

Digital Financial Literacy and Vulnerability to Online Financial Fraud Among Working Women in Delhi-NCR: The Mediating Role of Protective Financial Behavior and Financial Confidence

Dr. Priyanka Daya Choudhary¹ | Ms. Asmita T² | Dr. L R. Paliwal^{3*}

¹ Assistant Professor, Pacific Academy of Higher Education & Research University, Udaipur.

² Research Scholar, Department of Commerce and Management, Pacific Academy of Higher Education and Research, Udaipur

³ Assistant Professor, Swami Shraddhanand College, University of Delhi

*Corresponding Author: lrpaliwal@ss.du.ac.in

Citation: Choudhary, P., Asmita, T. & Paliwal, L. (2026). Digital Financial Literacy and Vulnerability to Online Financial Fraud Among Working Women in Delhi-NCR: The Mediating Role of Protective Financial Behavior and Financial Confidence. International Journal of Global Research Innovations & Technology, 04(02(II)), 110–120. [https://doi.org/10.62823/IJGRIT/4.2\(II\).9144](https://doi.org/10.62823/IJGRIT/4.2(II).9144)

ABSTRACT

India has witnessed an unprecedented transformation in its financial ecosystem through the widespread adoption of digital payment systems, mobile banking, the Unified Payments Interface (UPI), internet banking, and digital wallets. While these innovations have enhanced financial inclusion and transactional efficiency, they have simultaneously increased individuals' exposure to sophisticated online financial fraud, including phishing, vishing, identity theft, QR-code scams, fake investment schemes, and social engineering attacks. This growing dependence on digital finance has shifted financial literacy beyond traditional budgeting, saving, and investing towards the ability to recognise digital risks, evaluate online financial information, and adopt secure financial practices.

Working women represent a particularly important demographic in this evolving landscape. Rising workforce participation, increasing financial independence, and greater reliance on digital services have expanded both their opportunities and their exposure to cyber-enabled risks. Despite improvements in inclusion, evidence suggests women often exhibit lower financial confidence, greater risk aversion, and varying digital competence, which may influence their susceptibility to fraud. Existing studies examine financial literacy in relation to savings, investment behaviour, or financial well-being, while limited attention has been paid to the behavioural mechanisms through which digital financial literacy contributes to fraud protection.

Drawing on the Theory of Planned Behaviour and Protection Motivation Theory, this study conceptualizes Digital Financial Literacy as the primary predictor of Online Fraud Vulnerability, with Protective Financial Behaviour as a mediating variable and Financial Confidence as an important psychological determinant. It proposes a cross-sectional survey of working women actively using digital financial services in Delhi-NCR, with data analyzed through Structural Equation Modelling (SEM) using SPSS and AMOS. The study extends the literature by reconceptualizing digital financial literacy to encompass not only financial knowledge and digital competence but also fraud detection and cyber-risk awareness, offering practical implications for policymakers, financial institutions, employers, and regulators seeking to strengthen women's digital financial resilience.

Keywords: Digital Financial Literacy, Online Financial Fraud, Working Women, Protective Financial Behaviour, Financial Confidence, Behavioural Finance, Financial Inclusion, Structural Equation Modelling.

Introduction

The digital transformation of financial services has reshaped how individuals access, manage, and use financial products worldwide. Advances in financial technology (FinTech), together with rising internet penetration and smartphone access, have accelerated the adoption of digital financial services, making transactions faster, more convenient, and more inclusive. In India, this transformation gained momentum through initiatives such as Digital India, Jan Dhan Yojana, Aadhaar-enabled services, and the Unified Payments Interface (UPI), which collectively reduced barriers to financial access while promoting cashless transactions across urban and semi-urban populations.

According to the National Payments Corporation of India (NPCI), UPI has become one of the world's fastest-growing digital payment systems, processing billions of transactions monthly. Mobile banking, internet banking, digital wallets, and investment applications have become integral to consumers' daily financial activities, extending beyond routine payments to savings, insurance, investments, lending, taxation, and wealth management, thereby increasing the complexity of financial decision-making.

However, this rapid expansion has generated new vulnerabilities. The growing sophistication of cybercriminals has produced a sharp rise in online fraud involving phishing emails, fraudulent links, fake customer-care services, QR-code manipulation, identity theft, SIM swapping, malware, remote-access applications, fake investment platforms, and social engineering. Unlike traditional fraud, digital fraud often exploits behavioural biases, cognitive limitations, and inadequate cyber-security awareness rather than technological weaknesses alone. Consequently, users possessing basic financial knowledge may still become victims if they fail to recognise deceptive practices or neglect security precautions.

