IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cyber Security Awareness and Preparedness in Digital Finance Users: Evidence from Karnataka

Ms. Bhramarambha T R[1], Dr. Manoj Kumara N V[2]
[1]Research Scholar, [2]Associate Professor & Research Guide
1,2Department of Management Sciences
[1,2]Maharaja Institute of Technology Mysore, Mandya, India
[1]ORCID: 0009-0003-7659-7819, [2]ORCID: 0000-0001-5066-1868

Abstract: This study examines the growing cyber security challenges associated with the rapid adoption of digital financial platforms. With increasing dependence on online banking, mobile payments, and digital transactions, users are becoming more vulnerable to cyber threats such as phishing, identity theft, online fraud, and unauthorized access. The main purpose of this study is to analyze the extent of cyber security vulnerabilities faced by digital finance users in Karnataka and to evaluate the role of cyber security awareness in reducing such risks. The objectives of the study are to identify the impact of cyber threats, particularly phishing and online fraud, on users in Karnataka and to analyze the impact of cyber security awareness among users of digital financial platforms. The study adopts a descriptive research design and uses convenience sampling to collect primary data from 401 respondents across Karnataka. Data analysis was conducted using JAMOVI software, employing statistical tools such as ANOVA and T-test to examine variations and relationships among variables. The findings of this research are expected to contribute to academic research, policy formulation, financial institutions, and digital platform providers by enhancing awareness and strengthening cyber security practices among users of digital financial services.

Index Terms - Cyber Security Awareness, Digital Finance, Cyber Threats, Phishing Attacks, Online Fraud, Digital Financial Platforms, User behavior, Karnataka.

I. INTRODUCTION

The rapid growth of digital finance has transformed the way individuals conduct financial transactions, making online banking, mobile wallets, and digital payment systems an essential part of daily life. India's digital payment ecosystem has witnessed tremendous growth, with over 18,000 crore digital payment transactions recorded during 2024–25, while UPI alone processed more than 228 billion transactions in 2025. In today's technology-driven environment, the convenience and speed of digital financial platforms have significantly increased their usage across urban and rural areas in Karnataka. However, this expansion has also led to a rise in cyber security vulnerabilities, exposing users to threats such as phishing, online fraud, identity theft, and unauthorized access to financial information. Karnataka alone reported cyber fraud losses of ₹861 crore until July 2025, highlighting the seriousness of digital financial crimes in the state.

In the present context, ensuring cyber security in digital finance has become a major concern for governments, financial institutions, and users alike. As cybercriminals continue to adopt advanced techniques, users with limited cyber security awareness are becoming more susceptible to financial losses and data breaches. This study focuses on understanding the impact of cyber threats on digital finance users in Karnataka and analysing the importance of cyber security awareness in minimizing such risks. The

research is highly relevant in today's context as digital transactions continue to increase rapidly in both personal and commercial activities.

II. Conceptual Background

The conceptual background of the study highlights the growing importance of cyber security awareness in the digital financial environment. Digital finance platforms have transformed the financial sector by making transactions and investments faster, easier, and more accessible. At the same time, the increased use of these platforms has created cyber security risks such as phishing attacks, identity theft, data breaches, malware, and fake investment applications. Cyber security awareness helps users identify these threats and adopt safe online practices like using strong passwords, enabling two-factor authentication, avoiding suspicious links, and regularly monitoring accounts. Greater awareness improves users' confidence and reduces the fear of online fraud while using digital financial services.

Cyber security awareness, cyber hygiene practices, and effective legal frameworks play an essential role in protecting investors from cyber risks. The study emphasizes that greater awareness and secure digital practices can positively influence investment behaviour by increasing trust, reducing perceived risk, and encouraging safe participation in digital financial activities. The Technology Acceptance Model further supports the understanding of how users adopt digital financial technologies based on perceived usefulness, ease of use, and security. In addition, cyber hygiene practices and legal frameworks such as the Information Technology Act, 2000, RBI guidelines, and the Digital Personal Data Protection Act, 2023 help protect users and ensure secure digital financial transactions.

