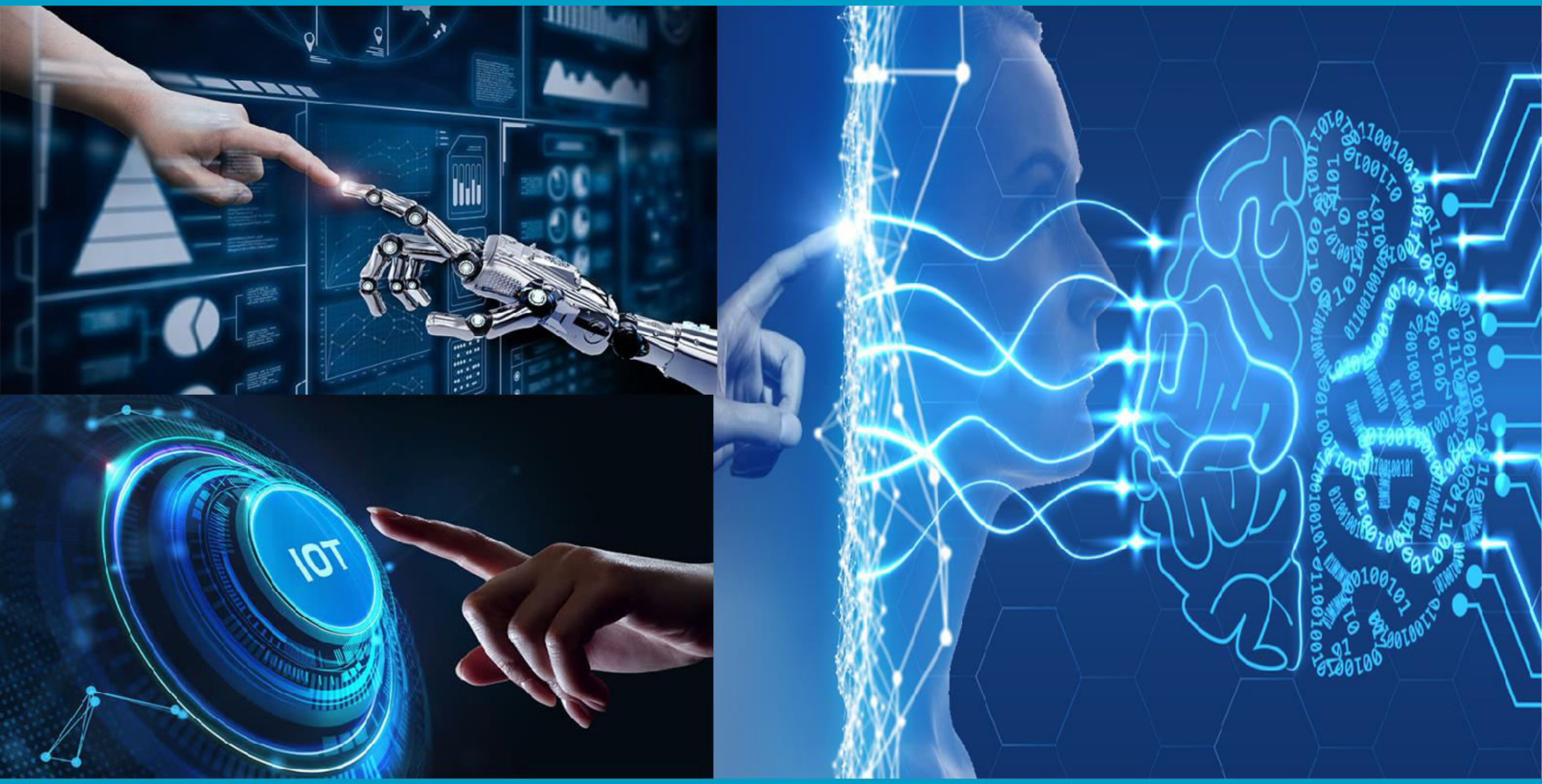
IJMRSETM

e-ISSN: 2395 - 7639



INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

Volume 10, Issue 5, May 2023

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.580

☎ +91 99405 72462 ✆ +9163819 07438 ✉ ijmrsetm@gmail.com @ www.ijmrsetm.com

| ISSN: 2395-7639 | www.ijmrsetm.com | Impact Factor: 7.580| A Monthly Double-Blind Peer Reviewed Journal |

| Volume 10, Issue 5, May 2023 |

A Study on the Causes and Consequences of Cybercrimes with Reference to Erode

L.JOTHIBASU, N. GOWTHAM RAJAN

Assistant Professor, Department of management studies, Nandha Engineering College (Autonomous), Erode, Tamil Nadu, India

