Investor Trust and Trading App Verification: A Conceptual Framework

Ashoka K. G.
Assistant Professor, Alva's College, Karnataka, India
Email: rch.spt24@gmail.com | ORCID: 0009-0004-3926-2873
Shilpa Bhat N. H.*
Dr. NSAM First Grade Degree College, Nitte, Karnataka, India
Email: rch.spt24@gmail.com | ORCID: 0009-0001-2259-8950
Mahendra H. R.
Research Scholar, Mangalore University, Karnataka, India
Email: mahendraripponpet@gmail.com | ORCID: 0009-0001-4203-0748
Karthik Naik
Assistant Professor, Alva's College Autonomous, Moodubidire, Karnataka, India
Email: knaik751992@gmail.com | ORCID: 0009-0008-0431-3617
**Corresponding author: Shilpa Bhat N. H.,* rch.spt24@gmail.com

Abstract

This conceptual paper examines why investors may trust a trading application that looks official without confirming who published it. It asks whether displayed verification symbols affect perceived legitimacy, whether independently checkable app origins and actual source checks improve identification, and whether a short reminder can help people distinguish genuine from deceptive applications. The analysis draws on selected financial-literacy, investor-behaviour and digital-finance studies, together with research on online trust signals and Indian securities regulation. It proposes a framework separating visible assurances, source provenance, independent checking and correct authentication. Seven hypotheses are developed and a controlled vignette experiment is outlined for later testing. The conceptual analysis suggests that a verification symbol should be interpreted in the context where it appears: a label attached to a genuine marketplace listing is not equivalent to its image in an unsolicited message. The paper does not report survey observations or estimated effects. Its contribution is a testable explanation of how investors can move from initial confidence to justified trust, while recognising genuine apps and rejecting deceptive copies.

Keywords: trading apps; investor trust; verification signals; source provenance; investment fraud

1. Introduction

Digital trading has made access to securities markets easier, but it has also created new opportunities for impersonation. An investor can encounter an application through an official app marketplace, a broker's website, a social-media advertisement or a forwarded message. These routes may display the same broker name and similar graphics, although only some provide a dependable way to confirm the software publisher. This is a current investor-protection issue in India. On 25 March 2026, the Securities and Exchange Board of India (SEBI) introduced a verified label for trading applications of SEBI-registered stockbrokers on Google Play, following warnings about social-media investment scams (SEBI, 2025, 2026). The label is intended to help investors identify genuine apps in that marketplace. It does not mean that a picture of the label pasted into a message verifies the download link supplied with that message. The question is therefore not whether a symbol looks official, but whether its origin can be established independently.

Studies of investor knowledge explain why this distinction cannot be solved by financial awareness alone. Lusardi and Mitchell (2014) established the importance of financial literacy for economic decisions, while van Rooij et al. (2011) connected literacy with stock-market participation. In India, Agarwalla et al. (2015) documented differences in financial knowledge, attitudes and behaviour among working young adults. Potrich et al. (2016) likewise treated financial literacy as more than the ability to answer factual questions. These findings are relevant because investors need knowledge to understand financial products and evaluate risk. However, participation, knowledge and a

favourable investment attitude do not establish whether an app actually belongs to the broker it names. Authentication requires evidence about the specific software and its publisher.

Digital skills and confidence also deserve separate attention. Ravikumar et al. (2022) developed a multidimensional measure of digital financial literacy among Indian adults, including awareness of digital risks and consumer protection. Lind et al. (2020) distinguished objective financial competence from confidence in that competence. Mishra and Metilda (2015) reported relationships between investment experience and overconfidence among Indian investors, while Chalissery et al. (2023) examined trading experience and susceptibility to behavioural biases. Kawamura et al. (2021) further showed that financial knowledge does not automatically eliminate problematic financial choices. More directly, Isaia et al. (2024) found that financial knowledge and overconfidence related differently to online-fraud exposure in an Italian study. That evidence concerns fraud experience rather than verification of Indian trading apps, but it gives a clear reason to measure what investors actually do instead of equating confidence with protection. Together, these studies support a narrower concern: someone may be comfortable using a trading app yet still rely on its appearance rather than examining independent evidence of its source. None of these studies directly establishes how investors react to a copied verified-app symbol; that connection remains a proposition for testing.