III. Review of Literature

Anayo Chukwu Ikegwu et.al (2026)[5] studied cyber security in mHealth applications. The study found that Cyber Threat Intelligence improves threat detection and data security. Isabel Maldonado, et al (2026)[14] examined cyber security challenges in SMEs. The findings showed that SMEs need stronger security frameworks and awareness programs. Duo Wang and Yanxi Li (2026)[10] analysed cyber security legislation and debt default risk. The study found that strong cyber laws help reduce financial risks. Ramlan Amir Isa, et al (2026)[27] studied cyber security awareness in digital commerce. The findings showed that awareness improves secure online practices. Fathey Mohammed et.al (2026)[12] explored fraud vulnerability among older adults. The study found that low awareness increases digital investment fraud risks. Harting, Ralf-Christian et.al (2025)[13] examined cyber risk management performance. The study showed that awareness and technology improve cyber security systems. Siyabulela Sandi and Carolien L. van den Berg (2025)[30] analysed cyber security education and resilience. The findings revealed that continuous learning improves security behaviour. Serpil Sevimli Deniz and Mehmet Ataş (2025)[29] studied phishing risks during employee onboarding. The study found that proper training reduces phishing attacks significantly. Mohammed Afzal et.al (2025)[21] examined cyber awareness in rural digital finance. The findings showed that awareness reduces fraud and improves trust. Damodharan Kuttiyappan and Dr. Rajasekar (2023)[7] developed a deep learning cyber-attack detection model. The study achieved high accuracy in identifying banking cyber threats.

Kevin F. McCrohan, Kathryn Engel, and James W. Harvey (2010)[19] analysed awareness training and password behaviour. The study found that cyber training improved password security strength. Dave Brown, et.al (2026)[8] studied privacy concerns among older digital users. The findings showed that low digital literacy reduces trust in online systems. Bo Nørregaard Jørgensen and Zheng Grace Ma (2026)[6] reviewed cyber security threats in smart grids. The study found that cyber-attacks create major risks to energy systems. Kate-Riin Kont and Denis Horenženko (2026)[18] examined cyber risk management among tax officials. The findings revealed gaps in formal cyber security practices. Julija Saveljeva and Tatjana Volkova (2025)[17] studied digital trust and banking risks. The study found that trust reduces perceived third-party cyber risks. Jones Márcio Nambundo, et.al (2025)[15] analysed cyber threats in smart meter systems. The findings showed risks like data tampering and weak authentication. Rahime Belen-Saglam, et.al (2025)[26] explored cyber risks in MaaS systems. The study identified privacy issues and weak security standards. Doney Abraham, et.al (2023)[9] examined cyber-attacks on energy infrastructure. The study found increasing vulnerabilities in critical energy systems. Martin Eling, et.al (2021)[20] reviewed cyber risk management frameworks. The study emphasized the importance of cyber resilience strategies. Natile

Nonhlanhla Cele and Sheila Kwenda (2024)[24] studied cyber threats affecting digital banking adoption. The findings showed that security concerns reduce user trust. Ahmed M. Abdelmagid, et.al (2025)[4] analysed maritime cyber risks. The study found that outdated systems increase cyber vulnerabilities.

Ntokozo F. Miya and Nazeer Joseph (2025)[25] examined cyber resilience trends in finance. The study highlighted limited focus on recovery and resilience strategies. Samir Bhowmik and Annesha Saha (2025)[28] studied digital finance adoption among MSMEs. The findings revealed challenges in cyber risk management practices. Joseph Opuni-Frimpong (2026)[16] analysed cyber security disclosures and credit risk. The study found that better disclosures reduce financial risk exposure. Abu Barkat Ullah, et.al (2025)[1] reviewed cyber security in mining infrastructure. The study recommended stronger policies and threat detection systems. Adetunji Paul Adejumo and Chinonso Peter Ogburie (2025)[2] studied cyber security in digital finance systems. The findings showed that strong security measures reduce cyber risks. Adetunji Paul Adejumo and Chinonso Peter Ogburie (2025)[3] analysed cyber security technologies in financial transactions. The study found that AI-based systems improve transaction safety. Mosope Williams, et.al (2021)[23] studied machine learning in fraud prevention. The findings showed improved cyber risk detection accuracy. Moshood F. Yussuf, et.al (2020)[22] examined machine learning for cyber risk assessment. The study found that predictive models strengthen financial security. Eugenio Lilli (2020)[11] analysed Obama's cyber security policy and digital protection systems. The study concluded that government policies strengthened national cyber security efforts.

