Public perception and responsibility in cyber security: A study on assessing awareness and effective prevention of cyber frauds in Lucknow region

Anubha Saxena[1], Research Scholar, Department of Commerce, University of Lucknow
rs2023comm_anubha@lkouniv.ac.in
Geetika T Kapoor [2], Professor, Department of Commerce, University of Lucknow
Geetika.t.kapoor@gmail.com

Abstract

Cybercrimes are on the rise and pose serious hazards to individuals, corporations, and governments as digital technologies become a part of our lives. This study looks at people's knowledge, awareness, perceptions, attitudes, and countermeasures regarding cyber frauds today. This study aims at determining the general awareness of cybercrimes, their perceptions across different demographic groups, and investigate the efficacy of current reporting procedures and preventive measures through a structured online questionnaire. The result of the study shows that though there is a growing awareness of cyber fraud and regulatory frameworks, there are still significant gaps in knowledge and the application of practical preventive measures. The report also emphasizes the underuse of resources that are accessible and may otherwise improve cybersecurity, such as local cyber cells and cyber insurance. The study also assesses the existing systems prevailing in India related to the cybercrimes, highlighting the areas that requires better public awareness campaigns and law enforcement intervention. Strengthening them will help in enhancing resource accessibility, and supporting educational programs are among the recommendations. By providing useful information and suggestions for people, organizations, policy makers, this paper seeks to promote a more knowledgeable and proactive approach to preventing cyber fraud.

KEYWORDS- Cyber awareness, cyber security, perception, cybercrime, cyber fraud, preventive measures

Introduction

In today's fast paced world, we all are surrounded by technology. Our day to day activities are now dependent on it & we spend a considerable amount of time online. Rising dependence on technology and extensive use of internet has caused the increase in the number of cyber frauds in the country. Thus, it is quite inevitable to protect our data and ourselves from the cyber frauds.

For effective protection and prevention from the cyber frauds, people should be well aware about it and their perceptions determine the degree of how much protected they are. Hence, it is important to check the level of

awareness, varied perceptions regarding the cyber frauds and measures adopted by people to protect themselves from it. In this paper, we will be assessing the level of awareness, perception of people as well as suggesting the preventive measures.

CERT-In which stands for Computer Emergency Response Team - India, is responsible for managing the cyber security incidents, offering threat intelligence as well as giving guidance on safety protocols. The IT Act 2000 of India gives legal acknowledgment for e-transactions and digital signatures, concerned with cyber security & also specifies the consequences for cybercrimes. RBI has set up rules to enhance cyber security and fight against cybercrimes in the financial industry. The helpline number for reporting cyber fraud in India is 1930. It can also be reported through the National Cybercrime Reporting Portal.

Research Gap of the study:

Most of the studies on the cyber frauds have been taken place either in southern area of India or in other countries. So, this study fills the gap by conducting an empirical study on the general public of Lucknow region, which is the capital of Uttar Pradesh. Moreover, a very limited broad-based studies on overall cyber fraud awareness across diverse populations have been conducted. There is also a gap in understanding the practical engagement with and impact of cyber insurance and local cyber cells. Thus, a study which measures the level of awareness, perception of the people on cyber fraud and suggesting the preventive measures is required.

Objectives of the study:

The objectives of the study are-

1. To assess the level of awareness of people regarding the various types of cyber frauds.
2. To examine the perceptions of people towards their responsibility in educating themselves about cyber security measures.
3. To suggest the preventive measures of cyber frauds to the general public in order to mitigate these cyber frauds.

Hypothesis of the study:

The hypothesis for the study are as follows-

1. H0: There is no significant association between demographic factors and awareness level of cyber frauds.

H1: There is a significant association between demographic factors and awareness level of cyber frauds.