This landscape has broadened the meaning of financial literacy. Traditionally, it referred to understanding budgeting, inflation, compound interest, risk diversification, savings, and investment planning. While these remain essential, they are no longer sufficient in a digitally connected economy. Contemporary financial capability increasingly requires individuals to evaluate the authenticity of digital platforms, understand cyber-security practices, safeguard credentials, identify fraudulent communications, and make informed decisions within technology-enabled environments. Accordingly, digital financial literacy has emerged as an extension of traditional financial literacy, integrating financial knowledge with digital competence, cyber-risk awareness, and secure behaviour.

Among the groups participating in India's digital economy, working women constitute an especially significant population. Increasing educational attainment, higher labor-force participation, rising incomes, and greater financial autonomy have encouraged women to adopt digital services for salary management, household expenditure, investment, insurance, and personal financial planning. Yet the expansion of access has not necessarily been matched by proportional improvements in digital capability or cyber-security preparedness.

Prior research consistently highlights gender differences in financial literacy, investment confidence, and decision-making. Women report lower financial confidence than men despite demonstrating comparable abilities when given adequate information. They also tend to exhibit greater caution and lower risk tolerance, characteristics that may either reduce or increase vulnerability depending on the nature of the fraud. Excessive trust in perceived authority, inadequate verification, limited awareness of emerging techniques, or conversely overconfidence in one's digital abilities may each contribute to different forms of susceptibility. Understanding these behavioural mechanisms among working women is therefore an important research priority.

Existing literature has examined financial literacy in relation to inclusion, investment decisions, retirement planning, savings, or well-being. Fewer studies investigate how digital financial literacy influences the ability to recognise and resist fraud, and fewer still explore the behavioural processes through which knowledge translates into protective action. Possessing knowledge does not guarantee secure behaviour; similarly, high usage of digital services does not imply adequate fraud resistance. The distinction between digital adoption and digital safety remains insufficiently explored, particularly in India.

A further gap concerns financial confidence. While appropriate confidence encourages informed participation and independent decision-making, excessive confidence can reduce vigilance, encourage heuristic decision-making, and increase susceptibility to sophisticated schemes. Conversely, insufficient confidence may discourage independent evaluation and increase reliance on misleading advice. Whether financial confidence serves as a protective factor or a source of vulnerability remains unresolved.

This study addresses these gaps by proposing an integrated conceptual model linking Digital Financial Literacy, Protective Financial Behaviour, Financial Confidence, and Online Fraud Vulnerability among working women in Delhi-NCR. Drawing on the Theory of Planned Behaviour and Protection Motivation Theory, it argues that digital financial literacy enhances protective behaviour by strengthening perceived behavioural control, threat appraisal, and coping mechanisms; protective behaviour, in turn, reduces fraud vulnerability. Financial confidence is examined as a psychological determinant that may either strengthen protective behaviour or contribute to vulnerability depending on how accurately it reflects actual competence. By shifting focus from financial participation to financial resilience, the study offers insights for policymakers, regulators, financial institutions, employers, and educational organizations designing evidence-based programmes that improve digital safety alongside inclusion.

Literature Review

Digital Financial Literacy: Concept and Evolution

Financial literacy has traditionally been defined as the knowledge and capability required to make informed decisions regarding saving, borrowing, investing, and wealth management. The rapid digitalization of financial services has expanded this concept to include the competencies necessary to safely access, evaluate, and use digital products. The emergence of internet banking, mobile payments, digital wallets, FinTech applications, and AI-driven services has altered consumers' interaction with financial systems, leading scholars and policymakers to emphasize digital financial literacy (DFL) as a multidimensional construct combining financial knowledge with digital competence, cyber-security awareness, and responsible behaviour.

The OECD has been instrumental in formalizing this perspective. The OECD/INFE Survey Instrument to Measure Digital Financial Literacy (2024) defines DFL as the combination of knowledge, skills, attitudes, and behaviours enabling individuals to use digital financial services safely and effectively while protecting their financial well-being. Unlike traditional measures, the framework incorporates cyber-security practices, online authentication, fraud recognition, privacy protection, and informed use of digital technologies.

Similarly, the OECD/INFE 2023 International Survey of Adult Financial Literacy demonstrated that DFL remains inadequate across many economies despite widespread adoption of digital payments. A substantial proportion of adults continue to lack the minimum competencies to recognise digital risks, verify online information, and maintain secure practices; those with higher DFL consistently reported greater financial resilience and safer online behaviour.