Research on online assurance provides a reason to examine the appearance of trust separately from its basis. Hu et al. (2010) studied how web-assurance seals shape initial online trust. Kirlappos et al. (2012) showed that people may misunderstand what a trust seal actually certifies. In research on real and fake websites, Kelley et al. (2023) found that analytical reasoning can improve discrimination, although this did not operate uniformly across levels of expertise. This adds a reason to examine how investors interpret the evidence, not only whether they notice a mark. In investment settings, Kumar and Goyal (2016) described behavioural biases in financial choices, while Chandani et al. (2025) examined Indian investors' willingness to rely on financial-influencer advice. These studies point to different sources of influence, but they do not establish whether a person correctly authenticates a trading application when a visually persuasive symbol is not supported by the publisher record. A copied badge and a genuine marketplace-originated label must therefore be treated as different forms of evidence rather than as interchangeable signs of legitimacy.

The research problem is the possible substitution of visible reassurance for source verification. Three questions guide this conceptual paper. First, do displayed verification cues increase perceived legitimacy and mistaken acceptance when offers come from unverified channels? Second, do independently checkable publisher records and observable source-checking actions support accurate identification of both genuine and deceptive apps? Third, can a short source-check prompt improve this distinction without making investors reject genuine apps unnecessarily? The paper develops a framework and hypotheses for these questions, then specifies an experimental procedure by which they could be tested. The proposed contribution is not a new measure of general financial literacy or an estimate of fraud in Karnataka. It is a clearer explanation of the specific decision that must occur before an investor treats a trading app as authentic.

1.1 Research Objectives

1. To explain how displayed verification cues and unverified offer channels may affect perceived legitimacy and mistaken acceptance of deceptive trading apps.

2. To examine the proposed roles of source provenance and observed independent verification in accurate identification of genuine and deceptive trading apps.

3. To develop and assess a testable source-check intervention intended to improve authentication accuracy without increasing false rejection of genuine apps.

2. Methods

2.1 Approach to conceptual analysis

This is a conceptual analysis, not a report of fieldwork. Its starting point is a defined authentication problem: the same visible assurance can be encountered inside an official distribution platform or as a detachable image supplied by an

unverified promoter. The analysis first distinguishes what is shown from what can be verified, then identifies relevant investor responses and develops relationships that can be falsified. Studies on financial literacy, digital knowledge, confidence, trading experience and behavioural bias were selected for this argument from the literature reviewed in the supplied Chapter 2. Related studies on online assurance, persuasion and fraud prevention already cited in the earlier manuscript were retained because they directly address the processes not covered by the Chapter 2 literature. Regulatory material is used to establish the Indian setting. No new systematic-review search or completed participant study is claimed here.

The literature was organised around the three research questions rather than by author or year. The first group concerns the persuasive effects of visual assurance and the risk of misplaced confidence. The second concerns the difference between general financial competence and independently observed verification of a particular app. The third concerns whether guidance provided at the decision point can change action and accuracy. A study was treated as relevant only when its finding or theory supported a specific step in this reasoning. For example, the financial-literacy studies are used to explain investor characteristics, not as proof that a short prompt prevents fraud. This rule keeps the argument connected to the problem and avoids transferring results from unrelated samples into the present setting.

2.2 Construct boundaries

Displayed verification cue refers to a visible badge, logo or regulatory statement attached to an app offer. Source provenance means independently checkable information connecting the software publisher, distribution listing and named intermediary. Perceived legitimacy is the investor's judgement that an application is genuinely associated with the stated provider. Independent verification behaviour is an observed action such as consulting an official intermediary listing or a trusted marketplace record rather than rereading promotional material. Correct authentication is agreement between the investor's classification and a pre-established, independently validated app status. A source-check prompt is a short instruction asking an investor to examine the origin before deciding. These distinctions prevent the model from treating perceived trust, actual checking and a correct decision as the same variable.