Literature Review

A study by Kumbhar M & Gavekar V (2017) on cybercrime awareness in Pune city revealed that most respondents felt neutral about online banking safety, indicating low awareness. Hacking was identified as the most common form of cybercrime. Rural areas showed a significant lack of cybercrime awareness, highlighting the need for targeted education. Additionally, students were found to be the most frequent victims of cybercrimes

Aldawood H & Skinner G (2019) addresses the overcoming challenges in training against social engineering within integrated information systems. It highlights the increased vulnerability from staff social media use and evolving attack techniques. The study suggests cost-effective strategies and preparedness exercises to enhance security training and improve organizational defenses against social engineering

Alzubaidi A (2021) conducted a study in Saudi Arabia which emphasised on improving the cyber security awareness among the general public which is required to combat rising cyberattacks. This study assessed the cyber security knowledge of people & highlighted the effectiveness of the Technology Acceptance Model (TAM). It underscores the need for targeted educational programs in both private sector and public sector to prevent cybercrime.

Kimpe, L., et al. (2021) conducted a study which discovers that although protective behaviour is enhanced by a greater sense of self-efficacy and understanding of the seriousness of cybercrime, users who feel well-informed may actually lose motivation to take more security precautions because they incorrectly think they are less exposed.

Zwilling M, et al. (2022) carried out a study which explores cyber security awareness and skills across countries with varying GDP levels, revealing the need for tailored training programs. It highlights that user traits impact cyber security behaviours and suggests both technological and educational investments in high-GDP countries.

Nair RR (2023) stated that the students are well aware about cybercrimes and have the ability to identify the latest online scams. Knowledge and perception of respondents were assessed using a structured questionnaire. At the end, the preventive measures were suggested by the author to mitigate the cybercrime threats.

Fatoki JO (2023) conducted a study on Nigerian banking industry & revealed various tactics employed by cybercriminals to deceive individuals and unlawfully acquire their funds. The study demonstrated that employing cloud-based security solutions is particularly effective in preventing fraud in Nigerian banks.

Singh K, et al. (2023) assesses customer awareness of cyber security and fraud prevention in nationalized banks, finding that while customers understand online banking products and cyber threats, they lack knowledge about cyber security laws. The study highlights the need for improved consumer education on security and privacy in online banking.

Walvekar S (2023) conducted a study which finds a link between students' class, department, and course of study and their level of knowledge about online banking fraud. Additionally, the information booklet was successful in enhancing undergraduate students' awareness of online banking frauds.

Pillai AS, et al. (2024) conducted a study to understand the impact of cybercrimes on BFSI sector. It emphasizes that cyber security policies, educational initiatives, and protection strategies must account for demographic diversity. Effective cyber security education requires targeted campaigns that focus on specific cyber threats and their prevention, rather than a onesize-fits-all approach.

Research Methodology

- In this study, descriptive research design has been applied, where the individual collects data, analyses, prepares and then presents it in a precise manner. It involves

  the analysis of awareness level, perception regarding cyber frauds and preventive measures of it.
- In this study, a non-probability sampling method has been employed, specifically the convenience sampling technique.
- As this is an academic research, it is restricted to very small sample size and due to time constraints the research is carried out in Lucknow city with 160 respondents from different parts of the city.
- The Primary data has been collected through Google form questionnaire which was circulated using social media. These responses have been analysed with the help of tables and pie charts for better understanding. The other secondary data has been collected from authenticated websites.

Data Collection & Analysis:

The Primary data has been collected using an online questionnaire, Google Form. The data has been analysed using MS Excel.

