International Journal of Academic Research
P-ISSN: 2348-7666: Impact Factor: 6.023
Homepage: https://www.ijar.org.in/
Volume-12, Issue-3(2), Jul-Sep-2025

"INVESTORS' PERCEPTION TOWARDS CYBER THREATS AND DIGITAL SECURITY IN THE INDIAN STOCK MARKET - AN EMPIRICAL STUDY"

[1] Vijay J. M., [2] Dr. Giridhar K. V.

[1] Research Schalor, Sahyadri Commerce and Management College, Constituent College of Kuvempu University, Shivamogga – 577203. Email: vijayjmjm@gmail.com
[2] Professor and Research Supervisor, Sahyadri Commerce and Management College, Constituent College of Kuvempu University, Shivamogga – 577203. Email: giridhar.management@gmail.com

Abstract:
The Indian stock market has seen a rise in retail participation due to digitalization and initiatives like Digital India. Though such a change is improving market access, it also makes retail investors more vulnerable to online scams such as phishing, OTP fraud and identity theft. The current inquiry focuses on the perceptions, the levels of awareness, trust, and preparedness of the investors on the topic of digital security, with a particular emphasis put on the retail members of investment community in Shivamogga, Karnataka. Findings show that a majority of them; particularly the younger and better-educated investors, recognize the threat to digitalization and are using protective measures like strong passwords and two-factor authentication. The results indicate that more digital literacy is needed and that at least region-specific awareness building programs are established in addition to heightened cybersecurity controls provided by the regulators and trading platforms so that India is not going to lose the level of security that its growing digital market is going to offer to everyone who is interested in investing.
Key Words: Investors' Perception, Digital Security, Cyber Threats, Indian Stock Market, Cybersecurity Awareness.

INTRODUCTION

The Indian stock market hold the middle ground of the national financial architecture by offering ways to bring about capital formation, growth of wealth and also the economic growth in India. It is the evolution of the informal community of brokers of the nineteenth century that has resulted into a well-regulated and high technological system governed by various institutions like the Bombay Stock Exchange (BSE) and the National Stock Exchange (NSE). Through these exchanges, it is able to trade in equities, derivatives and other forms of debt instruments hence invites both foreign and local investors to trade. The spread of digital infrastructure and programs such as the Digital India, have made the stock market available to a larger number of people. Investing has become a globally available business where investors can use their mobiles to start a trade and track their investments in real-time using mobile apps online trading services and digital payments. This technological upgrade has levelled the playing field when it comes to investing, attracting a new generation of retail customers both in cities and rural environs.

The digitization process that is being taken place in the financial markets is giving rise to a new set of challenges. Movement of transactional and trade processes towards internet-based

infrastructures has increased the amount of exposure to cyber threats. Examples of such vulnerabilities are phishing attacks, data losses, malware attacks, and identity thefts, among which they are very central issues in the capital market ecosystem. Players at any point of the chain (a single investor, a trading account, a trading platform, etc., all the way through to a stock exchange) remain vulnerable to hacking and thus exposing sensitive financial data and opening incidences of operations interruption.

It will be observed that in 2025, the digital participation in the stock market in India was considerably positive, with 194 million demat accounts in the retail stock market (Business Standard, 2025). This is also an attribute of increased financial inclusiveness, but it also creates greater exposure to cyber risk. Financial sector experienced more than 3, 4 lakh cybersecurity events in the previous fiscal year, with a strong spike in both phishing and ransomware activities (Fintegriti, 2024). The inability to secure data was also highlighted by a visible data leak at Angel One in the first months of 2025 when the market temporarily lost trust (Reuters, 2025).

Due to the increasing cyber-related risk, the Securities and Exchange Board of India (SEBI) has implemented a more demanding Cybersecurity and Cyber Resilience Framework in January 2025. The framework highlights competent security measures, enforcement of risk-management systems and increased investor education. At that, the central government increased its budget allocation on cybersecurity to 759 crore (Moneycontrol, 2025). The brokers and exchanges have in turn, strengthened their security, which involves the introduction of two-factor authentication (2FA), encryption, firewalls, and a set of regular cyber-audits. Despite these efforts, any cyber threats remain both increasing in size and sophistication, and the need to maintain consistent digital security in the financial environment within India that is quickly going through the digitalizing process.