Application authenticity must also be separated from investment suitability. A genuine broker app can offer investments involving substantial risk; a high-risk product is not automatically evidence that software is counterfeit. A deceptive app, for this study, would present an independently demonstrable contradiction between its claimed intermediary and its publisher or authorised distribution route. When evidence is insufficient, the appropriate response may be "cannot determine". A person should not be marked incorrect merely because they decline to guess. Likewise, a respondent who identifies an obviously deceptive app without opening several additional records need not be classified as careless. The model therefore evaluates the quality of evidence and final decisions together.

2.3 Protocol proposed for empirical evaluation

A later experiment could recruit about 220 consenting adults who use digital financial services in Karnataka, including current retail investors and potential users of trading apps. This figure is a provisional planning target, not a power calculation or a completed sample. A defensible sample size would be determined before recruitment from the smallest effect of interest, repeated observations and interaction tests. Recruitment from different locations and experience groups could support variation, but a non-probability sample would not justify statewide prevalence estimates. Participants should be able to stop without penalty. Their answers should be analysed without collecting broker passwords, financial balances or identifiable account details. Prior use of investing apps and exposure to investment messages should be recorded because both may shape how participants interpret a verification cue.

Participants could review fictional app offers created from four experimentally controlled features: genuine or deceptive app status, verification cue present or absent, source provenance checkable or obscured, and offer presented within a marketplace-style route or an unverified message. The full design contains 16 combinations; each participant might see a balanced selection of eight scenarios, with combinations rotated across respondents. A separate random assignment would present either a short source-check prompt or neutral instructions. The mock interface would permit participants to open a fictional authoritative app directory and compare publisher details. All app names, records and links would be invented and marked as research material. No participant would be required to install unknown software, provide account credentials or transfer money.

Independent reviewers drawn from investor education, brokerage operations and digital security would be asked to validate the status of each scenario, the realism of its presentation and the clarity of the official-source record. The cue, origin evidence and app status should be varied independently; otherwise the design could accidentally teach respondents that any badge means a genuine app or that unattractive spelling proves deception. A pilot would check whether people can distinguish a native marketplace label from an image within a message. This validation is essential to testing the research questions rather than measuring the participants' attention to superficial design errors.

2.4 Planned analysis and decision criteria

The first objective would be tested with perceived-legitimacy ratings and the rate of mistaken acceptance of deceptive apps under different cue and offer-route conditions. The second would be assessed through recorded source-check actions, the availability of provenance evidence and correct classifications, separately for genuine and deceptive apps. The third would compare participants randomly assigned to a prompt or control condition on source checking, correct identification and wrongful rejection. Mixed-effects logistic models are suitable for binary vignette decisions and can account for repeated assessments within participants. Ordinal or linear mixed models could be selected for legitimacy ratings after checking their measurement properties. Interaction terms should be specified in advance rather than added only after examining results. For the first question, the key contrast is whether cue exposure changes acceptance more strongly in unverified channels. For the second, the analysis should compare participants with and without usable provenance evidence and document which source they consulted. For the third, the relevant comparison is the randomly assigned prompt versus control condition, including both scam rejection and valid-app acceptance. Confidence intervals would show the precision of these estimates; an isolated significant p-value would not establish practical protection.

Confidence, financial literacy, trading experience and digital familiarity may be included as respondent characteristics, but statistical adjustment would not make a voluntary source check causally equivalent to random assignment. The proposed reporting should separate scam detection, recognition of genuine apps, mistaken acceptance, false rejection and defensible uncertainty. An intervention that causes respondents to reject every offer would not demonstrate improved authentication. The intended outcome is better discrimination, not general suspicion. Table 1 summarises how the literature and planned measures connect to each objective.