Table 1: Analysis of Socio-demographic factors

		Gender	Age group	Occupation

	Valid	160	160	160
N	Missing	0	0	0

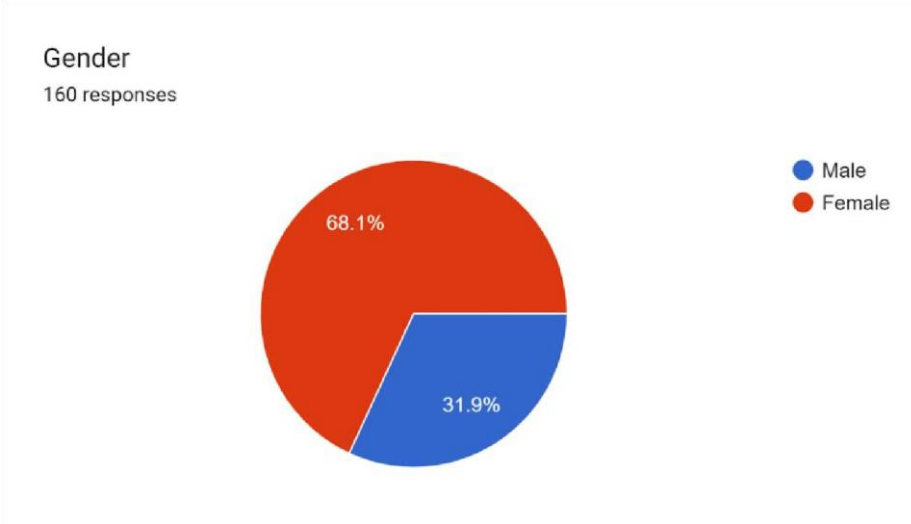
(Source: Compiled from Primary data)

Table 2: Percentage Analysis of Socio-Demographic factor- Gender Classification

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	109	68.1	68.1	68.1
	Male	51	31.9	31.9	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: Table 2 shows the demographic factors of gender classification which exhibits 68.1% of the respondents are males & 31.9% are females.



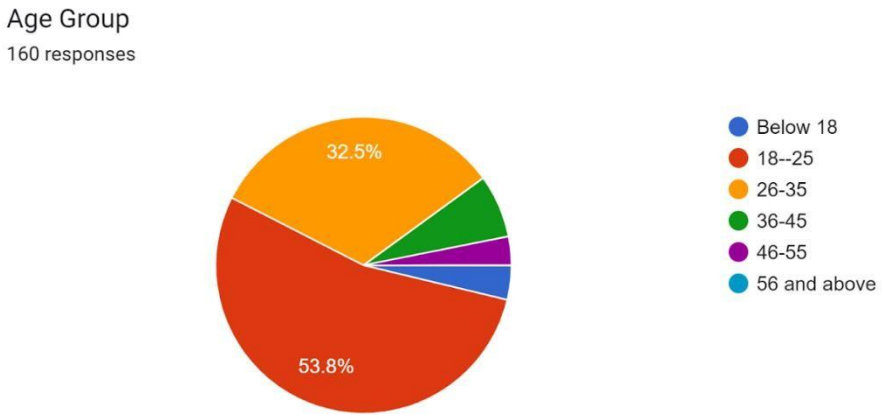
(Source: Compiled from the Primary data)

Table 3: Percentage Analysis of Socio-Demographic factor-Age Group Classification

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18--25	86	53.8	53.8	53.8
	26-35	52	32.5	32.5	86.3
	36-45	11	6.9	6.9	93.1
	46-55	5	3.1	3.1	96.3
	Below 18	6	3.8	3.8	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: Table 3 shows that 53.8% of the respondents belong to the age group of 1825 and 32.5% of the respondents are from 26-35 range.



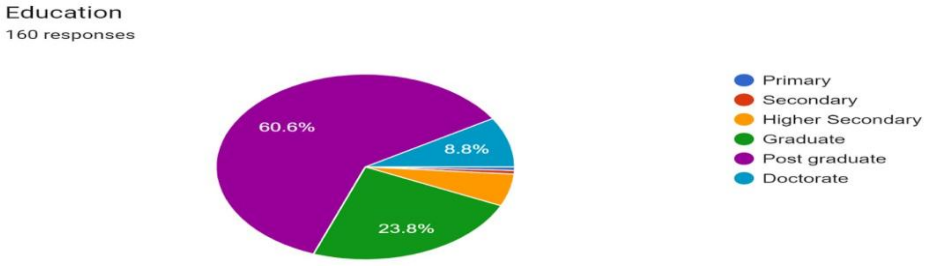
(Source: Compiled from the Primary data)

Table 4: Percentage Analysis of Education qualification

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Doctorate	14	8.8	8.8	8.8
	Graduate	38	23.8	23.8	32.5
	Higher Secondary	9	5.6	5.6	38.1
	Post graduate	97	60.6	60.6	98.8
	Primary	1	.6	.6	99.4
	Secondary	1	.6	.6	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: In Table 4, 60.6% of the respondents are post graduated & 23.8% are graduates.



