IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

"A Study On Cybercrime Its Impact And Awareness Towards Society"

NAMRATA K (Assistant Professor) **CHETHAN V K(Assistant Professor)**

City College, Jayanagar **City College, Jayanagar**

Abstract

Cybercrime is targeted as the criminal activity which either targets or uses a computer, a computer network or a device which is networked. Most of the cybercrime are committed by either cybercriminals or hackers who want to make money. However, occasionally cybercrime main focus is to damage computers or networks for many reasons other than profit. As in today's world technology is continuously upgrading in many ways Cybercrime and hacking activities are also growing very drastically. As per the research cybercrime is considered as the fastest growing area of the crime.

Earlier, Cybercrime was committed by many small group or individuals, but now it has become a place for Professional hackers, organized hackers, children and adolescents between the age group of 6- 18 years, scammers, phishes, insiders, malware authors, spammers, etc to be carried as a source of income. Few of the common Cybercrime which is been taken place in India are frauds related which credit cards, robbery of bank, downloading illegally, industrial espionage, child pornography, kidnapping of children via chat rooms, scams, cyber terrorism, creation and or distribution of various viruses, spam and so on.

As we are living in a digital age, cyberspace is just not limited to one's boundary but rather it covers an entire world. As a result cybercrime is increasing drastically in all the countries including India. The biggest challenge faced by cybercrime is its dynamic nature of the ongoing evolution of digital technology. As the digital landscape expands, so does the threat of cyber crime increases. In India, the Information Technology Act, 2000, serves as the backbone of the legal framework used for combating cyber crime and promoting cyber security. Through a combination of robust legislation, technological advancements, and public awareness, India can build a safer digital environment towards its citizens and effectively combat cyber crime. As a result many new cybercrime methods and techniques come into practice it is essential to continuously update and strengthen cyber laws to keep an upgrade with evolving cyber threats.

Key words: Cyber-Crime, Cyber-Criminals, Awareness, Cyber Security, Internet, IT Act.

Introduction

Cybercrime can be committed by the technology use where the device is used as a tool for committing the crime and the target of the crime. One of the examples includes malware which targets the victims to delete or damage the data by hacking and for financial gain. Other form of Cybercrime includes cyber enabled fraud and data theft.

Moreover, the study seeks to assess the level of awareness and preparedness among individuals and organizations in confronting cyber threats. While some may possess a keen understanding of cyber security best practices and actively implement preventive measures, others may remain vulnerable due to a lack of awareness or resources. By identifying knowledge gaps and barriers to awareness, we can develop targeted strategies to enhance cyber security education and promote a culture of vigilance in cyberspace.

In addressing these objectives, this study aims to contribute to the body of knowledge on cybercrime and its societal impact, ultimately guiding efforts to strengthen resilience and mitigate risks in the digital age. By fostering collaboration among stakeholders and raising awareness among the populace, we endeavor to build a safer and more secure digital environment for present and future generations.

In the subsequent sections, we will delve into the various forms of cybercrime, explore its impact on society, assess the level of awareness among individuals, and propose recommendations for enhancing cyber security efforts. Through a comprehensive analysis of these factors, we aim to provide insights and actionable strategies for combating cybercrime and promoting a culture of cyber resilience in society.

Cyber Crime in World

▪ 2018	▪ 208,456 to 212,485 Cases
▪ 2019	▪ 394,499 to 1,158,208 Cases
▪ 2020 – 2021	▪ 1,402,809 Cases

Below table showing the number of Cybercrime cases in India

2022	26,121
2021	27,248
2020	21,796
2019	12,317
2018	11,592

Emerging cybercrime statistics and trends

Types of Cybercrimes:

Cybercrime ranges variety of activities. Cybercrime can be basically divided into three major categories.

A. Cybercrimes against persons like harassment leading to cyberspace or by the use of cyberspace. Harassment by sexual, racial, religious, or other.
B. Cybercrimes against property like computer wreckage (destruction of others' property), transmission of harmful programs by various websites, unauthorized trespassing, unauthorized possession and leaking of computer information.

C. Cybercrimes against government like Cyber terrorism. The IT can be used by the individual and terrorist group to attack for information exchanging and making electronically threats.