REVIEW OF LITERATURE

A literature review summarizes existing research on a topic. Here, it highlights studies on how cyber-attacks affect stock markets, investor behavior, and firm responses.

Tosun (2020) analysed the impacts of cyber-attacks on U.S. stock markets by corporations. The analysis applied an event study and also difference in differences (DID) analysis to show that firm specific breaches trigger short-term drop-in stock returns, increased sell side gobbling, and diminished liquidity. Another finding involves showing that investor interest increases drastically post attacks hence affecting firm reputation and market conduct at large. The long-term performance indicators as such appear to be rather stable, but the changes in R&D budgets, dividends, and the compensation of CEOs display the long-lived effects of policies. The research thus shows that computer attacks are reputational shocks able to change the perception in the market as well as corporate strategy.

Garg and Garg (2023) analysed the cybersecurity issues in the Indian securities market and considers the phishing, malware, and insider attacks as the main threats that undermine investor confidence. The study discuss Securities and Exchange Board of India (SEBI) theory of cybersecurity and outline the essential risk factors that can threaten the stability of the market. The conclusion talks about the need of having stronger regulation, greater awareness on the part of the investor, and the use of the emerging technology, so as to safeguard the digital securities ecosystem.

Jiang et al. (2023) explored a firm-level measure of cyber risk as a predictor of cyberattacks and their effects on stock returns based on machine learning. Using it logistic ridge regression

on company data and ten-K disclosures from 2006 to 2018, they have constructed the metric. The research found that in companies dealing with greater cyber risk occur more frequently problems and higher, on average, credit earning – evidence prevails of risk premium. It also demonstrated that cyberspace Exchange Traded Funds (ETFs) do well when high-risk companies lose, backing the notion that cyber-risk is a critical, priced factor in financial markets.

Veiga et al. (2023) explored recent systematic review of what is known currently about cybersecurity in financial organizations. The three related areas that the authors focus on include threat landscape, countermeasures at the firm level and the financial implications. Some of the main weaknesses include data breaches and service outages, which act to destroy stakeholder confidence, as well as the stability of the market. The review also notices an increase level of attention towards regulation and emerging technology state-of-art including artificial intelligence and blockchain. Lastly, the authors recommend further investigation of the ways investors and market players can react to the threat of cyber-attacks, referring to this dimension as a particularly insufficiently studied one.

Cele and Kwenda (2025) considered the critical review of 58 empirical studies that determine the level of cybersecurity risks on the adoption of digital banking in South Africa. The authors came up with the identification of major threats namely phishing, vishing, malware and identity theft that undermine customer confidence. The review identified 17 precise threats and suggested 13 adequate mitigation strategies involving training of users and implementation of secure software. According to the analysis, the hurdle to its wider use continues to be cybersecurity, despite the apparent benefits of digital banking.

RESEARCH GAP

Although the study has focused on the effects of cyber-attacks on stock prices and digital banking practices in the United States and South Africa, very little has been given to the view of Indian investors regarding security on digital security. Therefore, empirical studies so far focus on the institutional responses with little information on how individual investors perceive threats, gain trust, and develop behavior. In addition, there are no particular studies of this phenomenon in one of the areas of participation in the digital stock market, which is growing steadily in Shivamogga. This is the gap that this research paper aims at filling its title is given as, "**Investors Perception towards Cyber Threats and Digital Security in the Indian Stock Market - An Empirical Study"** has been undertaken.

OBJECTIVES

The objectives guide the purpose of the study. This research aims to understand investor perception and response to digital security and cyber threats in the Indian stock market.

1. To examine individual investors' perception, awareness, and trust regarding cyber threats and digital security in the Indian stock market.
2. To assess the preparedness and behavioural response of investors towards cybersecurity risks in digital stock trading.