Within India, the penetration of UPI, digital banking, and mobile-based services has made DFL a critical component of inclusion. Mishra, Agarwal, Sharahiley, and Kandpal (2024), in an empirical study of Indian women, argued that DFL significantly enhances decision-making by strengthening users' ability to evaluate products, understand risks, and confidently participate in technology-enabled markets, and that digital competence contributes directly to women's empowerment and economic participation. Collectively, these studies suggest DFL extends well beyond operational knowledge of payment applications to encompass the ability to critically evaluate information, recognise fraudulent communications, protect credentials, and make secure decisions in complex digital environments.

Online Financial Fraud in the Digital Economy

The growth of digital services has been accompanied by a rapid increase in cyber-enabled financial crimes. Fraudsters increasingly exploit behavioural vulnerabilities rather than technological weaknesses through phishing, vishing, fake customer-care services, QR-code manipulation, identity theft, remote-access applications, investment scams, and social engineering.

The OECD (2026) identifies the accelerating pace of digitalization, low levels of DFL, and increasingly sophisticated scam techniques as principal drivers of financial fraud worldwide. It argues that while innovation has improved accessibility, it has created an environment in which consumers must make complex security decisions without adequate preparation. Fraud prevention therefore requires not only stronger technological safeguards but also improvements in behavioural capability and digital awareness. Evidence from India reflects similar concerns: government data indicate a substantial increase in digital payment fraud alongside the growth of online transactions, exposing consumers to scams that exploit limited cyber-awareness. Recent reviews of cyber-security threats in the FinTech ecosystem similarly conclude that human behaviour remains one of the weakest links; users frequently compromise their own safety through weak authentication, inadequate password management, or misplaced trust, reinforcing that behavioural capability is central to digital financial security.

Digital Financial Literacy and Fraud Vulnerability

An important stream of research investigates whether higher financial literacy reduces susceptibility to online fraud. Although traditional literacy has consistently been associated with improved decision-making, few studies have examined its relationship with fraud victimization in digital settings.

The most comprehensive investigation is Isaia, Oggero, and Sandretto (2024). Using representative Italian data, the authors found that higher objective financial literacy significantly reduced the likelihood of online fraud victimization. More importantly, overconfidence in financial knowledge substantially increased vulnerability: individuals who believed they possessed high competence despite lacking objective knowledge were considerably more likely to become victims. The authors concluded that financial literacy functions as a protective resource only when accompanied by realistic self-assessment and appropriate caution. These findings align with OECD evidence showing that consumers with stronger digital competencies better recognise suspicious communications, verify information, and adopt safer practices, while inadequate DFL increases exposure to phishing, identity theft, and fraudulent schemes. Within India, empirical evidence remains limited, as existing studies primarily examine DFL in relation to inclusion, investment decisions, or payment adoption rather than fraud resistance.

Protective Financial Behaviour as a Behavioural Mechanism

Behavioural theories explain why knowledge alone does not always translate into secure outcomes. The Theory of Planned Behaviour (Ajzen, 1991) proposes that behaviour is influenced by attitudes, subjective norms, and perceived behavioural control; individuals with greater confidence in their ability to perform protective actions are more likely to adopt secure practices. Protection Motivation Theory (Rogers, 1975; Maddux & Rogers, 1983) argues that individuals engage in self-protective behaviour when they perceive threats as serious and believe they can respond effectively. Applied to digital finance, these theories suggest that DFL influences fraud vulnerability indirectly by encouraging protective behaviours such as verifying website authenticity, safeguarding passwords and OTPs, avoiding suspicious hyperlinks, enabling multi-factor authentication, and monitoring accounts. OECD policy reports reinforce this perspective: individuals who practice secure password management, avoid financial transactions over unsecured public Wi-Fi, and verify payment requests exhibit substantially lower exposure to fraud. Protective behaviour thus serves as the practical mechanism through which DFL is translated into fraud resistance.

Financial Confidence and the Risk of Overconfidence

Financial confidence represents an individual's subjective belief in their ability to make effective decisions. Behavioural finance distinguishes between well-calibrated confidence, which facilitates informed decision-making, and overconfidence, which often results in excessive risk-taking and reduced vigilance. Isaia et al. (2024) provide compelling evidence that overconfidence increases the probability of victimization: individuals who overestimated their competence were more likely to ignore warning signs, trust fraudulent communications, and underestimate risks, suggesting subjective confidence may not correspond with objective capability. Research on women indicates that female consumers frequently report lower subjective confidence despite comparable capabilities when given adequate information. Mishra et al. (2024) argue that strengthening DFL improves women's confidence, which enhances decision-making and economic participation. However, whether increased confidence consistently reduces vulnerability or occasionally promotes overconfidence remains largely unexplored, particularly in India.

