International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

A Study an Emerging Tends and Impact of Cyber Scam

ASWATHY B[1], SARATH VINOD NAIR[2]

[1]Assistant Professor, Department of Forensic Science, S.E.A College of Science, Commerce, and Arts (Autonomous)

[2]Student, Department of Forensic Science, Jain University

Abstract

In the rapidly advancing digital era, the growing dependence on internet-based technologies has significantly increased the risk and impact of cyber scams. This study investigates the emerging trends in cyber scams and examines their social, economic, and psychological effects on individuals. The research focuses on the level of public awareness, vulnerability factors, and preventive practices associated with cyber fraud. A descriptive research design was adopted, and primary data were collected through a structured questionnaire administered to 90 respondents from the Krishnarajapuram locality using simple random sampling. The study analyzed factors such as age and education as independent variables, and vulnerability, socio-economic impact, and awareness as dependent variables. Data were processed using Microsoft Excel, and the results were presented through charts and percentage analysis. Findings reveal that lack of awareness is the primary reason people fall victim to cyber scams, with fake online shopping websites and phishing attacks being the most common forms of fraud. The study highlights the urgent need for strengthened digital literacy, stricter cyber laws, and improved preventive strategies. The research contributes to understanding the growing threat of cyber scams and offers practical recommendations to enhance public awareness and cyber security practices.

Keywords: Cybercrime, Cyber Scams, Digital Fraud, Phishing

1.Introduction

In the contemporary digital age, often described as the *Tech Era*, technology has evolved into an essential component of human life, influencing almost every aspect of daily existence. From communication, education, healthcare, and banking to entertainment and social interaction, individuals increasingly depend on digital tools and online platforms to fulfill both personal and professional needs. While this technological advancement has brought immense convenience and opportunities for growth, it has simultaneously given rise to new forms of threats and vulnerabilities. Among the most alarming of these is **cybercrime**, a modern dimension of criminal activity that exploits digital technologies as its primary weapon.

Unlike traditional offenders who rely on physical force, weapons, or disguises, cybercriminals remain hidden in the virtual world, often masking their true identities behind layers of anonymity. They manipulate human psychology through fake promises, fraudulent schemes, and convincing digital interactions, making it easier to deceive unsuspecting victims. Cybercrimes may take several forms, including financial fraud, identity theft, hacking into personal or organizational systems, phishing scams, online harassment, and blackmail. In many cases, victims are targeted not only for monetary gain but also for revenge, personal vendetta, or the mere thrill of exploiting vulnerabilities.

The rise of such crimes has had severe consequences on individuals, institutions, and even nations, ranging from economic losses and emotional distress to breaches of privacy and threats to national security. With technology advancing at a rapid pace, cybercriminals continuously devise sophisticated techniques that make

detection and prevention increasingly challenging. Thiss growing menace underscores the urgent need for cyber awareness, digital literacy, and preventive strategies to safeguard individuals and societies.

2. RESEARCH METHODOLOGY

2.1. STATEMENT OF THE PROBLEM

This paper aims to provide a comprehensive exploration of the emerging trends in cybercrime**,** focusing on how rapidly evolving technologies have not only transformed the way individuals and organizations interact but also created new avenues for criminal activities. With the proliferation of the internet, smartphones, cloud services, and artificial intelligence, cybercrime has shifted from traditional forms of online fraud to more sophisticated, organized, and large-scale operations. The study will highlight the rise of advanced cyber threats such as ransomware attacks, phishing scams, identity theft, cryptocurrency-related fraud, deepfake technologies, and state-sponsored cyber fraud.

2.2. Objectives

a) To study the emerging trends and lack of awareness among society for cyber fraud.
b) To analyze the socio-economic and psychological impacts of cyber scam on victims.
c) To suggest effective preventive strategies to reduce the risk of cyber scam

2.3. Significance of the Study

Cybercrime is widely regarded as one of the most pressing challenges of the digital era, as it involves illegal acts conducted through cyberspace where offenders gain unauthorized access to personal data, financial information, and digital assets of individuals and organizations. Unlike traditional crimes, cybercrimes transcend geographical boundaries, allowing perpetrators to operate from anywhere in the world with just a device and internet connectivity. This borderless nature makes it difficult for law enforcement agencies to track and apprehend offenders, thereby intensifying the threat. The significance of this study lies in its potential to highlight the urgent need for awareness and preparedness among the general public**.** Many cybercrimes succeed because victims are unaware of fraudulent schemes such as phishing emails, fake websites, or malicious third-party applications that harvest personal information. By fostering digital literacy, individuals can be empowered to recognize, avoid, and report suspicious activities, thereby reducing their vulnerability to cyber threats. Furthermore, the study is significant as it seeks to bridge the gap between technological advancements and their ethical, legal, and social implications. By providing insights into prevention strategies, case studies, and real-world implications**,** it contributes to the growing body of knowledge that can guide both individuals and institutions in developing effective defense mechanisms against cybercrime.