IV. PROBLEM OF STATEMENT

The use of digital financial platforms has increased among investors in Karnataka because it is easy and convenient. However, this has also increased cyber risks like phishing, hacking, and online fraud. Due to lack of awareness, investors may face financial loss and lose trust in digital platforms. It is important to understand how cyber threats affect investors and how awareness influences their trust and decisions. Also, the effectiveness of cyber security awareness programs is not clearly known. Therefore, this study focuses on understanding investor awareness, the impact of cyber threats, and ways to improve safety in digital financial activities.

V. OBJECTIVE OF THE STUDY

To identify the impact of cyber threats such as phishing and online fraud on users of digital financial platforms in Karnataka.
To analyze the influence of cyber security awareness on the safe usage behavior of digital financial platforms users.

VI. RESEARCH METHODOLOGY

6.1 Research Method

The study adopts a **descriptive research methodology** to understand and explain the level of cyber security awareness among users using digital financial platforms. This method focuses on describing the current situation without influencing or controlling variables. Primary data is collected through structured questionnaires and surveys, while secondary data is gathered from reliable sources such as websites, research articles, and financial reports.

6.2 Sampling Design

- **Sampling Method** -The study uses convenience sampling, a non-probability sampling method where respondents are selected based on availability and willingness. Users who are easily accessible and use digital financial platforms are chosen for the study. This method is simple, cost-effective, and suitable for collecting data within limited time and resources.
- **Sampling Size –** According statistics times website, As of 2026, Karnataka's estimated population is 6.91 crore, with around 86% of people using digital payments, resulting in a considerable population of 5,23,83,600. Using Cochran's sample size formula with a 95% confidence level, 0.5 proportion, and 5% margin of error, the calculated sample size is 385 respondents. To improve the validity of the study, the researcher considered 400 respondents for data collection.

6.3 Source of Data

Primary Data - This study relies on primary data collected from investors to examine cyber security awareness among users in digital finance.

- **Research Instrument**

Structured Questionnaire

Data were collected through a structured questionnaire designed based on the objectives of the study to gather quantitative data for statistical analysis.

- **5-Point Likert Scale**

A 5-point Likert scale ranging from 1 (Strongly Disagree) to 5 (Strongly Agree) was used to measure respondents' opinions, attitudes, and awareness levels, enabling easy comparison and analysis.

- **Reliability Statistics**

Table 1 Scale Reliability Statistics

Objectives	Cronbach's α
Objective	0.768
Objective	0.827
Overall	0.898

Source: Survey Data-SPSS output

The Cronbach's alpha values for Objective 1 (0.768) and Objective 2 (0.827) indicate good reliability of the scale items. The overall Cronbach's alpha value of 0.898 shows a high level of internal consistency, confirming that the questionnaire is reliable and suitable for the study.

Secondary Data

Secondary data was collected from existing sources such as websites, research papers, journals, articles, and reports related to digital finance and cyber security. It helped in understanding background information, current trends, and supporting the findings of the study.

6.4 Tools of the Study

Descriptive Analysis-Descriptive analysis is used to summarize and present the collected data using percentages, mean, and standard deviation. It helps in understanding cyber threats, cyber security awareness, users' trust, and investment behaviour in Karnataka. This analysis identifies general patterns and supports the study hypotheses.

ANOVA- ANOVA is used to compare mean differences among more than two groups. It is applied to test H_{01} by examining whether cyber threats significantly affect investment behaviour across demographic groups such as age, income, and education. This analysis helps in understanding how cyber threats influence investment decisions among different categories of users in Karnataka.

Post hoc test- Post hoc tests are conducted after ANOVA to identify specific group differences. In this study, they compare demographic groups such as age, income, and education regarding the impact of cyber threats on investment behaviour. This helps in understanding group-wise differences among users in Karnataka.