HYPOTHESIS

A hypothesis is a tentative assumption made to draw conclusions and guide the direction of research. The following hypotheses have been formulated for the purpose of this study.

H_0: There is no significant association between investors' awareness of cybersecurity risks and their preparedness for secure digital stock trading.

International Journal of Academic Research
P-ISSN: 2348-7666: Impact Factor: 6.023
Homepage: https://www.ijar.org.in/
Volume-12, Issue-3(2), Jul-Sep-2025

SCOPE AND METHODOLOGY

This study examines the individual investors perceive digital security and the awareness they have towards it and subsequent response concerning the issue of cyber threats in the Indian equity market. Quantitative and descriptive methodology has been followed in which a structured questionnaire was used to collect primary data on 50 retail investors in Shivamogga. These data were enhanced through secondary sources that are books, journals, and the web sites. It used convenience sample and statistical measures of percentages, mean, standard deviation and Spearman rank correlation test to analyse the research hypotheses were done.

RESULT AND DISCUSION

This part summarizes the empirical results of the empirical study which have been developed in accordance with the collection of empirical statistics results. The findings are discussed against the research objectives and hypothesis thus throwing the light on the behaviour and the perception of the investor as regards to the digital protection and cyber threats in the Indian stock market.

Table No. 1 Demographical Profile

Demographical Factors	Variables	Frequency (N)	Percentage
Gender	Male	38	76%
	Female	12	24%
	Total	**50**	**100%**
Marital Status	Married	19	38%
	Unmarried	31	62%
	Total	**50**	**100%**
Age(Years)	Below 25	16	32%
	25-30	19	38%
	31-40	7	14%
	41-50	4	8%
	Above 50	4	8%
	Total	**50**	**100%**
Occupation	Student	28	56%
	Self Employed	5	10%
	Private Sector Employee	9	18%
	Government Employee	8	16%
	Total	**50**	**100%**
Education Level	High School or Below	2	4%
	Undergraduate	5	10%
	Postgraduate	39	78%
	Professional	4	8%
	Total	**50**	**100%**

International Journal of Academic Research
P-ISSN: 2348-7666: Impact Factor: 6.023
Homepage: https://www.ijar.org.in/
Volume-12, Issue-3(2), Jul-Sep-2025

Monthly Income (₹)	Less than 25000	32	64%
	25000-50000	8	16%
	50001-75000	2	4%
	75001-100000	0	0%
	Above 100000	8	16%
	Total	**50**	**100%**

Source: *Field Survey*

Population of the discussed 50 surveyed people depicts the dominated number of the young respondents; that is to say; the majority of the participants are males and are academically educated: 76 % are male and 62 % unmarried. Around 70 % are aged below 30, and 56 % were students, thus, defining the sample as technologically forward and digital in a sense. Educationally, 78 % have postgraduate academic status, which demonstrates high cognitive and practical potential to deal with digital finance. In terms of income, 64 % of respondents earn up to 25000 rupees per month, which is characteristic of young workforce or those in a non-working capacity. Summing these facts up, they can be compared to modern trends in digital investment uptake: the younger, educated population has an increased level of using online resources and is highly aware of digital security problems.

Table No. 2 Perceived common Cyber Threats among Respondents

Cyber Threats	**Frequency**	**Rank**
Phishing – Fake messages to steal info.	42	1
OTP Fraud – Tricking you to give OTP.	32	2
Password Hacking – Stealing your password.	26	3
Identity Theft – Using your details for fraud.	24	4
Malware – Harmful software.	21	5
Spyware – Secretly tracks your activity.	20	6
Ransomware – Locks files, demands money.	14	7

Source: *Field Survey*

The current set of data suggests that phishing (42) is the most common type of cyber threat followed by OTP fraud (32) and password hacking (26). These results highlight the high danger of predatory behavior. It is important to mention that identity theft (24), malware (21), and spyware (20) are also prominent, although ransomware (14) is the least reported category of attacks still being regarded as rather severe. Together, the users face significant risk of scam aimed at stealing personal and log-in details.