2.4. Scope of the Study

This study focuses on exploring the nature and methods of cyber scams, with emphasis on how fraudsters use new techniques to trap the public. It highlights the importance of awareness and digital literacy as key tools to prevent such crimes. The scope includes identifying common scam activities such as phishing, identity theft, and fraud through third-party applications, while also examining the role of government policies and preventive measures. By addressing both public awareness and institutional responses, the study aims to provide a clear understanding of how society can counter the growing threat of cybercrime.

2.5. Universe of Study

The present study comprises of 100 samples collected from Krishnarajapuram locality

2.6. Sampling Technique

The sampling technique used here is Simple random sampling technique

2.7. Research design

The present study adopts a descriptive research design to examine the issues of cyber fraud, and its implications in contemporary society

2.8. Variable of study

The independent and dependent variables are given below

Independent Variables: Age and Educational Qualification

Dependent Variables : Vulnerability, Socio-economic impact, and Awareness

2.9. Method and Data collection

This data is collected through a structured questioner administered to 85 responded the responses were tabulated and analyzed using Microsoft excel, which facilitated calculation of percentages and preparation of charts for interpretation

- Section 1- The interview schedule consisted of socio-economic profile of the respondence.
- Section 2- Consisted of items related to awareness of cyber scams.
- Section 3- Consist of questions related to perception of the society relating to cyber scam.
- Section 4- Consist of public's opinion on the cyber scam.
- Section 5- Consist of questions relating to suggestions and preventive measures from the public.

2.10. DATA PROCESSING AND ANALYSIS

In order to analyze the data Microsoft, excel was used. To fulfil the research objectives, a structured methodology was adopted:

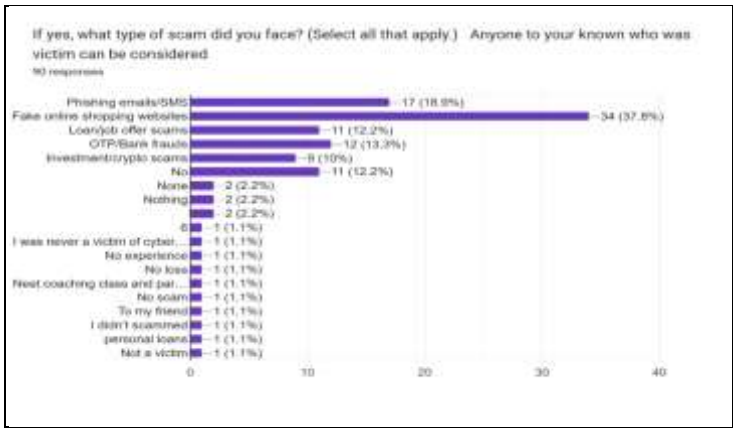
- **Google Forms** was used to collect primary data through a mix of quantitative (Likert scale, multiple choice) and qualitative (short answer) questions.
- The survey focused on three areas: awareness of cyber fraud, victim experiences, and preventive strategies.
- The form was distributed digitally across social groups, educational institutions, and professional networks.
- A total of **90** responses were received, covering diverse demographics (age, gender, education, occupation).
- Responses were exported to **Microsoft Excel (.xlsx)** for processing and analysis.

- Data cleaning included removing incomplete entries, standardizing categories, and coding qualitative inputs.
- **Objective A (Awareness):** Frequency and percentage analysis of fraud types and information sources; cross-tabulation by age and education.
- **Objective B (Impacts):** Descriptive statistics on financial loss; thematic analysis of emotional effects; correlation with income levels.
- **Objective C (Prevention):** Ranking of strategies; visualization of preferred awareness methods and law effectiveness.
- Charts and graphs were created in Excel to illustrate key findings
    - Awareness levels by demographic
    - Severity of psychological and financial impacts
    - Popularity and perceived success of preventive measures
- Insights were interpreted to align with the study's goals and inform recommendations.