T-test- The t-test is used to compare the mean values between two groups to identify significant differences. In this study, it is applied to test H_{02} by comparing users with different levels of cyber security awareness on digital financial platform usage. This helps in understanding how cyber security awareness influences the use of digital financial services in Karnataka.

6.5 Hypotheses

H_{01}: There is no significant impact of cyber security threats, such as phishing and online fraud, on users of digital platforms in Karnataka.

H_{02}: Cyber security awareness does not significantly influence the safe usage behavior of digital financial platform users.

VII. Data Analysis and Interpretation

This section presents the analysis and interpretation of data collected through structured questionnaires. Statistical tools are used to examine cyber threats, cyber security awareness, users' trust, and investment behaviour in Karnataka. The findings support the objectives and hypotheses of the study.

H_{01}: There is no significant impact of cyber security threats, such as phishing and online fraud, on users of digital platforms in Karnataka.

Table 2 *HOMOGENEITY OF VARIANCES TEST (LEVENE'S)-OBJECTIVE-1*

Factors	F	df1	df2	p
Place	14.9	3	397	<.001
Gender	0.56	1	399	0.455
Age group	18.7	3	397	<.001
Educational Qualification	4.4	4	396	0.002
Occupation	5.75	4	396	<.001
Income (Per Annum)	11.1	3	397	<.001
Investment Experience	14.2	3	397	<.001
Preferred Investment Mode	5.81	2	398	0.003
Type of Digital Platforms Used	12.3	4	396	<.001

Source: Survey Data-SPSS output

Levene's Test results for 401 respondents show significant variance differences across most demographic factors ($p < 0.05$), with age group recording the highest F value (18.7). However, gender showed a non-significant p-value (0.455), indicating equal variances between male and female respondents. Overall, variance differences exist among most respondent groups.

Table 3 *ANOVA - OBJECTIVE-1*

Factors	Sum of Squares	df	Mean Square	F	p
Place	5.92	3	1.98	9.24	<.001
	84.87	397	0.21		
Gender	3.18	1	3.18	14.5	<.001
	87.62	399	0.22		
Age group	2.80	3	0.93	4.21	0.006
	87.99	397	0.22		
Educational Qualification	0.46	4	0.11	0.499	0.736
	90.34	396	0.23		
Occupation	3.83	4	0.96	4.36	0.002
	86.96	396	0.22		
Income (Per Annum)	0.51	3	0.17	0.74	0.529
	90.29	397	0.23		
Investment Experience	3.26	3	1.09	4.93	0.002
	87.53	397	0.22		
Preferred Investment Mode	0.37	2	0.19	0.822	0.44
	90.42	398	0.23		
Type of Digital Platforms Used	0.88	4	0.22	0.964	0.427
	89.92	396	0.23		

Source: Survey Data-SPSS output

The ANOVA results for Objective-1 with 401 respondents show significant differences across place, gender, age group, occupation, and investment experience ($p < 0.05$), with gender recording the highest F value (14.5). However, educational qualification, income, preferred investment mode, and type of digital platforms used showed no significant differences ($p > 0.05$). Overall, demographic variables significantly influence respondents' opinions on online fraud and investment behaviour.

Table 4 *POST HOC COMPARISONS OBJECTIVE -1*

Factor		Basis	MD	SE	df	t	p_{tukey}
Place	Bangalore	Mysore	0.32	0.06	397	5.04	<.001
		Hassan	-0.20	0.06	397	-3.10	0.011
	Mysore	Chamarajanagara	-0.23	0.06	397	-3.64	0.002
Gender	Male	Female	0.18	0.05	399	3.80	<.001
Age- Group	18-25	26-33	-0.21	0.06	397	-3.47	0.003
Occupation	Student	Salaried Employee	-0.21	0.06	396	-3.41	0.006
		Business/ Self Employed	-0.19	0.06	396	-3.02	0.023
Investment Experience	Less than 1 year	1-3 years	-0.20	0.07	397	-3.11	0.011
		3-5 years	-0.17	0.06	397	-2.78	0.029

Source: Survey Data-SPSS output

The post hoc analysis for Objective-1 identified significant differences across place, gender, age, occupation, and investment experience. Bangalore respondents differed significantly from Mysore (MD = 0.32, p < .001), while males scored higher than females (MD = 0.18, p < .001). Significant differences were also found among age groups, occupations, and investment experience levels, indicating their influence on the study variable.