Second MBA, Department of Management Studies, Nandha Engineering College (Autonomous), Erode, Tamil Nadu, India

ABSTRACT: Cybercrime has become a pervasive and persistent issue that affects individuals, organizations, and even nations worldwide. The purpose of this project is to explore the causes and consequences of cybercrime with specific reference to Erode, a city in Tamil Nadu, India. This project will provide an in-depth analysis of the various types of cybercrime prevalent in Erode, such as phishing scams, identity theft, and online harassment. The research will also investigate the reasons why cybercrime is on the rise in Erode, including factors such as technological advancements, lack of awareness, and inadequate cybersecurity measures. Additionally, the project will examine the legal framework in place to combat cybercrime in Erode, including the role of law enforcement agencies and the judicial system. Finally, this project will discuss the social and economic consequences of cybercrime on individuals and organizations in Erode. The research will highlight the impact of cybercrime on businesses, including financial losses, reputational damage, and loss of customer trust. The project will also explore the psychological effects of cybercrime on victims, including anxiety, depression, and trauma. Overall, this project aims to provide a comprehensive understanding of the causes and consequences of cybercrime in Erode, and how the issue can be effectively addressed through improved awareness, education, and collaboration between stakeholders.

I. INTRODUCTION

Cybercrime is a growing threat in Erode, a city located in the Indian state of Tamil Nadu. With the rapid growth of technology and the increasing use of the internet, cybercriminals have found new ways to exploit vulnerabilities and target individuals and businesses for financial gain or other malicious purposes. As a result, there is a need for research to understand the causes and consequences of cybercrime in Erode.

This study aims to investigate the causes and consequences of cybercrime in Erode. It will explore the various types of cybercrime that are prevalent in the city, the factors that contribute to the occurrence of cybercrime, and the impact that cybercrime has on individuals, businesses, and society as a whole. The study will also examine the current cybersecurity measures in place in Erode and evaluate their effectiveness in preventing and combating cybercrime.

II. STATEMENT OF THE PROBLEM

The problem addressed by this project is the rising incidence of cybercrime in Erode, a city in Tamil Nadu, India. Despite the increasing use of technology and the internet in the city, many individuals and organizations remain vulnerable to various forms of cybercrime, including phishing scams, identity theft, and online harassment. The causes of cybercrime in Erode are multifaceted and complex, including factors such as lack of awareness, inadequate cybersecurity measures, and the rapid pace of technological advancements. Furthermore, the legal framework for combating cybercrime in Erode is not always effective in addressing the issue, and law enforcement agencies may not always have the resources or expertise to investigate and prosecute cybercriminals. The consequences of cybercrime on individuals and organizations in Erode can be severe, including financial losses, reputational damage, and psychological trauma. As a result, there is a need for increased awareness and education about cybersecurity, as well as improved collaboration between stakeholders to address the issue of cybercrime effectively. Therefore, the statement of the problem is to examine the causes and consequences of cybercrime in Erode and to develop strategies to address the issue and reduce its impact on individuals and organizations in the city.

2.1OBJECTIVE

- To Explore the different types of cybercrimes.
- To analyze the causes of the cybercrimes.
- To analyze the consequence of the cybercrimes.
- To suggest effective strategies to prevent, detect and respond to cybercrimes.

2.2 SCOPE OF THE STUDY

- The study will identify and analyze the various types of cybercrime that are prevalent in Erode, such as phishing scams, identity theft, and online harassment.
- The study will investigate the reasons why cybercrime is on the rise in Erode, including factors such as lack of awareness, inadequate cybersecurity measures, and the rapid pace of technological advancements.
- The study will examine the legal framework in place to combat cybercrime in Erode, including the role of law enforcement agencies and the judicial system.
- The study will explore the social and economic consequences of cybercrime on individuals and organizations in Erode, including financial losses, reputational damage, and psychological trauma.