Table 1. Evidence and planned tests by research question

Research question	Supporting evidence	Proposed observation
Q1. Can a visual cue mislead?	Hu et al. (2010); Kirlappos et al. (2012); Lind et al. (2020)	Cue effect on legitimacy ratings and mistaken acceptance, by offer route
Q2. Do origin records and checks matter?	Ravikumar et al. (2022); Mishra and Metilda (2015); Chalissery et al. (2023)	Publisher-record checks and separate correct decisions for genuine and deceptive apps
Q3. Can an immediate reminder help?	Friestad and Wright (1994); Burke et al. (2022); Kaiser et al. (2022)	Randomised prompt contrasts on valid checks, correct identification and false rejection

Note. Supporting studies provide related evidence, not previously observed results for the proposed trading-app experiment. Source: Authors' conceptual synthesis.

3. Results of the Conceptual Analysis

The outcome of the present analysis is a set of proposed relationships, not an empirical results table. No respondents have been recruited and no hypothesis has been tested. The propositions below are organised by the three research questions so that later statistical results would have a stated purpose and interpretation.

3.1 Displayed cues and perceived legitimacy

The first research question arises because a visual symbol can affect perceived legitimacy before an investor checks its origin. Online assurance studies support the general possibility that a trust mark influences initial impressions (Hu et al., 2010), while research on misunderstood trust seals warns against assuming that the displayed symbol communicates its meaning correctly (Kirlappos et al., 2012). The possibility is especially relevant when an investor receives a promotional screenshot that resembles a verified listing but is not itself part of an authenticated marketplace. This does not imply that the official SEBI-backed marketplace label is misleading. It implies that the evidential value of a symbol depends on the context in which it can be verified. The first proposition therefore concerns belief; the second concerns the resulting classification error under an unverified delivery route.

H1. A displayed verification cue increases perceived legitimacy when other visible app information is held constant.

H2. A displayed cue produces a larger increase in mistaken acceptance of deceptive apps when an offer is received through an unverified source than when it is viewed in an authenticatable marketplace context.

3.2 Provenance, checking and correct authentication

The second question concerns the movement from a favourable impression to justified identification. Financial literacy may help users understand why source information matters, but a score on financial knowledge is not the source record itself (Lusardi & Mitchell, 2014; Ravikumar et al., 2022). The difference is reinforced by findings on subjective confidence and behavioural bias (Lind et al., 2020; Mishra & Metilda, 2015; Kumar & Goyal, 2016). Provenance is an opportunity to inspect an external record; verification behaviour is the action of consulting it. A person can have access to reliable records yet decide not to use them. Conversely, an active check may fail if it relies only on a promoter-controlled document. These separate steps allow the proposed study to test what information is available and whether it is actually used. Kelley et al. (2023) offer related evidence that reasoning can help distinguish genuine from fake websites, while Isaia et al. (2024) show why overconfidence can matter for online-fraud outcomes. Neither finding determines the result for Indian trading apps. The model instead specifies a chain that later evidence may support or reject: available source information, an independent checking action and the correctness of the app decision.

H3. Availability of independently checkable source provenance increases correct authentication of both genuine and deceptive trading apps.

H4. Observed independent verification behaviour is positively associated with correct app authentication after accounting for assigned experimental conditions and respondent characteristics.