Table. No. 3 Showing the Perception, Awareness, and Trust of the respondents towards Cyber Threats and Digital Security. (SD-1, D-2, N-3, A-4, SA-5)

Sl. No	**Perception, Awareness, and Trust**	**1**	**2**	**3**	**4**	**5**	**Total**	**Mean**	**Standard Deviation**
1	I am aware of the risks involved in online stock trading.	3	2	3	24	18	50	4.04	10.27

2	I believe cybersecurity is important in digital investing.	0	2	8	23	17	50	4.1	9.82
3	I follow cybersecurity news related to financial markets.	2	0	10	23	15	50	3.98	9.46
4	I understand basic online trading safety practices.	0	4	2	28	16	50	4.12	11.83
5	I trust the security measures of my trading platform.	4	0	6	29	11	50	3.86	11.34
6	I believe SEBI ensures digital safety in stock markets.	0	3	8	23	16	50	4.04	9.46

Source: *Field Survey*

The data indicates a strong awareness and positive attitude toward cybersecurity among digital investors. Most respondents agree or strongly agree that they understand online trading risks (mean = 4.04), value cybersecurity (mean = 4.1), and follow safety practices (mean = 4.12). They also stay updated on cybersecurity news (mean = 3.98), trust their trading platforms (mean = 3.86), and believe SEBI ensures digital safety (mean = 4.04). Overall, the findings reflect a high level of cybersecurity awareness in digital stock trading.

Table. No. 4 Showing the Preparedness and Behavioural Response of the respondents towards Cyber Threats and Digital Security. (SD-1, D-2, N-3, A-4, SA-5)

SI. No	Perception, Awareness, and Trust	1	2	3	4	5	Total	Mean	Standard Deviation
1	I use strong, unique passwords for trading.	2	0	1	20	27	50	4.4	12.59
2	I enable two-factor authentication (2FA).	2	0	6	28	14	50	4.04	11.40
3	I avoid suspicious links and do not share OTPs.	1	2	11	12	24	50	4.12	9.30
4	I check my trading account for unusual activity.	2	2	8	20	18	50	4	8.60
5	I would stop using a platform with repeated breaches.	3	0	7	24	16	50	4	9.87

Source: *Field Survey*

The responses indicate that most participants practice good cybersecurity habits while trading online. A majority use strong, unique passwords (mean = 4.4), enable two-factor authentication (mean = 4.04), and avoid suspicious links or sharing OTPs (mean = 4.12). Many regularly check their accounts for unusual activity (mean = 4) and are willing to stop using platforms with repeated security breaches (mean = 4). Overall, the data reflects a high level of awareness and proactive behavior toward securing online trading accounts.

HYPOTHESIS TESTING

The Spearman rank correlation plot of the association between the perception of cyber threat among the investors and the preparedness to conduct safe online stock trading was used. Being a non-parametric, it perfectly fits ordinal data and measures the degree as well as direction of the properties between two ranked variables.

International Journal of Academic Research
P-ISSN: 2348-7666: Impact Factor: 6.023
Homepage: https://www.ijar.org.in/
Volume-12, Issue-3(2), Jul-Sep-2025

H_0: There is no significant association between investors' awareness of cybersecurity risks and their preparedness for secure digital stock trading.

Spearman rank correlation

Particulars			**Awareness Score**	**Preparedness Score**
Spearman's rho	Awareness Score	Correlation Coefficient	1.000	0.459
		Sig. (2-tailed)		.001
		N	50	50
	Preparedness Score	Correlation Coefficient	0.459	1.000
		Sig. (2-tailed)	.001	
		N	50	50
Correlation is significant at the 0.01 level (2-tailed).				

Source: *SPSS Output*

Interpretation of Results

A Spearman rank correlation was conducted to assess the relationship between investors' awareness of cybersecurity threats and their readiness for secure digital stock trading, using data from **50** respondents. The analysis yielded a **correlation coefficient (ρ) of 0.459,** indicating a moderate positive association. This suggests that increased awareness is linked to greater preparedness. The p-value was **0.001**, which is **below** the **0.05** significance level, confirming that the result is **statistically significant**.