H_{02}: Cyber security awareness does not significantly influence the safe usage behavior of digital financial platform users.

Table 5 *ONE SAMPLE T-TEST OBJECTIVE-2*

Variables	Statistic	df	P
Awareness-driven usage	35.4	400	<.001
Secure app preference	31.1	400	<.001
Risk-aware app usage	26.1	400	<.001
Security feature checks	27.3	400	<.001
Untrusted platform avoidance	25.8	400	<.001
Confidence in usage	28.2	400	<.001
Safe app practices	26.9	400	<.001
Increased digital usage	32.3	400	<.001
Regular app updates	28.8	400	<.001
OTP and biometrics	32	400	<.001

Note. H_a $\mu \neq 3$

Source: Survey Data-SPSS output

The One Sample T-Test indicates that all variables are statistically significant at the 0.001 level, showing that respondents' perceptions differ significantly from the test value of 3. Awareness-driven usage recorded the highest t-value (35.4), reflecting strong digital awareness. Increased digital usage (32.3) and OTP and biometrics (32.0) also showed high significance, indicating widespread adoption of secure practices. Although untrusted platform avoidance had the lowest t-value (25.8), it remained highly significant. Secure app preference, regular app updates, and confidence in usage further contributed positively. Overall, the results confirm strong digital awareness and safe app usage behavior among respondents.

VIII. Results and Discussions

- Cyber threat awareness recorded the highest mean score (Mean = 4.59, SD = 0.70), followed by investment precautions (Mean = 4.26) and platform avoidance (Mean = 4.20), indicating strong awareness and preventive behaviour.
- Significant differences were found across place ($F = 9.24$, $p < .001$), gender ($F = 14.5$, $p < .001$), age group ($F = 4.21$, $p = 0.006$), occupation ($F = 4.36$, $p = 0.002$), and investment experience ($F = 4.93$, $p = 0.002$); post hoc results showed differences between Bangalore and Mysore (MD = 0.32, $p < .001$) and males and females (MD = 0.18, $p < .001$).
- As ANOVA significance values were below 0.05 for key demographic variables, H_{01} was rejected, confirming a significant impact of cyber threats on users' investment behaviour in Karnataka.
- Awareness-driven usage recorded the highest mean score (Mean = 4.42, SD = 0.81), followed by OTP and biometrics (Mean = 4.28) and increased digital usage (Mean = 4.19), indicating strong security awareness and practices.
- All variables were statistically significant ($p < .001$), with awareness-driven usage showing the highest t-value (35.4), followed by increased digital usage (32.3) and OTP and biometrics (32.0).
- As all significance values were below .001, H_{03} was rejected, confirming that cyber security awareness significantly impacts users of digital financial platforms.
- Strengthen cyber security awareness programs to further enhance users' ability to identify and prevent phishing, fraud, and other online threats.
- Promote the use of secure authentication measures such as OTPs, biometrics, and multi-factor authentication to improve confidence in digital financial platforms.
- Implement demographic-specific security education initiatives, focusing on groups showing significant differences by place, gender, age, occupation, and investment experience to ensure effective risk mitigation.

IX. Conclusion

This study concludes that cyber security threats such as phishing, online fraud, and unauthorized access have a significant impact on the behavior and trust of digital finance users in Karnataka. The findings reveal that demographic factors such as place, gender, age, occupation, and investment experience influence users' perceptions of cyber risks. Furthermore, cyber security awareness plays a crucial role in promoting safe digital financial practices, including the use of secure authentication methods and cautious platform usage. Overall, enhancing cyber security awareness and strengthening preventive measures can significantly reduce vulnerabilities and improve confidence in digital financial platforms among users.

Future research can expand the study by covering a larger sample across different states of India to improve the generalizability of the findings. Comparative studies between urban and rural digital finance users can provide deeper insights into cyber security awareness levels and risk exposure. Additionally, longitudinal studies can assess how cyber security awareness and user behavior evolve over time with changing digital threats.