Digital Financial Literacy among Working Women

Women's increasing participation in formal employment has expanded their engagement with digital services. Salaries, investments, insurance premiums, tax payments, and everyday transactions are increasingly managed through digital platforms, making working women an economically significant segment of India's ecosystem. Despite this, prior research has primarily examined women's financial literacy from the perspectives of inclusion, savings, entrepreneurship, or investment decisions, with little attention to their preparedness to identify and resist fraud. Mishra et al. (2024) suggest DFL positively influences women's decision-making by improving access to information, increasing confidence, and strengthening independence, but focuses on financial decisions rather than fraud prevention, indicating an important opportunity for further investigation.

Research Gap

The review reveals several gaps. First, a conceptual gap exists because most studies measure DFL in terms of digital adoption or usage rather than the capability to recognise, evaluate, and resist

fraud. Second, a behavioural gap remains: few empirical studies investigate the mediating role of protective financial behaviour in translating knowledge into fraud resistance. Third, a psychological gap persists regarding financial confidence, which may function as both a protective factor and a source of vulnerability through overconfidence. Fourth, a population gap exists, as research on professionally employed women using digital services remains scarce. Finally, a methodological gap is evident, since few studies have employed SEM to simultaneously examine the direct and indirect relationships among DFL, protective behaviour, confidence, and fraud vulnerability. Addressing these gaps, the present study proposes an integrated behavioural model grounded in the Theory of Planned Behaviour and Protection Motivation Theory.

Digital Financial Landscape in India: Opportunities and Emerging Risks

India's Digital Financial Revolution

India has emerged as one of the world's leading digital economies, driven by FinTech advances, smartphone adoption, affordable internet, and proactive government initiatives. Over the past decade, the ecosystem has shifted from cash-dominated transactions to a digital infrastructure facilitated by the Digital India Programme, Pradhan Mantri Jan Dhan Yojana (PMJDY), Aadhaar-enabled services, and UPI, collectively creating a robust Digital Public Infrastructure that has enhanced access to formal financial services.

The launch of UPI in 2016 by NPCI marked a defining moment, enabling seamless real-time transfers through mobile devices and eliminating many barriers to conventional banking. Its ease of use, interoperability, and minimal cost drove unprecedented adoption growth. According to the Reserve Bank of India (2024), digital payment volumes have increased exponentially, with UPI accounting for a substantial share of retail electronic transactions. Mobile banking, internet banking, digital wallets, QR-code payments, and contactless systems have become integral to everyday activity.

This expansion has produced significant benefits: improved inclusion for underserved populations, reduced transaction costs, enhanced transparency, cashless commerce, and direct benefit transfers under welfare programmes. The rapid growth of the FinTech sector has introduced digital lending, robo-advisory services, online investment platforms, peer-to-peer lending, and digital insurance, embedding financial services deeply in consumers' daily lives. Women have emerged as important beneficiaries, adopting digital services for salary management, household expenditure, investment, insurance, tax payments, and retirement planning, supported by initiatives promoting women's inclusion.

Despite these achievements, digital inclusion does not necessarily imply digital capability. Many individuals possess limited understanding of cyber-security, fraud detection, and safe online behaviour. The ease of transacting has often outpaced users' ability to identify fraud or protect themselves, meaning the transformation has simultaneously created new opportunities and new vulnerabilities.

The Growing Threat of Online Financial Fraud

The growth of digital services has been accompanied by a parallel increase in fraud. As transactions become more frequent and sophisticated, cybercriminals have adapted to exploit behavioural tendencies, technological unfamiliarity, and information asymmetry, relying increasingly on psychological manipulation and social engineering rather than physical theft or system breaches.

Online fraud encompasses deceptive activities intended to obtain unauthorized access to financial information, credentials, or assets. Common forms include phishing, vishing, smishing, QR-code scams, fake KYC verification requests, fraudulent customer support, impersonation of institutions, remote-access scams, identity theft, fake investment platforms, cryptocurrency fraud, and employment-related scams. Artificial intelligence has enabled deep-fake audio and video, making fraudulent communications harder to detect. A defining characteristic is reliance on behavioural manipulation: fraudsters exploit fear, urgency, trust, curiosity, and greed to pressure victims into sharing OTPs, clicking malicious links, scanning fraudulent QR codes, downloading remote-access software, or transferring funds, often bypassing technological safeguards by targeting human judgement.

India has experienced a substantial increase in cyber-enabled fraud. Reports from the RBI, Ministry of Home Affairs, National Crime Records Bureau, and Indian Cyber Crime Coordination Centre indicate rising complaints related to payment fraud, identity theft, unauthorized transfers, and investment scams. The human element remains one of the most vulnerable components of the ecosystem. Consequences extend beyond monetary loss to psychological distress, diminished trust, reduced willingness to adopt digital services, and prolonged insecurity, undermining broader inclusion objectives and making fraud prevention a shared responsibility.