(Source: Compiled from the Primary data)

Table 5: Percentage Analysis of Socio-Demographic factor- Occupation

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Business	8	5.0	5.0	5.0
	Employment	34	21.3	21.3	26.3
	Not Applicable	10	6.3	6.3	32.5
	Profession	20	12.5	12.5	45.0
	Self employed	8	5.0	5.0	50.0
	Student	80	50.0	50.0	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: As we can see in the Table 5, 50% of the respondents are Students, 21.3% of the respondents have selected employment i.e. they are an employee.

Table 6: Association between demographic factors and awareness about cyber frauds

Demographic factors	**Chi-Square test (Pearson Chi-Square)**	**Asymptotic Significance**
Gender	3.475	.176
Age	11.192	.191
Occupation	7.703	.658

(Source: Compiled from Primary data)

Interpretation: The chi-square test results reveal no significant association between cyber security awareness and demographic factors such as gender, age, and occupation. The pvalues for gender (0.176), age (0.191), and occupation (0.658) all have exceeded the typical significance level of 0.05, indicating that these factors do not significantly influence cyber security awareness. Hence the null hypothesis for the study i.e., there is no significant association between demographic factors and awareness level of cyber frauds, has been accepted.

Table 7: Familiarity with the word 'Cyber Crime/Fraud'

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Maybe (Not Sure)	3	1.9	1.9	1.9
	No	3	1.9	1.9	3.8
	Yes	154	96.3	96.3	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: Around 96.3% of the respondents are aware about cybercrime/cyber frauds and 1.9% are unsure about it, and 1.9% of the respondents are not aware about it.

Table 8: Vulnerability to cybercrimes

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Anyone	74	46.3	46.3	46.3
	Businesses	8	5.0	5.0	51.2
	Financial Institutions like banks etc.	8	5.0	5.0	56.3
	Government	2	1.3	1.3	57.5
	Old age people	30	18.8	18.8	76.3
	Teenagers	29	18.1	18.1	94.4
	Young working professionals	9	5.6	5.6	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: In table 8, we can see that 46.3% of the total respondents think that anyone can be prone to cybercrimes. Respondents also think that old age people & teenagers are also more vulnerable to it.

Table 9: Reporting a cybercrime

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Always	29	18.1	18.1	18.1
	Never experienced	31	19.4	19.4	37.5
	Not at all	8	5.0	5.0	42.5
	Often	8	5.0	5.0	47.5
	Rarely	35	21.9	21.9	69.4
	Sometimes	49	30.6	30.6	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: Around 30.6% people report a cybercrime sometimes, 21.9% reports rarely, 19.4% have never experienced it & 18.1% always report the cybercrimes. 5% never report any cyber frauds.

Table 10: Awareness about IT Act 2000

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	39	24.4	24.4	24.4
	Yes	121	75.6	75.6	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: In table 10, 75.6% of the respondents are aware about IT Act 2000 and 24.4% are not aware about it.

Table 11: Awareness of National Cybercrime helpline number i.e.1930

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	44	27.5	27.5	27.5
	Yes	116	72.5	72.5	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: In table 11, 72.5% of the total respondents are aware about National Cybercrime helpline no. & 27.5% are not aware about it.

Table 12: Source of info about Cybercrimes & security?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Cyber security awareness campaigns by banks	18	11.3	11.3	11.3
	Print Media (Newspaper, Magazines, etc.)	32	20.0	20.0	31.3
	Social Media	104	65.0	65.0	96.3
	TV/Radio	6	3.8	3.8	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: 65% of the respondents got to know about cybercrimes from social media. 20% got to know from print media and 11.3% got to know from cyber security awareness programmes.