Bibliography

Journal Details

1. Abu Barkat Ullah, Wanli Ma, Mohiuddin Ahmed, Bazlur Rashid, Munir Ahmad Saeed, Omer Arshad & Utkarsh Raghav (2025) "A comprehensive review of cyber security and current practices in global mining critical infrastructure", *Journal of Cyber Security Technology*, Vol 10, Issue 1, pp. 1-27.
2. Adetunji Paul Adejumo & Chinonso Peter Ogburie, (2025) "The role of cyber security in safeguarding finance in a digital era", *World Journal of Advanced Research and Reviews*, Vol 25, Issue 3, pp. 1542–1556.
3. Adetunji Paul Adejumo and Chinonso Peter Ogburie, (2025) "Strengthening finance with cyber security: Ensuring safer digital transactions", *World Journal of Advanced Research and Reviews*, Vol 25, Issue 3, pp. 1527-1541.
4. Ahmed M. Abdelmagid, Farshid Javadnejad, Michael Mcshane, Rafael Diaz & Cesar A. Pinto (2025) "A New cyber risk identification and assessment approach of the maritime cyber risks", *Enterprise Information Systems*, Vol. 19, Issue 10, pp. 1-25.

5. Anayo Chukwu Ikegwu, Jasmine Chifurumnanya Nnabue, Annastasia Shako Kinse and Uzoma Rita Alo (2026) "Cyber Threat Intelligence and Embedded System Driven Security for mHealth Data", *Journal of Cloud Computing*, Vol. 15, Issue 11, pp. 1–24.
6. Bo Norregaard Jørgensen and Zheng Grace Ma (2026) "Cyber security and Resilience of Smart Grids: A Review of Threat Landscape, Incidents, and Emerging Solutions", *Applied Sciences Multidisciplinary Digital Publishing Institute*, Vol 16, Issue 2, pp. 981–1011.
7. Damodharan Kuttiyappan and Dr.Rajasekar V (2023) "Improving the Cyber Security over Banking Sector by Detecting the Malicious Attacks Using the Wrapper Stepwise Resnet Classifier", *KSII Transactions on Internet and Information Systems*, Vol. 17, Issue 6, pp 1657–1681.
8. Dave Brown, Usman Butt, Bilal Naqvi, & Saber Farag, (2026) "Bridging the digital gap: security, privacy and challenges for older adults in governmental digital services", *Information & Computer Security*, Vol. 34, Issue 2, pp. 245-263.
9. Doney Abraham, Siv Hilde Houmb, & Laszlo Erdodi (2023) "Cyber-Attacks on Energy Infrastructure-A Literature Overview and Perspectives on the Current Situation", *Applied Sciences Multidisciplinary Digital Publishing Institute*, Vol. 15, Issue 17, pp. 1-19.
10. Duo Wang and Yanxi Li (2026) "A stitch in time saves nine: Does cyber security legislation decrease debt default risk?" *Journal of Accounting Literature*, Vol. 48, Issue 3, pp. 321-352.
11. Eugenio Lilli (2020) "President Obama and US cyber security policy", *Journal of Cyber Policy*, Vol 5, Issue 2, pp. 265-284.
12. Fathey Mohammed, Muadh Mukred, Mubbasher Munir and Ibrahim T. Nather Khasro (2026) "Understanding older adults' vulnerabilities to digital investment fraud: a conceptual model and instrument development", *The Journal of Adult Protection*, Vol. 28, No. 2, pp. 104-121.
13. Harting, Ralf-Christian, Bueechl Joerg, Anderlohr Philipp, Betz Lukas, (2025) "The Impact of Effective Risk Management on the Cyber Performance of Enterprises", *Procedia Computer Science*, Vol. 270, Issue -, pp. 4343–4352.
14. Isabel Maldonado, Amélia Ferreira da Silva, Carlos Pinho, and Gonçalo Santos (2026) "Cybersecurity in accounting: challenges and strategies for SME resilience", *Journal of Accounting & Organizational Change*, Vol. 22, Iss. 1, pp. 1-25.
15. Jones Márcio Nambundo, Otávio de Souza Martins Gomes, Adler Diniz de Souza, and Raphael Carlos Santos Machado (2025) "Cyber security and Major Cyber Threats of Smart Meters: A Systematic Mapping Review", *Energies Multidisciplinary Digital Publishing Institute*, Vol 18, Issue 6, pp. 1445-1466.
16. Joseph Opuni-Frimpong (2026) "Cyber security disclosures and bank credit risk exposure", *International Journal of Bank Marketing*, Vol. 44, Issue 1, pp. 1–27.
17. Julija Saveljeva and Tatjana Volkova (2025) "Category-specific effects of digital trust on third-party risks in the banking industry", *The Journal of Risk Finance*, Volume 27, Issue 2, pp. 329-345.
18. Kate-Riin Kont, & Denis Horenženko (2026) "Cyber risk management among tax and customs officials: the pilot study in Estonia", *Information & Computer Security*, Vol. 34, Issue 2, pp. 245–262.
19. Kevin F. McCrohan, Kathryn Engel, & James W. Harvey (2010) "Influence of Awareness and Training on Cyber Security", *Journal of Internet Commerce*, Volume 9, Issue 1, pp. 23-41.
20. Martin Eling, Michael McShane, Trung Nguyen, (2021) "Cyber risk management: History and future research directions", *Risk Management and Insurance Review*, Vol. 24, Issue 1, pp. 93–125.
21. Mohammed Afzal, Maryam Meraj, Manpreet Kaur & Mohd. Shamim Ansari (2025) "How does cyber security awareness help in achieving digital financial inclusion in rural India under escalating cyber fraud scenario?", *Journal of Cyber Security Technology*, Vol 9, Issue 2, pp 88-126.
22. Moshood F. Yussuf, Pelumi Oladokun, Mosope Williams (2020) "Enhancing Cybersecurity Risk Assessment in Digital Finance through Advanced Machine Learning Algorithms", *International Journal of Computer Applications Technology and Research*, Volume 09, Issue 06, pp. 217-235.
23. Mosope Williams, Moshood F. Yussuf, and Ayomide Oluwaromika Olukoya (2021) "Machine learning for proactive cyber security risk analysis and fraud prevention in digital finance ecosystems", *International Journal of Engineering Technology Research & Management*, Vol-05, Issue 12, pp. 160-177.
24. Natile Nonhlanhla Cele and Sheila Kwenda (2024) "Do cyber security threats and risks have an impact on the adoption of digital banking? A systematic literature review", *Journal of Financial Crime*, Vol. 31, No. 1, pp. 31–48.
25. Ntokozo F. Miya, Nazeer Joseph. (2025) "Banking on resilience: 20 years of Cyber security evolution", *South African Journal of Information Management*, Vol. 25, Issue 1, pp. 1-16.