3.3 Source-check prompt and balanced fraud resistance

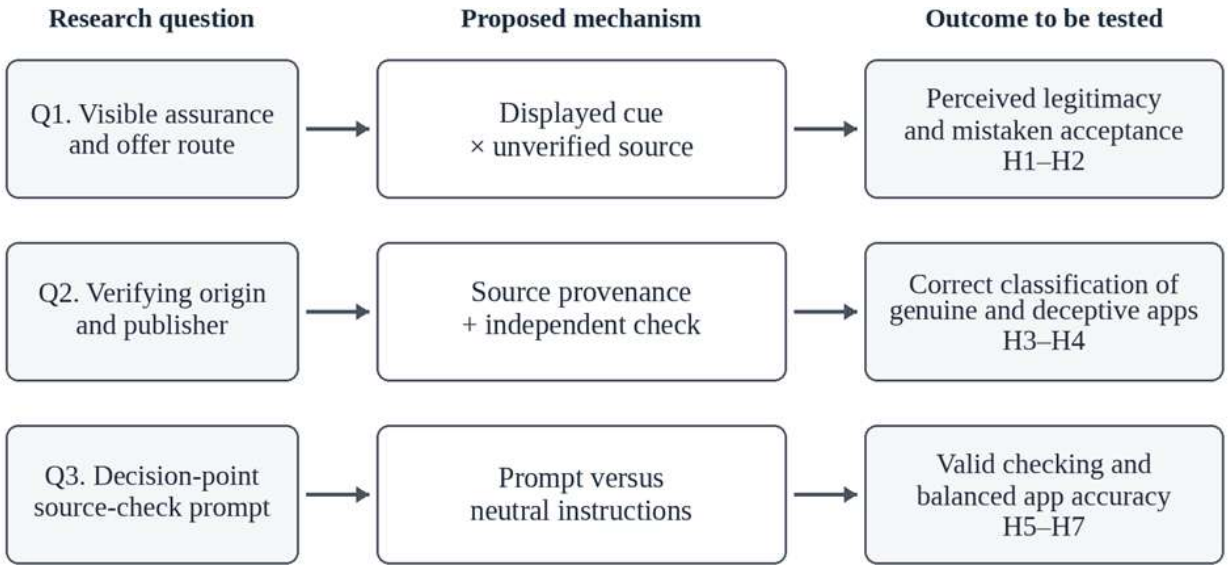
The third question concerns an actionable intervention rather than a broad investor-awareness campaign. Friestad and Wright (1994) described how people can recognise and respond to persuasion attempts. Fraud-education research has found benefits from some brief interventions, although their effects should not be assumed to last indefinitely (Burke et al., 2022). Kaiser et al. (2022) provided broader evidence that financial education can influence subsequent behaviour. These findings justify examining a narrowly designed reminder, not claiming that this particular reminder has already worked. The proposed text would ask users to examine the publisher, official intermediary listing and distribution route before trusting the image of a badge. Its effect must be evaluated against both kinds of error: accepting a deceptive application and rejecting a legitimate one.

H5. Assignment to a short source-check prompt increases the frequency of valid independent verification actions.

H6. Assignment to the prompt increases correct authentication of deceptive and genuine apps without increasing wrongful rejection of genuine apps.

H7. The prompt weakens the positive effect of displayed verification cues on mistaken acceptance of deceptive apps.

Figure 1. Proposed links between research objectives, source evidence and authentication outcomes



Note. Arrows show proposed relationships; H4 is observational rather than randomly assigned. H1–H7 are untested hypotheses, not estimated coefficients. Source: Authors' conceptual synthesis.

4. Discussion

4.1 What the framework adds to investor-trust research

The conceptual findings clarify three closely related decisions. First, a visible mark may produce confidence before there is sufficient evidence of origin. Existing work on assurance symbols helps explain this first impression, but it does not license the conclusion that every displayed verified label is untrustworthy. The source setting matters: a badge attached to a genuine app listing is an institutional authentication feature, while an image of a badge in a forwarded message is only a representation of one. Treating these encounters separately avoids a contradiction between the value of legitimate security labels and their possible imitation. The contribution to trust-signal theory is therefore the proposed boundary between a signal embedded in its authentic source and a visually similar signal detached from that source.

Second, the paper separates knowledge, confidence, verification action and decision accuracy. The Chapter 2 literature demonstrates why this separation is warranted. Financial literacy is relevant to participation and planning (van Rooij et al., 2011; Agarwalla et al., 2015), but experience and confidence can coexist with bias (Mishra & Metilda, 2015; Chalissery et al., 2023). Digital financial literacy covers more than everyday app use (Ravikumar et al., 2022). The new research question is whether an investor takes the further step of using an independent publisher record and identifies the app correctly. Recording actual checks is more informative for this question than asking only whether participants say they are careful investors. This does not dismiss financial education; it identifies the precise behaviour that education may need to produce.