Table 13: Awareness about cyber cell in their area

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	No	82	51.2	51.2	51.2
	Yes	78	48.8	48.8	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: In table 13, 48.8% of the respondents are aware about cyber cell in their area and majority that is 51.2% are not aware about it.

Table 14: Awareness about Cyber Insurance

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid					
	No	108	67.5	67.5	67.5
	Yes	52	32.5	32.5	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: In table 14, 32.5% of the respondents are aware about cyber insurance and 67.5% are not aware about it.

Table 15: Do you think you are protected from cyber crimes?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Not protected	42	26.3	26.3	26.3
	Somewhat protected	96	60.0	60.0	86.3
	Well protected	22	13.8	13.8	100.0
	Total	160	100.0	100.0	

(Source: Compiled from Primary data)

Interpretation: 60% of the respondents have chosen they are somewhat protected from cybercrimes, while 26.3% still think they are not protected.

Cybercrimes experienced by the respondents

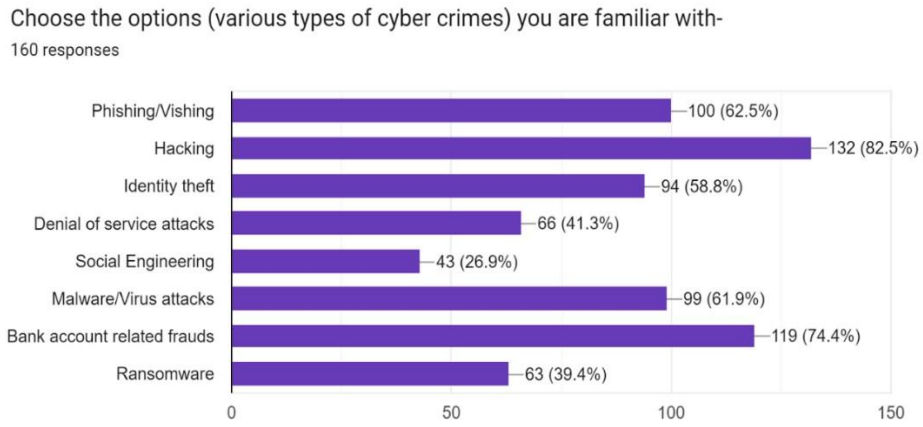
(Source: Compiled from the Primary data)

Interpretation: In given figure, around 82.5% have experienced fake calls, 71.3% have experienced spam messages/emails. Around 55.6% chose lottery/Ponzi schemes & 48.8% chose fake employment scams and 10% have never experienced any cyber frauds.

Table 16: Frequencies of the types of cybercrimes most familiar with

Type of Cyber Crime	Frequencies
Phishing/Vishing	100
Hacking	132
Identity theft	94
Denial of service attacks	66
Social Engineering	43
Malware/Virus Attacks	99
Bank a/c related frauds	119
Ransomware	63

(Source: Compiled from the Primary data)



(Source: Compiled from the Primary data)

Interpretation: In the above figure, we can see that 82.5% are aware about hacking, 62.5% aware of phishing/vishing, 74.4% aware with bank a/c frauds, 58.8% aware about identity theft and 61.9% aware about malware. We can also infer that people are least familiar with Social Engineering (26.9%), Ransomware (39.4%), DOS attacks (41.3).

Table 17: Frequencies of measures chosen which are adopted for cyber security

Measures adopted for cyber security	Frequencies	Percentage
Installing anti-virus software and firewall applications	87	54.4%
Regular monitoring of bank accounts	83	51.9%
Not using public Wi-Fi/ charger points	74	46.3%
Not sharing sensitive and personal information on social media sites	128	80%
Frequently updating the applications	52	32.5%
Using strong passwords and frequently changing it	98	61.3%
Using two factor authentication for the apps	77	48.1%
Not responding to spam messages or links	114	71.3%
Downloading only from trusted sources	85	53.1%
Not sharing the confidential information to strangers	117	73.1%

(Source: Compiled from the Primary data)

Interpretation: The most frequently adopted cyber security measure is not sharing sensitive information on social media (80%), followed by using strong passwords and changing them regularly (61.3%) and not sharing confidential information with strangers (73.1%). Other common practices include installing anti-virus software (54.4%) and not responding to spam (71.3%). The least adopted measure is frequently updating applications (32.5%).