26. Rahime Belen-Saglam, Haiyue Yuan, Maria Sophia Heering, Ramsha Ashraf, & Shujan Li (2025) "A Systematic Literature Review on Cyber Security and Privacy Risks in MaaS (Mobility-as-a-Service) Systems", *Information Multidisciplinary Digital Publishing Institute*, Vol 16, Issue 6, pp 1–36.
27. Ramlan Amir Isa, Bambang Setiawan, & Pakaja, (2026) "Cyber security awareness in the digital commerce ecosystem: factor analysis, program impact and future trends for consumers and MSMEs", *Information & Computer Security*, Vol. 34, No. 1, pp. 1-22.
28. Samir Bhowmik & Annesha Saha (2025) "Digital finance in MSMEs: Adoption, governance, and risk management", *The EDP Audit, Control, and Security Newsletter*, Volume 70, Issue 10, pp. 1-22.
29. Serpil Sevimli Deniz, Mehmet Atas (2026) "Human cyber risk in the on boarding process: a quantitative assessment of phishing susceptibility among new hires", *Information & Computer Security*, Vol. 3, Issue 4, pp. 3-33.
30. Siyabulela Sandi and Carolien L. van den Berg (2025) "Cyber security mind set and up skilling: Resilience via lifelong learning and security education", *South African Journal of Information Management*, Vol. 27, Issue 1, pp. 1–12.

Webliography

https://www.pib.gov.in/
https://timesofindia.indiatimes.com/
https://statisticstimes.com/
https://indiadatamap.com/