Who are the Cyber Criminals? Cyber Criminals are differentiated among 4 groups:

- **Kids (**age group 9-16): It is very hard to believe but the young generation knowingly or unknowingly involved in Cyber activities. Most of them are considered as teenagers who things that it is a matter of pride to hack any computer system or a website. Sometimes they may commit the crimes without actually knowing that they are doing is a crime.
- **Organized Hacktivists:** Group of hacker combines together for a particular motive known as hacktivists. Such groups operate for a political basis. In other cases it motivates religious or social activism or any other.
- **Disgruntled Employees:** As there is increase in being dependent on computers and the automation of processes, disgruntled employers are expected to do lot more harm their employers just by committing crime using computers so that they can bring their entire system down.
- **Professionals Hackers:** One of the highest earning professions is ethical hackers for network management who operates for computer and IT security. Most of the hackers are employed by the rivals organizations so that they can steal other industrial information and secrets which could be beneficial for them, hacking can utilize the required information from rival companies.

LITERATURE REVIEW:

Aparna and Chauhan (2012): The authors conducted a research paper in Tricity related with awareness on cybercrime which stated that by giving due importance to Cybercrime that can be an efficient tool to reduce or prevent the Cybercrimes. They also concluded that it remains the responsibility of the government and the net user to ensure a safe, secure and trustworthy with computing environment.

Mehta and Singh (2013):

The survey was conducted by the author stating the awareness about cyber laws in Indian society. He found that there is a drastic difference between the awareness level of male and female users of the internet services. In simple words it states that the male netizens are more aware of cyber laws as compared to the women users.

Hasan et al., (2015):

Conducted a survey to analyze the cybercrime awareness in Malaysia and they found that female students are more aware of cybercrime as compared to male students.

Archana Chanuvai Narahari and Vrajesh Shah (2016):

The author in this conducted a survey on 100 respondents to analyze whether netizens are really aware of cyber-crimes. They found that the respondents are somewhat aware of the cyber-crimes, cyber security but still there is a need to increase awareness among them.

Steps to Prevent Cyber Crimes

- Personal information is good when it personal but it's dangerous when personal information is publicly on websites. This is equal to disclosing one's identity to a stranger in public place.
- Avoid sending photographs to while chatting with friends, strangers and online particularly, they are many incidents specifying misuse of photographs.
- Never disclose bank details, OTPs and information about personal documents, as its can lead to malpractices.
- Avoid visiting unknown websites and downloading unknown apps.
- Always use cyber secured apps.

Certainly, here are some potential impacts of the study titled "A Study on Cybercrime: Its Impact and Awareness towards Society":

1. **Increased Understanding**: The study can lead to a deeper understanding of the various forms and implications of cybercrime within society.
2. **Heightened Awareness:** By shedding light on the prevalence and severity of cybercrime, the study can raise awareness among individuals, businesses, and policymakers about the importance of cyber security measures.
3. **Policy Implications**: The findings of the study may inform the development of policies and regulations aimed at combating cybercrime and protecting society from its adverse effects.
4. **Behavioral Changes**: Increased awareness resulting from the study might lead to changes in online behavior, with individuals and organizations adopting more cautious and security-conscious practices.
5. **Empowerment of Stakeholders**: The study can empower individuals, businesses, and governments with knowledge and resources to better protect themselves against cyber threats.
6. **Economic Impacts**: Understanding the economic repercussions of cybercrime highlighted in the study can drive investment in cybersecurity measures and technologies, ultimately safeguarding financial resources.
7. **Psychological Effects**: Awareness of the psychological toll of cybercrime, such as stress, anxiety, and fear, can prompt initiatives to provide support and resources for affected individuals.
8. **Trust Building:** Efforts to enhance awareness and mitigate cyber threats can contribute to rebuilding trust in digital platforms, fostering a more secure online environment.
9. **Education and Training**: The study may underscore the importance of cyber security education and training programs, leading to increased investment in initiatives aimed at improving digital literacy and resilience against cyber threats.
10. **International Collaboration**: Recognizing cybercrime as a global issue, the study may stimulate collaboration among nations to develop coordinated strategies for prevention, detection, and response.

Overall, the impact of the study on cybercrime, its implications, and societal awareness can be multifaceted, influencing various aspects of policy, behavior, and collaboration in the realm of cyber security.

Awareness and Perception of Cybercrime

Despite the prevalence of cybercrime, there are significant knowledge gaps and misconceptions among the public. Many individuals underestimate the risks of cyber threats and fail to take adequate precautions to protect themselves online. Education and training programs play a crucial role in raising awareness and promoting cyber security best practices. The media and pop culture also influence public perceptions of cybercrime, shaping attitudes towards online security and privacy.