Working Women in India's Digital Financial Ecosystem

Working women represent one of the fastest-growing user groups. Rising labour-force participation, educational attainment, access to banking, and financial independence have encouraged active engagement with digital systems for wages, household expenses, investments, insurance, taxes, and routine transactions. The integration of digital services has generated benefits: convenience, reduced dependence on cash, independent decision-making, and enhanced access to formal products, offering flexibility valuable to women balancing professional and household responsibilities.

However, greater participation increases exposure to risk. Working women frequently transact under time constraints, multitask across responsibilities, and rely on mobile devices, circumstances that may increase susceptibility to communications demanding immediate responses or exploiting urgency. Varying levels of digital confidence and cyber-security awareness influence how women evaluate suspicious requests. Research shows women report lower subjective confidence despite comparable capabilities; while caution may reduce some risk-taking, limited confidence may discourage independent verification, whereas excessive confidence may reduce vigilance. These contrasting tendencies highlight the need to examine not only knowledge but also the behavioural and psychological dimensions influencing vulnerability.

Behavioural Perspectives on Fraud Vulnerability

The sophistication of online fraud has shifted attention from technological security towards behavioural vulnerability. Contemporary fraud rarely succeeds through infrastructure weaknesses alone; it exploits predictable patterns of human decision-making. Behavioural finance and consumer psychology therefore help explain why individuals with similar knowledge exhibit different responses.

Several biases contribute to susceptibility. Authority bias encourages trust in communications appearing to originate from banks, government, or law enforcement. Urgency bias prompts action without verification when fraudsters claim accounts will be blocked. Social proof increases trust when messages falsely suggest others have complied. Loss aversion motivates individuals to avoid perceived losses even when doing so requires unnecessary risk. Overconfidence bias leads experienced users to underestimate risks, while confirmation bias encourages acceptance of information consistent with existing beliefs. These tendencies demonstrate that vulnerability cannot be explained by technological competence or traditional literacy alone; effective prevention requires an integrated understanding of knowledge, digital skills, behavioural decision-making, confidence, and protective practices.

Digital Financial Literacy as a Protective Mechanism

The expansion of digital services has transformed inclusion from a question of access to one of capability. While platforms have enabled millions to participate in the formal system, their increasing use has created new risks, making the ability to safely navigate digital environments an essential life skill. This has expanded financial literacy beyond knowledge to include digital competence, cyber-risk awareness, and the behavioural ability to protect oneself. Existing literature has examined DFL as a determinant of inclusion, payment adoption, investment participation, and well-being, with little attention to how it translates into actual protection. This paper argues DFL should be viewed not merely as knowledge acquisition but as a dynamic capability enabling individuals to recognise threats, evaluate information critically, and adopt protective behaviours—a behavioural resource strengthening resilience.

Understanding Digital Financial Literacy

DFL extends beyond familiarity with applications to encompass the knowledge, skills, attitudes, and behaviours required to access, evaluate, use, and protect digital services responsibly. Building on the OECD/INFE framework, this study proposes five interrelated dimensions.

Financial Knowledge refers to understanding basic concepts such as budgeting, interest rates, inflation, savings, investments, insurance, and risk diversification. Individuals with stronger knowledge are better equipped to recognise the unrealistic promises that characterize fraudulent schemes. Digital Competence reflects the technical ability to operate platforms effectively, including navigating banking applications and payment interfaces and using authentication procedures such as biometric verification, two-factor authentication, and secure passwords. Cyber-security Awareness represents the ability to recognise threats and understand safe practices, including identifying phishing, fraudulent websites, suspicious hyperlinks, fake QR codes, and impersonation attempts. Critical Evaluation Skills enable consumers to verify sources, assess credibility, distinguish legitimate opportunities from fraud, and avoid impulsive decisions based on misinformation encountered through social media, advertisements, and applications. Responsible Financial Behaviour translates knowledge into consistent practice—

safeguarding passwords and OTPs, updating software, monitoring statements, avoiding unsecured connections, and reporting suspicious activity. Together, these dimensions suggest DFL should be viewed as a holistic capability integrating cognitive understanding with practical behavioural competence.

Protective Financial Behaviour: Translating Knowledge into Action

A central argument is that knowledge does not automatically produce safe behaviour. Individuals may understand cyber-security principles yet engage in risky practices because of convenience, habit, time pressure, misplaced trust, or biases. The effectiveness of DFL therefore depends on whether individuals consistently implement protective behaviours—verifying payment requests, refusing to disclose credentials, enabling multi-factor authentication, creating strong passwords, updating applications, avoiding unknown hyperlinks, and confirming suspicious communications through official channels.