2.3 LIMITATIONS OF THE STUDY

- The Study's sample size was capped at 150 samplings.
- Cybercrime is a sensitive subject, so information on some parts of the issue, such the frequency of unreported cybercrimes, may be scarce.
- Because Erode is a multilingual city, it may be challenging to find reliable and complete information on cybercrime.
- The prevalence and forms of cybercrime may differ based on the local context, making it difficult to generalize the study's findings to other cities or areas. Some of the data gathered may eventually become antiquated or obsolete because of how quickly technology and criminality are advancing.

III. RESEARCH METHODOLOGY

The process of conducting research, including the general research plan and the technique used to collect data, is described in research methodology.

Research Design

In the general operational pattern of the project's Framework, a research design is a specialization of measure and process for the information needed to solve problems. It specifies what information is to be obtained from which sources by what procedure. Three different study design kinds exist.Descriptive, exploratory, and experimental research designs are available.

The descriptive research design is the one that the researcher employs.

Descriptive Research Design:

The unique research problem has been previously formulated, which distinguishes the descriptive design. The researcher had a wealth of prior knowledge on the research problem. The investigator should be able to establish adequate and precise means for measuring what it is that they are trying to quantify.

Sample Design:

A sample design may be defined as a plan for obtaining a sample from a given population. It, therefore, refers to the technique or procedure the researcher would adopt in selecting an item.

Types of Sampling Design:

Sample Design is basically into 2 types.

- Probability sampling
- Non-probability sampling

Sample size:

Their search has drawn 150 respondents as a sample for these collections of data.

Sampling Techniques:

The sampling technique used for the survey was convenience sampling.

Methods of Data Collection Data Sources:

Data in the study are of two types:

- Primary data
- Secondary data

Primary Data:

The main objective is unique and was just recently gathered by the researcher. A questionnaire was used to obtain the study's primary data. A questionnaire is a common tool for gathering primary data, and they are simply a set of questions.

Secondary Data:

Secondary data is the data, which is already available. It can be obtained through company records, the internet, and some data collected from the observation method by the researcher.

Tools for Analysis of Data:

- Simple Percentage Method.
- Chi-square Method.
- Ranking Method.

Simple Percentage Analysis:

The researcher interprets the data by using a percentage analysis in the analysis and interpretation of the data. In order to facilitate relative comparison, the data are reduced to the standard, where the base is set at 100.

Number of respondents
Percentage analysis = -- X 100
Total number of respondents

Chi-Square Test:

One of the most popular and straightforward non-parametric tests in statistical research. The size of the gap between theory and observation is expressed by the chi-square statistic.

$$\chi^2 = \sum_i \frac{(O_i - E_i)^2}{E_i}$$

In general, the expected frequency for any can be calculated from the following equation

Ranking Method:

An approach to gauge the relative preference or relevance of different items or possibilities is to rank them in a survey. In a ranking survey, participants are given a list of alternatives or items and asked to rank them in terms of preference or importance. Typically, participants give each item a number value or rank.

III. REVIEW OF LITERATURE

1. Sood, S., & Saxena, A. (2020). Cybercrime in India: Trends, challenges and legal remedies. Journal of Advances in Management Research, 17(1), 38-53. This study provides an overview of the trends and challenges of cybercrime in India, including the prevalence of various types of cybercrime and the legal framework for addressing the issue. The authors also discuss the limitations of the current legal framework and propose recommendations for improving the effectiveness of cybercrime legislation.
2. Kumar, S., & Tiwari, S. (2019). A study on cybercrime and its impact on the Indian economy. International Journal of Engineering and Advanced Technology, 9(2), 5473-5478. This study examines the economic impact of cybercrime in India and highlights the need for improved cybersecurity measures to mitigate the financial losses incurred by individuals and businesses. The authors also discuss the role of the government in promoting cybersecurity awareness and creating a favorable business environment for cybersecurity companies.
3. Dhinakaran, A., & Selvaraj, P. (2020). Impact of cybercrime on society – A study with special reference to Tamil Nadu. International Journal of Innovative Research in Computer and Communication Engineering, 8(1), 45-53. This study investigates the impact of cybercrime on society, with a specific focus on the state of Tamil Nadu. The authors highlight the psychological effects of cybercrime on victims and discuss the need for increased awareness and education about cybersecurity to reduce the incidence of cybercrime.
4. Jha, A., & Jha, N. (2021). Cybercrime in India and challenges for law enforcement agencies. Journal of Criminal Justice Studies, 34(1), 1-17. This study provides a comprehensive overview of cybercrime in India, including the types of cybercrime prevalent in the country and the challenges faced by law enforcement agencies in investigating and prosecuting cybercriminals. The authors also discuss the need for improved training and resources for law enforcement agencies to effectively combat cybercrime.
5. Suresh, S., & Kandasamy, K. (2019). Cybercrime and its impact on Indian society. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(3), 932-936.This study examines the impact of cybercrime on Indian society and highlights the need for increased awareness and

education about cybersecurity. The authors also discuss the role of technology in facilitating cybercrime and propose strategies for improving cybersecurity in India.