Findings

- Most of the people are aware about cybercrime/fraud, IT Act & Cyber fraud National helpline number.
- The source of information about cyber security for respondents are social media followed by print media.
- There is no significant link between cyber security awareness and demographic factors like gender, age, and occupation.
- Majority of the people think anyone can be prone to cyber frauds while approx. 18% of them think old age and teenagers are more prone to it.
- Most of the respondents are aware about hacking, phishing etc but are not aware about Ransomware and Social Engineering.
- Most respondents experience the situation occasionally or infrequently. A smaller number report it consistently or not at all. To improve overall engagement or awareness, target those who encounter it less frequently.

- 60% of the respondents are somewhat protected from cybercrimes, while 26.3% still think they are not protected.
- Most of them have experienced fake calls, spam messages/emails, lottery/Ponzi schemes & 48.8% chose fake employment scams and 10% have never experienced any cyber frauds.
- Most of the people are unaware about cyber cells in their area and cyber insurance.
- The most effective cyber security practices include not sharing sensitive information on social media (80%) and using strong passwords (61.3%). However, less emphasis is placed on updating applications (32.5%) and using two-factor authentication (48.1%).

Conclusion

The study indicates that there is a high level of awareness of basic cyber threats and security as well as of the best practices, such as avoiding publishing sensitive information on social media and using secure passwords. However, there are significant gaps in understanding of modern threats such as Ransomware and Social Engineering. Moreover, while many respondents realize the necessity of specific cyber security practices, they place less weight on application updates and the use of two-factor authentication. There is also a general lack of information regarding local cyber cells and cyber insurance. To address these concerns, it is critical to improve advanced threat education through targeted campaigns, encourage comprehensive cyber security practices by incorporating updates and two-factor authentication into regular training, and raise awareness of local cyber resources and insurance options. Programs tailored to involve people who encounter cyber dangers less frequently, and the use of effective communication channels like social media and print media, can help to improve general cyber security knowledge and protection.

Suggestions

1. Every individual should keep himself/herself updated in regards with cyber security and measures.
2. The Cyber cells should actively strive to promote cyber security measures and redressed mechanism.
3. To improve overall cyber security, individuals should increase efforts to update applications regularly, use two-factor authentication, and adopt other best practices like avoiding public Wi-Fi and being cautious with spam messages.
4. The authorities should work towards promoting the cyber related information more extensively to curb cyber frauds.
5. The insurance companies should advertise more about cyber insurance and its benefits

References

- Kumbhar, M., & Gavekar, V. (2017). A study of Cyber Crime awareness for prevention and its impact. International Journal of Recent Trends in Engineering & Research (IJRTER), 3(10), 240-246.
- Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future internet, 11(3), 73.
- Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. Heliyon, 7(1).
- De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41(8), 1796-1808.
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97.
- Nair, R. R. (2023). AWARENESS, THREATS & PERCEPTION OF CYBER SECURITY. Rejani, Awareness, Threats and Perception of Cyber Security (July-Dec 2023). Humanities and Social Science Studies.
- FATOKI, J. O. (2023). The influence of cyber security on financial fraud in the Nigerian banking industry. International Journal of Science and Research Archive, 9(2), 503-515.
- Singh, K., Mistrean, L., Singh, Y., & Barak, D. (2023). Fraud prevention in digital payment systems and cybersecurity education for customers of nationalized financial institutions. In Development Through Research and Innovation (pp. 98-115).
- Samidha, S. W. (2023). Impact of Banking Fraud Awareness Booklet Among The Students of Satara.
- Pillai, A. S., Doreswamy, H., & Jai Raj Nair, R. (2024). Unveiling the Dark Side of Technology: Understanding the Impact of Cybercrime on the BFSI Sector. Journal of Informatics Education and Research, 4(2).