Protection Motivation Theory explains this relationship: individuals adopt protective behaviour when they perceive both the seriousness of a threat and their ability to respond. Consumers with higher DFL are more likely to recognise threats, understand consequences, and believe preventive actions reduce risk. The Theory of Planned Behaviour similarly suggests protective behaviour is influenced by attitudes towards security, perceived behavioural control, and subjective norms. Protective behaviour thus represents the behavioural pathway through which DFL contributes to resilience.

Financial Confidence: A Double-Edged Psychological Construct

Financial confidence represents an individual's subjective belief regarding their ability to make effective decisions. It encourages independent decision-making, increases willingness to participate in markets, and reduces dependence on informal advice—but is beneficial only when it accurately reflects competence. Well-calibrated confidence enables individuals to evaluate information carefully, question suspicious requests, verify transactions, and implement protective practices consistently. In contrast, excessive confidence may increase vulnerability: individuals who overestimate their competence may underestimate risks, ignore warnings, bypass security procedures, or assume fraud is unlikely to affect them, and fraudsters frequently exploit this by presenting credible-seeming scams. Conversely, insufficient confidence may also increase vulnerability, as individuals may hesitate to question requests or rely excessively on external advice. Effective decision-making therefore requires confidence appropriately aligned with objective capability. This paper conceptualises financial confidence as a psychological factor capable of either strengthening or weakening resilience depending on that alignment.

A Conceptual Framework for Fraud Vulnerability Among Working Women

The framework positions Digital Financial Literacy (DFL) as the foundational cognitive capability influencing behavioural and psychological responses to risk. Individuals with higher DFL are expected to exhibit stronger cyber-security awareness, better critical evaluation, and greater understanding of secure practices. These competencies are translated into practical security through Protective Financial Behaviour (PFB), the primary behavioural mechanism reducing exposure—recognizing that behavioural implementation, not knowledge alone, is essential. Financial Confidence (FC) is incorporated as an independent psychological construct influencing both protective behaviour and vulnerability; well-calibrated confidence encourages informed decision-making, whereas overconfidence may reduce vigilance. Finally, Online Fraud Vulnerability (OFV) represents the outcome of the interaction among knowledge, behaviour, and psychological factors, conceptualized not merely as previous victimization but as overall susceptibility to deceptive communications and unsafe practices.

The framework can be represented as:

Digital Financial Literacy (DFL) → Protective Financial Behaviour (PFB) → Online Fraud Vulnerability (OFV)

With Financial Confidence (FC) influencing both PFB and OFV, recognizing that confidence may operate as either a protective resource or a behavioural risk depending on calibration.

An Integrated Behavioural Perspective

Online fraud cannot be adequately explained through technological or financial variables alone; vulnerability emerges from the interaction of cognitive capability, behavioural practices, and psychological characteristics. DFL provides the knowledge to recognise risks; protective behaviour operationalizes this into everyday practice; and confidence shapes how individuals interpret information, assess risk, and respond. For working women, these relationships assume particular significance given

their expanding participation. Strengthening DFL must therefore extend beyond improving knowledge to fostering secure behavioural habits and appropriately calibrated confidence, offering a foundation for empirical investigation using behavioural finance models and SEM.

Policy Implications and Recommendations

The expansion of India's digital ecosystem has created opportunities for inclusion and empowerment, but the parallel rise in fraud demands a comprehensive approach to digital capability. DFL should be viewed not merely as an education objective but as a critical component of consumer protection and cyber resilience, requiring coordinated efforts from policymakers, institutions, employers, educators, technology providers, and consumers.

Government and Financial Regulators

Regulators such as the RBI, SEBI, NPCI, and the Ministry of Electronics and Information Technology play a pivotal role, but the sophistication of fraud requires a shift from awareness campaigns towards behavioural capability. First, national financial literacy programmes should explicitly integrate DFL, adding modules on phishing detection, QR-code verification, password security, digital identity protection, investment scams, AI-enabled fraud, and secure use of applications. Second, regulators should encourage behavioural nudges within platforms—timely warnings, security reminders, fraud notifications, and verification prompts—to reduce impulsive decisions during high-risk transactions. Third, greater collaboration between regulators, cyber-security agencies, telecommunication providers, and law enforcement is essential for rapid detection and coordinated response. Finally, policymakers should develop gender-responsive strategies recognizing women's unique responsibilities, usage patterns, and behavioural challenges.

Banks and Financial Institutions

As the primary interface between consumers and services, banks should move beyond periodic messages to continuous education through interactive modules, simulated phishing exercises, mobile tutorials, and multilingual content. AI and machine learning should strengthen fraud detection via real-time monitoring, anomaly detection, geolocation verification, and adaptive authentication. Banks should simplify reporting procedures, since victims often delay reporting because of complex mechanisms, and personalize education, recognizing that working women, senior citizens, first-time users, and small business owners face different risks.