Third, fraud resistance must include genuine-app recognition. If a warning simply increases refusal of all offers, users may avoid some scams but also reject authorised services. Such an outcome does not demonstrate a better ability to distinguish sources. The proposed design therefore assesses correct rejection, correct acceptance, false acceptance and false rejection separately. This distinction is particularly important for a public regulator that aims both to prevent impersonation and to support safe use of legitimate markets. The intervention hypothesis is deliberately conditional: a reminder is valuable only if it improves evidence-based choices without shifting all responses towards refusal.

4.2 Practical implications and limits of inference

For brokers, marketplaces and investor-education providers, the model suggests a narrowly specified message: check the publisher and official app listing rather than trusting a screenshot of a label. Consistent links on an intermediary's official site could make this task simpler. SEBI's 2026 verified-label initiative creates a specific setting in which to test whether users understand where a platform-generated label is meaningful (SEBI, 2026). The proposed experiment

could also show whether source records remain confusing even after a reminder, suggesting that clear publisher information is as important as warnings. These are potential design implications, not evaluated policy outcomes.

Several limits remain. The literature used here was selected for conceptual relevance; this manuscript does not claim an exhaustive search of all fraud-detection studies. The source chapter addressed general financial awareness and investment decisions, so its findings should not be treated as direct evidence of responses to counterfeit app listings. An experiment using mock offers cannot fully recreate emotional pressure, financial consequences, persuasion by acquaintances or repeated contact by scammers. A convenience sample would limit generalisation. A brief source check may also work only when reliable reference information can be found and understood. Future evidence would be needed on retention after a delay, vulnerable user groups, different languages and actual journeys across app stores and broker sites. A short laboratory task cannot estimate how many people have been defrauded or how much money a particular warning would save. Because the verified label is tied to a defined marketplace setting, later trials must also assess whether users distinguish an official label displayed by the platform from an image reproduced elsewhere. This boundary is central to the study, not an incidental design detail.

5. Conclusions

This paper addresses a specific investor-protection problem: a trading app may look verified even when the evidence of its publisher has not been checked. For the first research question, prior research supports the possibility that visible assurance affects perceived legitimacy; the proposed model tests whether that effect becomes unsafe when a badge is detached from an authentic source. It does not claim that verified marketplace labels themselves are deceptive. For the second question, the paper identifies independently checkable provenance and observed checking as distinct requirements for evaluating correct authentication. Financial knowledge and confidence may influence behaviour, but neither replaces confirmation of the app's origin. For the third question, the paper proposes a short reminder and specifies how to test whether it increases valid checking and improves classification without unnecessary refusal of genuine services.

The main contribution is a conceptual framework that links an investor's impression to the evidence used and the decision made. Its hypotheses and proposed experiment can be tested, but no effects or prevalence rates are reported here. Investor protection would be better assessed by the ability to distinguish genuine apps from deceptive copies than by trust ratings or fear of investment alone. The paper therefore places independent source authentication at the centre of future research on trading-app fraud resistance.

References

Agarwalla, S. K., Barua, S. K., Jacob, J., & Varma, J. R. (2015). Financial literacy among working young in urban India. World Development, 67, 101–109. https://doi.org/10.1016/j.worlddev.2014.10.004

Burke, J., Kieffer, C., Mottola, G., & Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud? Journal of Economic Behavior & Organization, 198, 250–266. https://doi.org/10.1016/j.jebo.2022.03.028

Chalissery, N., Tabash, M. I., Nishad, T. M., Aburezeq, I. M., & Daniel, L. N. (2023). Does the investor's trading experience reduce susceptibility to heuristic-driven biases? The moderating role of personality traits. Journal of Risk and Financial Management, 16(7), 325. https://doi.org/10.3390/jrfm16070325

Chandani, A., Sanghvi, M., Wagholikar, S., Pathak, M., Bagade, S., Ubarhande, P., & Saini, U. (2025). Extending the technology acceptance model (TAM): Factors influencing behavioural intentions of investors to use the advice of finfluencers. Journal of Behavioral and Experimental Finance, 47, 101092. https://doi.org/10.1016/j.jbef.2025.101092

Friestad, M., & Wright, P. (1994). The persuasion knowledge model: How people cope with persuasion attempts. Journal of Consumer Research, 21(1), 1–31. https://doi.org/10.1086/209380

