. Percentage analysis, chi square, correlation, independent sample t test, and ANOVA used for the study.

Keywords:Intentionally,Circuitously,Telecommunication,Additionally ,Offences, restricted

I. INTRODUCTION

There is a hacker attack every 39 seconds, affecting one in 3 Americans each year. 95 percentage of breech facts came from 3 industries in 2016: Government, retail, and technology.43 percentage of cyber attacks target small business. Sixty four% of corporations have experienced web-primarily based assaults. 62% skilled phishing & social engineering assaults. 59% of organizations experienced malicious code and botnets and 51% experienced denial of service assaults.The common value of a information breach in 2020 will exceed $150 million, as greater commercial enterprise infrastructure receives related.Over 75% of healthcare industry has been infected with malware over closing 12 months.

Large-scale DDoS assaults up 140 percentage in 2016's fourth quarter.Approximately $1 trillion is anticipated to be spent globally on cybersecurity from 2017 to 2021.

Unfilled cybersecurity jobs worldwide will reach three.Five million by using 2021. More than 209,000 cyber security jobs inside the U.S. Are unfilled, and postings are

up 74% over the past five year.By 2020 there could be kind of 200 billion linked gadgets. The danger is actual with IoT and its growing. According to figures compiled inside a latest Symantec Internet Security Threat Report, there are 25 related gadgets in step with one hundred population within the US.Only 38 percent of worldwide agencies claim they're

organized to deal with a sophisticated cyber assault,The aim of the study is to understand about cyber crime,The aim of the study is to understand about cyber crime. The objectives of the study are to know about the awareness of cyber crime, to analyse the association between the effect of cybercrime and the area of the respondent, to identify the level of agreeability regarding the cyber crime, and to analyse the relationship between online risks and education

II. LITERATURE REVIEW

Neelesh Jain,Vibhash Shrivasta(2018) The researcher has revealed that internet is described as a wonderful tool he also agrees that E-crime presents a new form of issues and H-tech criminals, he gives a overview of cyber crimes. Amna Saad, Ahmad Roshidi Arman,(2017) The researcher has provided new information on the field study of networking system, because cyber crime is becoming very widespread and its imperative to improve measures to contract such threats. and also,Danielle M Cummins and,Siegfried(2017) The researcher has revealed the prevalence of sexting behaviour among adults, and the relationship between sexting and moral foundation, self esteem, and individual differences, Alison Marganski(2017)The author investigates personal and social situational factors that influences sexting among samples of young adults in two countries with similar rates of technology use. Amy Adele Hasinoff(2017)He reveals that teens who concisely create and share sexual images of themselves criticised In media and criminalized in law. But there is less specific attention to those who distribute such images without permission.Kimberly O Cour, Michelle Drowin, (2017)The researchers analysed the sexting laws of 50 states in USA and the District of Columbia. They also examined laws related to aggravated circumstances such as in case of a revenge upon.Jo AME Suenny and Johnslack(2017)The researcher has revealed there has been a global decrease in sexual explicit social media message and consensual sexting among teenagers and adults of all ages. Soumi Satish (2017)the author reveals that the internet is growing very rapidly in india but internet has also many disadvantages.

Udris Rcins(2016)The authors reveal the continuous spread of information and considers technology has enabled sn increasing number of youth access to the internet leading to rise of legal activities and hacking problems.Kigali Alex (2016) The author reveals that cybercrime is a worldwide problem with the global research. Crimes do not respect national boundaries and so can be sent to and for any part in the world. ACAR Kunal Veli (2016) The researcher reveals and examines the sexualness of children abused in cyberspace which has gained honotonity despite the fact that it has recently emerged and it is also considered one of the most significant online threat to the children. Lavorgana, Anita (2016)The author says this paper is based on discourse analysis of policy document departs from a critic of the just position of the term various and organised in policies against organised crime in UK. Nycyk, Michael (2016) The researcher reveals that the hacker firms are places for new hackers, new babies to find information on hacking practices and to become part of a community. Aavan, Imran (2016)The authors reveals that the Facebook has become one of the fastest growing social media platforms. Lacbon, Wesley (2016)The author reveals that Silk Road was a online marketplace through which the consumers bought and sold drugs and other things.

III. METHODOLOGY

Descriptive analysis is used. Convenience sampling method is used for selecting sample size 1480 samples. Independent variable such as age, gender, and educational qualification are used. Percentage analysis, chi square, correlation, independent sample t test, and ANOVA used for the study.

IV. ANALYSIS AND DISCUSSION RESULTS

Null hypothesis:

There is no significant association between victim of cyber crime and area of the respondent

Alternate hypothesis:

There is significant association between victim of cyber crime and area of the respondent

Table 1: Chi Square test: Victim of Cyber Crime and Area

	Value	df	p-value
Pearson Chi-Square	48.478	9	0.000

Source: Primary data

Using Chi square test, it was found that p value is less than 0.05, which shows that null hypothesis is rejected. Therefore, there is significant association between victim of cyber crime and area of the respondent. Nearly 30% of the respondents are not been a victim of cyber crime. It also shows that majority of the Central Chennai respondents are victim of cyber crime.