3.RESULTS AND DISCUSSIONS

3.1.VISUAL AND DATA OBSERVATIONS

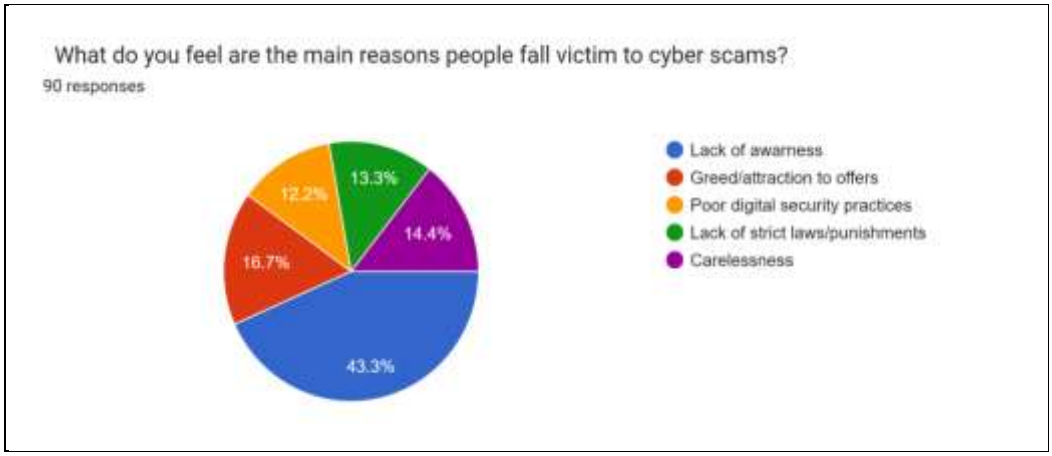
- The bar for **fake online shopping websites** is noticeably taller than all others, making it the dominant category by a wide margin.
- The middle tier of the chart (phishing, OTP/bank frauds, loan/job offer scams) shows **moderate prevalence**, together accounting for a substantial share of reported incidents.
- The lower end of the chart contains many **single-response free-text items** (e.g., "No experience", "personal loans", "To my friend"), which suggests respondents used the open field to add varied or ambiguous answers.



Graph 1. Graphical representation of response on cyber scam

The chart displays five factors with their corresponding percentages:

- **Lack of awareness** – *43.3%* (largest portion, almost half the chart)
- **Greed / attraction to offers** – *16.7%*
- **Carelessness** – *14.4%*
- **Lack of strict laws/punishments** – *13.3%*
- **Poor digital security practices** – *12.2%*

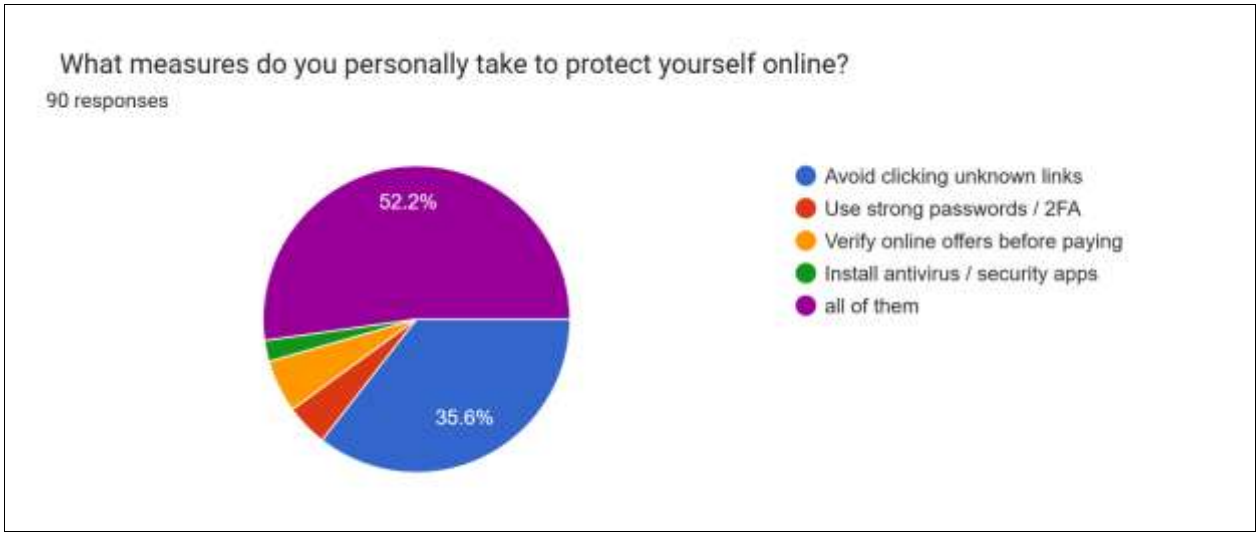


Graph 2, Graphical representation of Perception of society

The Graph 2 displays five factors with their corresponding percentages:

- **Lack of awareness** – *43.3%* (largest portion, almost half the chart)
- **Greed / attraction to offers** – *16.7%*
- **Carelessness** – *14.4%*
- **Lack of strict laws/punishments** – *13.3%*
- **Poor digital security practices** – *12.2%*

The chart shows that **lack of awareness** is by far the biggest reason people fall for cyber scams, making it the most significant concern. The remaining factors—greed, carelessness, weak laws, and poor digital habits—are smaller but still meaningful contributors.



Graph 3, Graphical representation of Measures of protection on cyber scams

The pie chart (Graph 3)includes five options:

- **All of them** – *52.2%* (largest portion)
- **Avoid clicking unknown links** – *35.6%*
- **Use strong passwords / 2FA** – small portion
- **Verify online offers before paying** – small portion
- **Install antivirus / security apps** – very small portion

Most respondents (**over half**) take **all recommended safety measures**, showing strong overall cybersecurity awareness. A significant number (35.6%) focus mainly on **avoiding unknown links**, which indicates this is seen as a major protective step. However, fewer people rely specifically on strong passwords, verifying offers, or installing security apps, suggesting these habits may need more emphasis in awareness programs.

4. SUMARY AND CONCLUSIONS

4.1. Major Findings of the study

This study examined the emerging trends and impacts of cyber scams in the digital era, with special focus on public awareness, vulnerability, and preventive practices. The research was conducted using a descriptive research design, and primary data were collected from respondents in the Krishnarajapuram locality through a structured questionnaire. The findings revealed that cyber scams such as fake online shopping websites, phishing, and OTP/banking frauds are increasingly common. The study also identified that lack of awareness is the major factor contributing to victimization, followed by carelessness, attraction to unrealistic offers, and weak digital security practices. The research highlighted the socio-economic and psychological impacts of cyber fraud, including financial loss, stress, fear, and loss of trust in digital platforms. Overall, the study emphasized the growing need for digital literacy and stronger preventive mechanisms to protect individuals from cyber threats.

4.2. CONCLUSION

Cyber scams have become a serious threat in today's technology-driven society, affecting individuals across different age groups and educational backgrounds. This study concludes that the rapid growth of digital

platforms, combined with insufficient public awareness and weak cyber security practices, has made people highly vulnerable to cyber fraud. The findings clearly show that most cyber scam incidents can be prevented through proper education, safe online behavior, and stronger enforcement of cyber laws. Awareness programs, strict legal frameworks, and improved digital security measures such as two-factor authentication and secure browsing practices are essential to reduce cybercrime. The study also concludes that collaboration between government agencies, educational institutions, technology companies, and the public is necessary to combat the increasing menace of cyber scams. Strengthening digital literacy and promoting responsible online behavior will play a crucial role in ensuring a safer cyberspace.

REFERENCES

1. Anderson, R. (2001). *Security engineering: A guide to building dependable distributed systems*. Wiley.
2. Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. Praeger.
3. Grabosky, P. (2007). The nature of cybercrime. *Crime and Justice, 10*(2), 243–257. https://doi.org/10.1080/10439460701369724
4. Holt, T. J. (2012). *Cybercrime and digital forensics: An introduction*. Routledge.
5. Jewkes, Y., & Yar, M. (2010). *Handbook of internet crime*. Willan Publishing.
6. Kshetri, N. (2013). *Cybercrime and cybersecurity in the global south*. Palgrave Macmillan.
7. Levi, M. (2017). Assessing the trends, scale, and nature of economic cybercrimes. *Crime, Law and Social Change, 67*(1), 3–20. https://doi.org/10.1007/s10611-016-9647-4
8. McGuire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. Home Office Research Report.
9. National Crime Records Bureau. (2022). *Crime in India: Cybercrime statistics*. Government of India.
10. Robo, M. (2019). Cyber crime and cyber security challenges. *International Journal of Computer Science and Network Security, 19*(6), 45–50.
11. Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts. *International Journal of Engineering Research and Applications, 2*(2), 202–209.
12. Tavani, H. T. (2016). *Ethics and technology: Controversies, questions, and strategies for ethical computing* (5th ed.). Wiley.
13. Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age*. Polity Press.