Hu, X., Wu, G., Wu, Y., & Zhang, H. (2010). The effects of Web assurance seals on consumers' initial trust in an online vendor: A functional perspective. Decision Support Systems, 48(2), 407–418. https://doi.org/10.1016/j.dss.2009.10.004

Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? Journal of Behavioral and Experimental Finance, 44, 100977. https://doi.org/10.1016/j.jbef.2024.100977

Kaiser, T., Lusardi, A., Menkhoff, L., & Urban, C. (2022). Financial education affects financial knowledge and downstream behaviors. Journal of Financial Economics, 145(2), 255–272. https://doi.org/10.1016/j.jfineco.2021.09.022

Kawamura, K., Mori, Y., Motonishi, T., & Ogawa, K. (2021). Is financial literacy dangerous? Financial literacy, behavioral factors, and financial choices of households. Journal of the Japanese and International Economies, 59, 101131. https://doi.org/10.1016/j.jjie.2021.101131

Kelley, N. J., Hurley-Wallace, A. L., Warner, K. L., & Hanoch, Y. (2023). Analytical reasoning reduces internet fraud susceptibility. Computers in Human Behavior, 142, 107648. https://doi.org/10.1016/j.chb.2022.107648

Kirlappos, I., Sasse, M. A., & Harvey, N. (2012). Why trust seals don't work: A study of user perceptions and behavior. In S. Katzenbeisser et al. (Eds.), Trust and trustworthy computing (pp. 308–324). Springer. https://doi.org/10.1007/978-3-642-30921-2_18

Kumar, S., & Goyal, N. (2016). Evidence on rationality and behavioural biases in investment decision making. Qualitative Research in Financial Markets, 8(4), 270–287. https://doi.org/10.1108/QRFM-05-2016-0016

Lind, T., Ahmed, A., Skagerlund, K., Strömbäck, C., Västfjäll, D., & Tinghög, G. (2020). Competence, confidence, and gender: The role of objective and subjective financial knowledge in household finance. Journal of Family and Economic Issues, 41, 626–638. https://doi.org/10.1007/s10834-020-09678-9

Lusardi, A., & Mitchell, O. S. (2014). The economic importance of financial literacy: Theory and evidence. Journal of Economic Literature, 52(1), 5–44. https://doi.org/10.1257/jel.52.1.5

Mishra, K. C., & Metilda, M. J. (2015). A study on the impact of investment experience, gender, and level of education on overconfidence and self-attribution bias. IIMB Management Review, 27(4), 228–239. https://doi.org/10.1016/j.iimb.2015.09.001

Potrich, A. C. G., Vieira, K. M., & Mendes-Da-Silva, W. (2016). Development of a financial literacy model for university students. Management Research Review, 39(3), 356–376. https://doi.org/10.1108/MRR-06-2014-0143

Ravikumar, T., Suresha, B., Prakash, N., Vazirani, K., & Krishna, T. A. (2022). Digital financial literacy among adults in India: Measurement and validation. Cogent Economics & Finance, 10(1), 2132631. https://doi.org/10.1080/23322039.2022.2132631

Securities and Exchange Board of India. (2025, May 21). Caution to investors on stock market scams through social media platforms. https://www.sebi.gov.in/media-and-notifications/press-releases/may-2025/caution-to-investors-on-stock-market-scams-through-social-media-platforms_94064.html

Securities and Exchange Board of India. (2026, March 25). Chairman, SEBI today launched an important investor protection measure in the form of verified label for stock trading apps of brokers registered with SEBI, on Google Play Store (Press release No. 20/2026). https://www.sebi.gov.in/media-and-notifications/press-releases/mar-2026/chairman-sebi-today-launched-an-important-investor-protection-measure-in-the-form-of-verified-label-for-stock-trading-apps-of-brokers-registered-with-sebi-on-google-play-store_100616.html

van Rooij, M., Lusardi, A., & Alessie, R. (2011). Financial literacy and stock market participation. Journal of Financial Economics, 101(2), 449–472. https://doi.org/10.1016/j.jfineco.2011.03.006