Societal Responses to Cyber crime:

Governments, law enforcement agencies, private sector organizations, and civil society groups play essential roles in combating cybercrime. Legal and regulatory frameworks establish the basis for prosecuting cybercriminals and enforcing cyber security standards. Law enforcement initiatives aim to identify and apprehend cybercriminals, often through collaboration with international partners. Public-private partnerships facilitate information sharing and collaboration on cyber security initiatives. Cyber security awareness campaigns raise public awareness of cyber threats and promote best practices for online safety.

Recommendations and Future Directions:

To address the challenges posed by cybercrime, it is essential to enhance education and training efforts, strengthen collaborative initiatives, leverage technology for defense, and promote responsible online behavior. Continued research and innovation are needed to develop new approaches to cybersecurity and adapt to evolving cyber threats.

RESEARCH METHODOLOGY:

To calculate the awareness of cyber-crime and security, the following methodology has been applied:

a) Objectives of the study:

1. To understand the bridge between education level of the respondent and the awareness of cyber-crime and security.
2. To calculate the number of times respondents have been a victim of cybercrime
3. To examine the usage of regular internet by the respondents.
4. To identify various level of awareness on safety, while using personal computers and internet among internet users regarding cyber-crimes.
5. To measure various situations experienced by the respondents.

Nature and Sources of data

Primary data: With the help of primary data the collection of information was gathered by personal survey using the questionnaire method.

Secondary data Through published journals, internet and the articles published in the newspaper, collection of information has be taken for the secondary data.

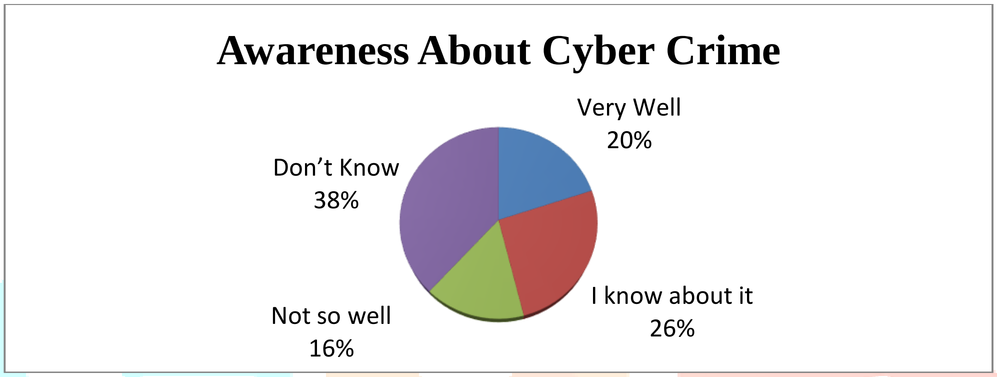
Sample size: The sample size used here is 50

Sample Method: The sample method which is been used is descriptive method which involved collection of data through survey, observation and case study. Its aims to observe understand the document and create a thorough profile of the subject under study, using often exploring patterns, behaviors or attributes.

Results and interpretation

Table 1: Demonstrate the awareness about cyber crime by the respondents.

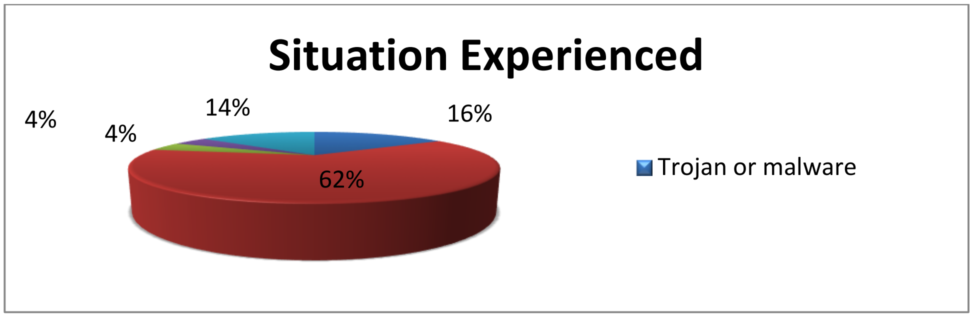
Category	**Number of respondents**	**Percentage**
Very well	10	20
I know about it	13	26
Not so well	8	16
Don't know	19	38
Total	**50**	**100 %**



Analysis: From the above, table represents that the awareness about cybercrime by the respondents not so well know which was for 16% and 20% respondents were very well aware about Cybercrime. When it comes to don't know 38% are totally unaware about Cybercrime.