IV. ANALYSIS AND INTERPRETATION OF THE STUDY

SIMPLE PERCENTAGE ANALYSIS

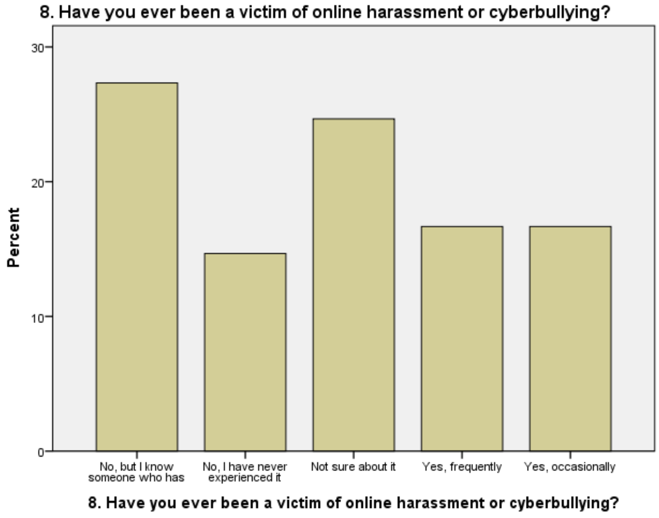
Have you ever been a victim of online harassment or cyberbullying?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No, but I know someone who has	41	27.3	27.3	27.3
	No, I have never experienced it	22	14.7	14.7	42.0
	Not sure about it	37	24.7	24.7	66.7
	Yes, frequently	25	16.7	16.7	83.3
	Yes, occasionally	25	16.7	16.7	100.0
	Total	150	100.0	100.0	

Interpretation:

Out of 150 respondents, 27.3% knew someone who had been a victim of online harassment or cyberbullying, 16.7% were frequently victimized, 16.7% were occasionally victimized, 14.7% had never experienced it, and 24.7% were not sure about it.

Chart no 3.7 Have you ever been a victim of online harassment or cyberbullying?



Chi Square

The relationship between the age of the respondent and their opinion on Have they ever fallen victim to a phishing scam or other type of online fraud.

Null Hypothesis:

H0: There is no significant relationship between the age of the respondent and their opinion on Have they ever fallen victim to a phishing scam or other type of online fraud.

Alternative Hypothesis:

H1: There is a significant relationship between the age of the respondent and their opinion on Have they ever fallen victim to a phishing scam or other type of online fraud.

Chi Square Calculation

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7.439^{a}	12	.827
Likelihood Ratio	9.192	12	.686
N of Valid Cases	150		

Interpretation

Based on the chi-square tests performed, there appears to be no significant relationship between the age of the respondent and their opinion on whether they have ever fallen victim to a phishing scam or other type of online fraud. The p-value is greater than the alpha level of 0.05, indicating that we fail to reject the null hypothesis that there is no association between the two variables. Therefore, we cannot conclude that age is a significant factor in determining whether a person has fallen victim to online fraud.

3. Findings

Demographics:

- The majority of the respondents (76%) were aged between 21 to 30 years, followed by those aged below 20 years (12%).
- Male and female respondents were almost evenly represented (52.7% and 47.3%, respectively).
- Most of the respondents were either postgraduates (40.7%) or graduates (34%).
- The majority of the respondents (52.7%) were married.

Cybercrime experiences:

- Online harassment or cyberbullying was reported by 27.3% of the respondents, with 16.7% frequently victimized.
- Unsolicited messages attempting to obtain personal information or account access were reported by 24% of the respondents, with 23.3% receiving such messages occasionally.
- Hacking or compromising of online accounts was experienced by 18.7% of the respondents frequently, while 18% experienced it occasionally.