Employers and Corporate Organizations

As employers encourage digital salary payments, reimbursement, tax filing, and benefit management, they can enhance employees' capability by incorporating DFL into wellness programmes through workshops on cyber-security, secure payment practices, investment fraud prevention, and identity theft. Collaboration with banks, cyber-security professionals, and educators can provide practical demonstrations of emerging techniques, with special attention to women employees managing both personal and household responsibilities.

Educational Institutions

Universities, colleges, and training institutions should integrate DFL into curricula irrespective of discipline, extending beyond theory to practical competencies such as online banking security, responsible payment use, fraud identification, and safe investment. Experiential approaches—case studies, simulations, role-playing, and awareness campaigns—improve outcomes. Business and management programmes should incorporate behavioural finance perspectives, equipping students to resist sophisticated fraud, supported by collaboration among academia, institutions, FinTech firms, and regulators.

FinTech Companies and Technology Providers

Technological innovation must be accompanied by strong consumer protection. Interface design should prioritize simplicity, transparency, and security, with clear explanations of permissions, authentication, privacy settings, and reporting. Providers should integrate AI-powered fraud alerts that identify suspicious patterns while educating users before transactions are complete. Regular updates, secure encryption, biometric authentication, and adaptive security should remain standard, alongside in-app educational content enabling users to strengthen capability during routine activity.

Working Women

Individuals should regularly update passwords, enable multi-factor authentication, avoid sharing OTPs, verify the authenticity of communications, and avoid transactions over unsecured public Wi-Fi.

Statements and transaction histories should be reviewed periodically to identify unauthorized activity early. Consumers should exercise caution with urgent requests received by call, message, email, or social media, adopting independent verification through official channels before disclosing information. Equally important is balanced confidence—confident enough to make informed decisions while recognising the limits of one's knowledge—supported by continuous learning and awareness of emerging threats.

Towards a Digital Financial Resilience Framework

These recommendations support a transition from digital inclusion towards digital resilience—the capability to anticipate, recognise, respond to, and recover from risks. Building resilience requires an integrated ecosystem in which policymakers establish enabling frameworks, institutions provide secure services, employers promote capability, educators develop lifelong competencies, technology providers prioritize protection, and individuals engage in safe practices. Within this ecosystem, DFL functions as the foundational capability connecting knowledge with behavioural competence and psychological preparedness. Strengthening it among working women can reduce fraud, enhance confidence, promote informed decision-making, and support sustainable inclusion.

Conclusion and Future Research Directions

Conclusion

India's progress towards a digitally empowered economy has transformed how financial services are accessed, delivered, and used. Digital India, UPI, Aadhaar-enabled services, and FinTech have strengthened inclusion by providing convenient, accessible services. Among the major beneficiaries are working women, whose growing participation and independence have driven adoption of digital payments, banking, investments, and technology-enabled products.

However, this expansion has introduced a complex landscape of cyber-enabled risks. Online fraud has evolved from isolated technological intrusion into sophisticated behavioural attacks exploiting trust, urgency, authority, fear, curiosity, and cognitive biases rather than infrastructure weaknesses. Consequently, inclusion without adequate capability may increase vulnerability rather than security.

This study argues that the understanding of financial literacy must evolve beyond traditional knowledge. While knowledge of budgeting, savings, investments, inflation, and interest rates remains essential, it is insufficient for the digital ecosystem. DFL should be recognized as a multidimensional capability integrating financial knowledge, digital competence, cyber-security awareness, critical evaluation, and responsible behaviour. A central contribution is the proposition that DFL protects consumers not directly but through protective financial behaviour: individuals frequently understand risks yet fail to implement protective measures because of biases, convenience, time pressure, misplaced trust, or excessive confidence. Protective behaviour is therefore the mechanism through which DFL translates into resistance.

The paper further highlights the complex role of confidence. Traditionally regarded as desirable, confidence is beneficial only when it reflects capability. Well-calibrated confidence strengthens protective behaviour by increasing self-efficacy, whereas overconfidence reduces vigilance and increases susceptibility. This dual nature suggests education should aim to increase confidence and align it with competence. By focusing on working women—one of the fastest-growing yet underexamined segments—the study addresses an emerging area, demonstrating that women face unique opportunities and challenges arising from increasing autonomy, expanding participation, multiple responsibilities, and evolving threats. The proposed framework integrates DFL, PFB, FC, and OFV into a unified perspective, illustrating how cognitive, behavioural, and psychological factors interact to influence resilience. Its practical implications suggest policymakers should reconsider programmes that emphasize knowledge while neglecting cyber-security and behavioural capability, adopting collaborative approaches that integrate education with protection. Ultimately, the future of inclusion depends not merely on access but on ensuring consumers can use services safely, confidently, and responsibly making DFL a strategic public policy priority.