Table 2: Demonstrate any of the below mentioned situation experienced by the respondents

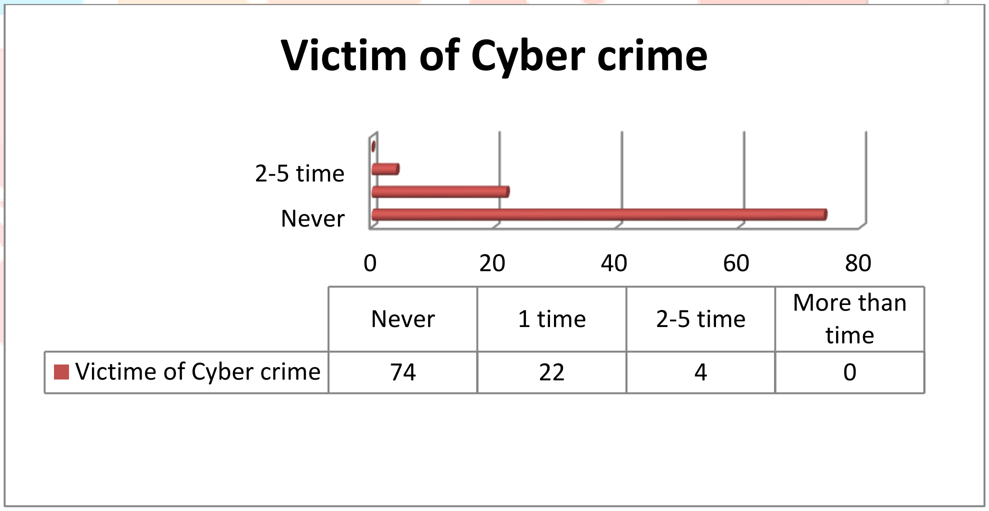
Category	**Number of Respondents**	**Percentage**
Trojan or malware	08	16
Auto generated mails to your inbox	31	62
Publishing obscure material on your profiles	02	04
Confidential reports/information being hacked	02	04
Never experienced such situation	07	14
Total	**50**	**100%**



Analysis: From the above table represents that, most of the auto generated mails to inbox are situations experienced by the respondents, 16% of malware and Trojan are experienced by the respondents. 14% are the respondents who have never experienced such situation. At the end 4% of respondents experienced publishing obscure material on their profile and confidential reports/information being hacked.

Table 3: Mention how many times respondents have been a victim of cybercrime.

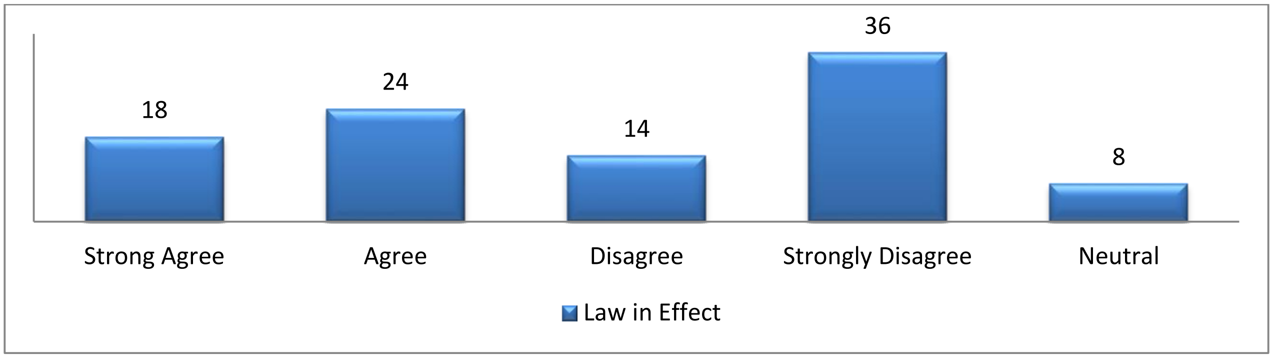
Category	**Number of respondents**	**Percentage**
Never	**37**	**74**
1 time	**11**	**22**
2-5 times	**2**	**04**
More than 5 times	**0**	**00**
Total	**50**	**100%**



Analysis: From the above the table represents, 4% of the respondents have been victims of cyber crime 2-5 times. 22% of the respondents have been victims of cyber crime 1 time. Almost 74% of the respondents have never been victim of cyber crime.