Null Hypothesis (H0):

There is no significant difference in the mean scores of level of agreeability regarding safety among the age groups.

Alternate Hypothesis (H1):

There is significant difference in the mean scores of level of agreeability regarding safety among the age groups.

Table 2: ANOVA for Safety and Age

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	3.880	3	1.293		
Within Groups	1809.606	1476	1.226	1.055	.367
Total	1813.486	1479			

Source: Primary data

Since the p value is greater than 0.05, it was found that there is no significant difference in the mean scores of level of agreeability regarding safety among the age groups. The level of agreeability regarding online transaction safety does not vary with age groups.

Null Hypothesis:

There is no significant relationship between the online risk reduction through OTP and the educational qualification

Alternate Hypothesis:

There is significant relationship between the online risk reduction through OTP and the educational qualification

Table 3: Correlation – Online Risk and Educational Qualification

Variable 1	Variable 2	p-value	Correlation coefficient
OTP reduces Online Risk	Educational Qualification	0.025	0.341*

Source: Primary data

Correlation analysis is used to test the relationship between the online risk reduction through OTP and the educational qualification. Since p<0.05, null hypothesis is rejected at 5% level of significance. There is significant relationship between the online risk reduction through OTP and the educational qualification. But there is a low correlation between the online risk reduction through OTP and the educational qualification.

Null hypothesis:

There is no significant difference between the awareness of cyber crime and the gender.

Alternate hypothesis:

There is significant difference between the awareness of cyber crime and the gender.

Table 4: Awareness of Cyber Crime and Gender

	Gender	N	Mean	Std. Deviation	Std. Error Mean
Awareness of Cyber Crime	Male	883	1.33	.471	.016
	Female	597	1.31	.461	.019

Source: Primary data

Table 5: Independent Sample t test: Awareness of Cyber Crime and Gender

	Value	df	p-value
Independent Sample t test	1.022	1478	0.039

Source: Primary data

Using Independent sample t test, it was found that p value is less than 0.05, which shows that null hypothesis is rejected. Therefore, there is significant difference between the awareness of cyber crime and the gender. It also shows that female are less awareness about cyber crime than male.

Null hypothesis:

There is no significant association between the level of agreeability of government accessing my account and the occupation.

Alternate hypothesis:

There is significant association between the level of agreeability of government accessing my account and the occupation.

Table 6: Chi Square test: Government Access and Occupation

	Value	df	p-value
Pearson Chi-Square	8.269	8	0.408

Source: Primary data

Using Chi square test, it was found that p value is greater than 0.05, which shows that null hypothesis is accepted. Therefore, there is no significant association between the level of agreeability of government accessing my account and the occupation. Nearly 30% of the respondents responded as neutral for government accessing the account.

V. CONCLUSION

It may be visible that the chance of laptop crime is not as massive because the authority claim. This manner that the approach s that they introducing to combat it represents an unwarranted attack on human rights and isn't proportionate to the hazard posed by way of cyber-criminals. Part of the hassle is that there are no reliable records on the hassle; which means it's miles tough to justify the expanded powers that the Regulation of Investigatory Powers Act has given to the government. These powers can also be ineffective in dealing with the trouble of pc. The international treaties being drawn up to cope with it are so vague that they're sure to be ineffective in managing the problem. It will even suggest the civil liberties might be unjustly stricken by the phrases of the treaties because they could, conceivably, suggest that everybody who owns a computer fitted with a modem may be suspected of being a hacker.

REFERENCES

1. https://www.researchgate.net/publication/275709598_CYBER_CRIME_CHANGING_EVERYTHING_-_AN_EMPIRICAL_STUDY
2. https://www.ijera.com/papers/Vol2_issue2 AG22202209.pdfhttps://www.researchgate.net/publication/241689595_A_Study_on_Cyber_Crime_in_India
3. https://www.slideshare.net/mobile/WhitneyBolton1/cybercrime-research-paper
4. https://www.enotes.com/research-starters/social-impacts-cyber-crimehttp://theconversation.com/global/topics/cybercrime-3809
5. https://www.irjet.net/archives/V4/i6/IRJET-V4I6303.pdf
6. https://www.ijrter.com/papers/volume-3/issue-10/a-study-of-cyber-crime-awareness-for-prevention-and-its-impact.pdf
7. https://www.scribd.com/document/262670458/Research-Paper-Cyber-Crime-India
8. https://www.rand.org/topics/cybercrime.html
9. http://paper.ijcsns.org/07_book/201202/20120214.pdf
10. https://www.papermasters.com/cybercrime.html
11. http://www.cameron.edu/uploads/54/8b/548b8ace3f40611b5f8102bad86fb443/2_Hackers.docx