Limitations of the Study

Several limitations should be acknowledged. First, the study is conceptual and does not include primary empirical data, so the proposed relationships are theoretically derived rather than statistically validated. Second, the discussion is situated within the Indian context, particularly working women in Delhi-NCR; differences in infrastructure, regulation, culture, and inclusion levels may affect applicability elsewhere. Third, the rapidly evolving nature of technology and cybercrime—advances in AI, deepfakes,

and cryptocurrency—presents an inherent limitation, requiring frameworks to remain dynamic. Finally, the interdisciplinary approach, while comprehensive, invites future empirical refinement.

Future Research Directions

The study opens several avenues. First, the framework should be empirically validated using SEM to examine direct and indirect relationships among DFL, PFB, FC, and OFV. Second, longitudinal designs could examine how DFL and protective behaviours evolve as technologies develop. Third, comparative studies across demographic groups—men and women, urban and rural, younger and older, public and private sector, and income levels—would reveal population-specific patterns. Fourth, researchers could investigate the influence of AI, machine learning, biometric authentication, blockchain, and digital identity systems on protection. Fifth, studies should explore additional psychological constructs such as digital trust, perceived risk, technology readiness, self-efficacy, cognitive reflection, financial anxiety, and cyber resilience. Sixth, cross-country comparisons would clarify how regulatory frameworks, culture, digital maturity, and education policies influence resilience. Finally, experimental studies evaluating fraud warnings, nudges, interactive education, simulation-based training, and AI-assisted consumer education would generate valuable evidence for policymakers and institutions.

Concluding Remarks

As economies become increasingly digital, inclusion can no longer be measured solely by accounts opened or transactions completed. True inclusion requires the knowledge, confidence, behavioural capability, and judgement to participate safely. Working women represent one of the most dynamic groups within India's digital economy; strengthening their DFL is an investment in household security, consumer confidence, gender-inclusive development, and national resilience. By shifting focus from adoption to resilience, this study contributes to the discourse on behavioural finance and consumer protection while offering a roadmap for empirical inquiry and evidence-based policymaking. In an era where financial decisions are increasingly mediated by technology, fostering digitally literate, behaviorally informed, and cyber-aware consumers will be indispensable for ensuring the benefits of innovation are realized without compromising safety or trust.

References

1. Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179–211.
2. 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>
3. Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, 19(5), 469–479.
4. Mishra, D., Agarwal, N., Sharahiley, S., & Kandpal, V. (2024). Digital financial literacy and its impact on financial decision-making of women: Evidence from India. *Journal of Risk and Financial Management*, 17(10), 468. <https://doi.org/10.3390/jrfm17100468>
5. Morgan, P. J., & Huang, B. (2019). The need to promote digital financial literacy for the digital age. In *The Future of Work and Education for the Digital Age*. Asian Development Bank Institute (ADB Press).
6. Nogueira, M. C., Almeida, L., & Tavares, F. O. (2025). Financial literacy, financial knowledge, and financial behaviors in OECD countries. *Journal of Risk and Financial Management*, 18(3), 167. <https://doi.org/10.3390/jrfm18030167>
7. OECD. (2018). G20/OECD-INFE policy guidance on digital financial literacy. OECD Publishing. <https://doi.org/10.1787/effe2693-en>
8. OECD. (2021). Digital delivery of financial education: Design and practice. OECD Publishing. <https://doi.org/10.1787/d02549e7-en>
9. OECD. (2021). G20/OECD-INFE report on supporting financial resilience and transformation through digital financial literacy. OECD Publishing.
10. OECD. (2024). OECD/INFE survey instrument to measure digital financial literacy. OECD Publishing. <https://doi.org/10.1787/548de821-en>
11. OECD. (2026). Protecting consumers from financial scams and frauds. OECD Publishing. <https://doi.org/10.1787/d41817bb-en>
12. Ogunola, A. A., Sonubi, T., Toromade, R. O., Ajayi, O. O., & Maduakor, A. H. (2024). The intersection of digital safety and financial literacy: Mitigating financial risks in the digital

- economy. *International Journal of Science and Research Archive*, 13(1), 673–691.
13. Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114.
 14. Tan, E. (2025). Review of research on digital financial literacy: Measurement, causes, and impact. *Journal of Economic Surveys*. Advance online publication. <https://doi.org/10.1111/joes.70109>