Based on the findings, the null hypothesis **(H_0)** - which states that there is no significant association between investors' cybersecurity awareness and their preparedness for digital stock trading is **rejected**. The results provide evidence of a significant **positive association** between the two variables. This supports the study's objective that enhanced awareness of cybersecurity risks positively influences investor preparedness, thereby contributing to safer and more informed digital investment practices.

Using data on 50 respondents, it was possible to conduct a Spearman rank correlation study that examined the connection between the awareness of the threat of cybersecurity among investors and their preparation towards making secure digital dealings in trading stocks. The resulting analysis gave a **correlation coefficient (p), 0.459,** which means that there was a moderate positive correlation. It is an indication that one needs to be aware of more to be prepared. The p-value is 0.001, less than 0.05 significance level which corresponds to the fact that the result is statistically significant.

With such results, the null hypothesis (H0) - According to which there is no substantial relationship between cybersecurity awareness among investors and their being ready to trade digitally with stocks - is rejected. The results offer support of strong positive relations between the two variables. The relevance of the study goal, namely, that greater awareness of cybersecurity risks has a beneficial effect on investor preparedness, is thus confirmed, and can be contributed to safer and better-informed digital investment behavior.

SUGGESTIONS AND CONCLUSION

The level of cybersecurity literacy is one of the key factors determining the safe involvement in the market, and it must be improved. SEBI and trading platforms ought to develop and carry out long-term awareness programs that concur widespread dangers like phishing and OTP fraud. Strengthening user-based defensive mechanisms, such as two-factor authentication, live notifications, advanced fraud prevention systems, would protect the market players further. Schools and colleges would benefit by integrating the basic course of studies in digital-security to instil the skills and knowledge needed by new investors. It is also recommended that the localized awareness programs be introduced in the semi-urban settings like the one in Shivamogga to fill the regional gaps on the spectrum of digital literacy.

Overall, the empirical evidence indicates that awareness as well as preparedness regarding cybersecurity is strong among the investors particularly amongst the younger and well-educated generations. The positive association that is strong between these two constructs reveals that informed investors have safer trading behavior. Increasing and perfecting of education delivery and technological protection will solidify investor assurance and more secure investment in the Indian stock-market.

REFERENCE

1. Cele, B., & Kwenda, F. (2025). Cybersecurity threats and digital banking adoption in South Africa: A systematic review. [Manuscript in preparation].
2. Garg, S., & Garg, D. P. (2023). Alarming concerns around cyber security in the securities market. SSRN. https://ssrn.com/abstract=4907612
3. Jiang, Z., Lee, C. M. C., & Xie, Y. (2023). Measuring firm-level cyber risk. Journal of Financial Economics, 149(2), 584–610. https://doi.org/10.1016/j.jfineco.2023.02.002
4. Tosun, O. K. (2020). The impact of corporate cyberattacks on U.S. stock markets. Journal of Corporate Finance, 62, 101590. https://doi.org/10.1016/j.jcorpfin.2020.101590
5. Veiga, A., Fernandes, L., & Silva, M. (2023). Cybersecurity in financial markets: A systematic literature review. Journal of Financial Markets, 63, 100806. https://doi.org/10.1016/j.finmar.2023.100806
6. Business Standard.(2025). (N.d. Stock markets in India go digital as the number of demat accounts is past 194 million, Retrieved from www.business-standard.com
7. Fintegriti. (2024). Annual Report on Cyber Security for Indian Financial Sector. It is downloaded at www.fintegriti.in
8. Moneycontrol. (2025). Cybersecurity budget to Go up by 25 per cent to 759 crores. Accessed 5th March 2012- http://www.moneycontrol.com
9. Reuters. (2025). In early 2025, the investor confidence is shaken by Angel One breach. The information was retrieved at www.reuters.com
10. SEBI. (2025). Circular No. SEBI/ HO / MIRSD / TPD / CIR / P / 2025/ 03 dated 10.06.2022 Cybersecurity and Cyber Resilience Framework. The source: www.sebi.gov.in