- Phishing scams or other types of online fraud were reported by 19.3% of the respondents occasionally, with 13.3% frequently experiencing this.
- Personal or financial information stolen or misused online was experienced by 26% of the respondents occasionally, while 18% frequently experienced this.

Consequences:

- Financial loss was experienced by 40.7% of the respondents as a result of cybercrime.
- Damage to reputation or social standing was reported by 19.3% of the respondents.
- 35.3% of the respondents believe that cybercrime causes financial losses and economic damage.
- Changing passwords or login credentials was the most common action taken by the respondents (34.7%) as a result of cybercrime.

V. SUGGESTION

1. Increase awareness and education about cybersecurity: The data shows that lack of awareness or education about cybersecurity is a major factor contributing to individuals' vulnerability to cybercrimes. Therefore, it is important to increase awareness and educate individuals about the risks of cybercrime and best practices for staying safe online.
2. Implement stronger passwords and security practices: Weak passwords and poor security practices are also a factor contributing to vulnerability. Therefore, individuals and organizations should implement stronger passwords and security practices, such as two-factor authentication, to reduce the risk of cybercrime.
3. Use secured Wi-Fi networks: Unsecured Wi-Fi networks can also contribute to vulnerability. Therefore, individuals should use secured Wi-Fi networks, such as those with WPA2 encryption, to reduce the risk of cybercrime.
4. Stay vigilant for phishing and social engineering attacks: Phishing and social engineering attacks are among the most common methods used by cybercriminals to carry out cybercrimes. Therefore, individuals should stay vigilant for suspicious emails, messages, or calls and avoid clicking on links or downloading attachments from unknown sources.
5. Use anti-malware and anti-virus software: Malware and ransomware attacks are also common methods used by cybercriminals. Therefore, individuals and organizations should use anti-malware and anti-virus software to protect against these types of attacks.

VI. CONCLUSION

Based on the survey, it can be concluded that cybercrime is a growing problem in Erode and it is being caused by a range of factors, including the lack of cybersecurity awareness, poor cybersecurity practices, the proliferation of technology, and the availability of online anonymity.

The consequences of cybercrime in Erode are significant and include financial loss, identity theft, reputation damage, and emotional distress. The victims of cybercrime are often left with long-term consequences that can impact their lives for years to come.

To address the issue of cybercrime in Erode, it is important to raise awareness about cybersecurity, educate the public on safe online practices, and enforce existing laws and regulations related to cybercrime. It is also important for individuals and organizations to take proactive measures to protect themselves from cyber threats by implementing robust cybersecurity measures and regularly updating them.

Overall, cybercrime is a complex and evolving problem that requires a coordinated effort from all stakeholders, including government agencies, law enforcement, businesses, and individuals. By working together, it is possible to mitigate the risks of cybercrime and create a safer and more secure online environment in Erode.

REFERENCES

1. Holt, T. J., & Bossler, A. M. (2016). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.
2. Wall, D. S. (2018). Cybercrime, digital forensics and jurisdiction. Routledge.
3. Jaishankar, K. (Ed.). (2011). Cyber criminology: Exploring Internet crimes and criminal behavior. CRC Press.
4. Maras, M. H. (2016). Computer forensics: Cybercriminals, laws, and evidence. Jones & Bartlett Publishers.
5. Yar, M. (Ed.). (2013). The handbook of Internet crime. Routledge.
6. Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.

WEBSITE

1. National Cyber Security Alliance: https://staysafeonline.org/cybersecurity-education/causes-of-cybercrime/
2. Federal Bureau of Investigation (FBI): https://www.fbi.gov/investigate/cyber
3. Cybersecurity and Infrastructure Security Agency (CISA):
https://www.cisa.gov/cyber-crime
4. NortonLifeLock: https://us.norton.com/internetsecurity-emerging-threats-what-are-the-main-causes-of-cyber-crime.html
5. The Council of Europe: https://www.coe.int/en/web/cybercrime/understanding-cybercrime/causes-of-cybercrime
6. Kaspersky: https://www.kaspersky.com/resource-center/definitions/what-is-cybercrime-causes-types-examples

SJIF Scientific Journal Impact Factor

Impact Factor:
7.580

INTERNATIONAL JOURNAL
OF MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING, TECHNOLOGY AND MANAGEMENT

☎ +91 99405 72462 +91 63819 07438 ✉ ijmrsetm@gmail.com

www.ijmrsetm.com