Table 4: Demonstrate that the respondents think that the laws in effect are able to control cyber criminals

Category	**Number of respondents**	**Percentage**
Strongly agree	**9**	**18**
Agree	**12**	**24**
Disagree	**7**	**14**
Strongly Disagree	**18**	**36**
Neutral	**4**	**08**
Total	**50**	**100%**



Analysis: From the above table 36% of respondents think that the laws in effect are able to control cybercrime. 24% of respondents agree and 18% of respondents strongly agree with the laws in effect will be able to control cyber crime. 8% are neutral respondents were as 14% respondents disagree and think that the laws in effect are able to control cyber crime.

Findings:

- It was examined that 38% of respondents were not aware about the cybercrime. From online hacking to phishing respondents were not aware about the fraud happening around due to lack of awareness.
- Experienced auto generated mails to their inbox was about 62% of respondents
- Only 16% of respondents experienced Trojan and malware practices
- Almost 22% of respondents have been a victim of cyber crime
- It was found that 36% of respondents strongly disagree about the law in effect are able to control cybercrime.

Sources:

Certainly! Here are some references for a study on "Cybercrime: Its Impact and Awareness towards Society":

- Akdeniz, Y., & . Walker, C. (2018). Cybercrime: Key Issues and Debates. Routledge.
- Holt, T. J., & Bossler, A. M. (2016). Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. Routledge.
- Grabosky, P. N. (2016). Cybercrime: The Transformation of Crime in the Information Age. Cambridge University Press.
- Jaishankar, K. (Ed.). (2016). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press.
- Wall, D. S. (2018). Cybercrime and the Culture of Fear: Social Science Fiction(s) and the Production of Knowledge about Cybercrime. Information & Communications Technology Law, 27(2), 195-213.
- Ruud, J., & Rollins, J. (2019). Cybercrime: A Reference Handbook. ABC-CLIO.

- Goodall, G., & Thorsen, E. (2019). Cybercrime and its Victims. Routledge.
- Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2018). Digital Crime and Digital Terrorism (4th ed.). Pearson.
- Grabosky, P. N. (2017). Understanding Cybercrime: A Guide for Developing Countries. Cambridge University Press.
- Kshetri, N. (2017). Cybercrime and Cybersecurity in the Global South. Springer.

These references cover various aspects of cybercrime, including its definitions, forms, impacts on society, and strategies for prevention and response. They provide a solid foundation for conducting a comprehensive study on cybercrime and its implications for societal awareness.

Websites:

1. https://www.kaspersky.com/resource-center/threat
2. https://aag-it.com/the-latest-cyber-crime-statistics/
3. https://purplesec.us/resources/cyber-security-statistics/
4. https://us.norton.com/blog/emerging-threats/cybersecurity-statistics

Conclusion:

As we are living in the digital age where every nation is looking forward to increase in the technology, it is important to be aware about the pros and cons of the ongoing evolution of the digital technology. Cybercrime are the fastest going crimes in the world where malpractices like hacking, malware, phishing, internet thefts, Trojan horses, stealing money while money transferring, etc. It is better to be safe when it come to our personal information. No matter what any personal information shouldn't be disclosed to a stranger, outsider or anyone who is not concerned to us. In India, Information Technology Act, 2000 severs as backbone for combating and promoting cyber security. Therefore each and every individual should be aware about the incident happening towards the technology and be away from the crime happening all over world. The government should spread more awareness and take more precaution as it takes care of other criminal acts.

Furthermore, the study has revealed disparities in the level of awareness and preparedness among different segments of society. While some individuals may possess a high level of awareness and actively employ preventive measures, others may lack the necessary knowledge and resources to protect themselves effectively. Therefore, efforts to enhance cybercrime awareness and promote cyber security education are essential in empowering individuals and organizations to defend against cyber threats proactively.

In light of these findings, it is imperative for governments, law enforcement agencies, private sector entities, and civil society organizations to collaborate closely in combating cybercrime. This collaboration should encompass the development and enforcement of robust legal and regulatory frameworks, the allocation of resources for cyber security initiatives, the promotion of international cooperation, and the implementation of effective awareness campaigns.

Ultimately, the study emphasizes that addressing cybercrime requires a multifaceted approach that combines technological solutions, policy interventions, and societal awareness efforts. By working together to raise awareness, enhance cyber security capabilities, and foster a culture of vigilance in cyberspace, we can build a safer and more resilient digital environment for all members of society.