



Strengthening Digital Financial Security Among Salaried Women: A Conceptual Framework for Safe Financial Practices

Harshitaben Dineshbhai Suva*

Research Scholar, Department of Commerce and Management,
Bhakta Kavi Narsinh Mehta University, Junagadh, Gujarat,
INDIA

Dineshkumar R. Chavda

Assistant Professor, Department of Commerce and Management,
Bhakta Kavi Narsinh Mehta University, Junagadh, Gujarat,
INDIA

* Corresponding author:

Harshitaben Dineshbhai Suva, Research Scholar, Department of Commerce and Management, Bhakta Kavi Narsinh Mehta University, Junagadh, Gujarat, India. ✉ Email: harshitasuva2002@gmail.com

Article Info

Article history:

Received: July 4, 2026
Revised: July 22, 2026
Accepted: August 30, 2026

Keywords:

Conceptual Framework
Cyber Fraud
Digital Financial Security
Digital Literacy
Salaried Women

Abstract

ABSTRACT

Background of study: India's rapidly expanding digital financial ecosystem, including UPI, internet banking, mobile banking, and digital wallets, has significantly improved financial inclusion and transaction convenience. However, the increasing use of digital financial services has also exposed salaried women to cyber threats such as phishing, OTP fraud, SIM-swapping, and fraudulent payment applications, making digital financial security awareness an important area of research.

Aims and scope of paper: This paper aims to develop a comprehensive conceptual framework that explains the determinants, mediating mechanisms, and outcomes of digital financial security awareness among salaried women. The study integrates insights from financial literacy, information security, and technology adoption literature to provide a theoretical foundation for future empirical research.

Methods: The study adopts a conceptual research design based exclusively on secondary data. Relevant information has been collected and synthesised from peer-reviewed journal articles, books, government reports, policy documents, and other authentic academic.

Result: The proposed conceptual framework identifies demographic factors, digital literacy, workplace/institutional training, and social influence as antecedent factors, while risk perception, trust in digital platforms, and self-efficacy are proposed as mediating mechanisms that may shape Digital Financial Security Awareness (knowledge and attitude). Higher awareness, in turn, is expected to support Secure Digital Financial Behaviour, reduced vulnerability to cyber fraud, and improved financial well-being.

Conclusion: The study contributes to the existing literature by presenting an integrated conceptual model that enhances understanding of digital financial security awareness among salaried women. The framework provides valuable implications for policymakers, financial institutions, employers, and educators in designing effective awareness programs and serves as a strong theoretical basis for future empirical validation.

To cite this article: Suva, H.D., Chavda, D. R. (2026). Strengthening Digital Financial Security Among Salaried Women: A Conceptual Framework for Safe Financial Practices. *International Journal of Sustainable Business, Management and Accounting*, 2(2), 93-109.

This article is licensed under a [Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/) ©2026 by author/s

INTRODUCTION

India's financial environment experienced a significant digital change in the last ten years. Due to government-led initiatives like Digital India, a growing number of smartphones, and affordable internet, Unified Payments Interface, or UPI, e-banking, mobile wallets, and digital lending platforms have all seen rapid growth (RBI, 2023–2025; NPCI, 2023–2025). (Zainuddin, A., Aziz, F. M. M., Harith,

N. H. M., Rahim, M. A., & Yusoff, B., 2024). Salaried women are now a more actively involved and financially independent user group since they use digital platforms for regular monetary transactions, debt management, savings, and investments (World Bank, 2021).

However, cyber-financial dangers have risen along with this digital footprint. The sophisticated nature of phishing attacks, bogus OTP requests, phone support lines, malicious mobile applications, and phishing scams has increased, and they often target consumers who are less tech-savvy or have a short time frame (CERT-In, 2023–2025). Digital financial security awareness is a significant but understudied problem because paid women typically balance work and home obligations, making it difficult for these individuals to stay updated with developing cyberthreats. Official statistics document a substantial volume of cybercrimes against women (National Crime Records Bureau, 2023). Although these data do not isolate cyber-financial fraud by gender in a fully disaggregated manner, they, together with secondary studies that report differences in technical training exposure and security practices among women employees (Kumari & Devi, 2022; Bothara & Khaire, 2025), reinforce the relevance of examining digital financial security awareness among salaried women. Claims of higher vulnerability are therefore treated cautiously and framed as indicating a need for targeted awareness rather than as definitive population-level evidence (Kumari & Devi, 2022).

While considerable research exists independently in the domains of financial literacy (OECD & INFE, 2020) and cybersecurity awareness (Parsons et al., 2017), an integrated conceptual model that explains how various factors interact to affect salaried women's perception of digital financial security and how this awareness translates into safe financial conduct and improved financial well-being is currently lacking. By offering a conceptual framework founded on commonly accepted notions of financial literacy, adoption of technology, and information awareness of security, this study aims to close that gap (World Bank, 2021).

Need and Significance of the Study

1. In recent years, there has been a steady increase in digital payment fraud instances in India. Official and secondary sources highlight cyber risks affecting women and indicate the need for gender-sensitive digital security awareness programmes (National Crime Records Bureau, 2023; Kumari & Devi, 2022). While NCRB data confirm a substantial volume of cybercrimes against women, fully gender-disaggregated statistics specifically on cyber-financial fraud remain limited. (National Crime Records Bureau, 2023).
2. Since salaried women handle their own income and make more financial decisions, their understanding of digital security is closely related to the financial well-being of both households and individuals (World Bank, 2021).
3. Current standards for financial literacy (OECD & INFE, 2020) do not fully account for hazards unique to digital payments, such as phishing, OTP fraud, and fraudulent applications (NPCI, 2023–2025).
4. Future empirical studies, financial institutions, employers, and legislators can create focused awareness campaigns with the use of a structured conceptual framework (RBI, 2023–2025).
5. Understanding the mediating psychological factors, risk perception, trust, and self-efficacy can help design more effective behaviour-change interventions rather than one-size-fits-all awareness campaigns.

Research Gap

Previous studies have examined digital financial security-related issues largely in separate streams. Financial literacy research (Maina & Györke, 2025) has focused on knowledge, attitude and behaviour; digital banking studies (Kaur & Arora, 2021; Choung et al., 2023) have assessed awareness and safe usage among working women; TRI 2.0 has explained adoption-related factors; Protection Motivation Theory, widely applied in digital security contexts) has linked risk perception and self-efficacy to protective behaviour; and information-security models such as HAIS-Q (Parsons et al., 2017; Latif et al., 2025) have conceptualised awareness as a knowledge–attitude–behaviour composite. Institutional sources (RBI, 2023–2025; NPCI, 2023–2025; CERT-In, 2023–2025; NCRB,

2023) have documented rising digital payment fraud and cyber risks, including those affecting women. However, these contributions remain fragmented. An integrated, gender-contextualised conceptual framework that simultaneously (a) combines financial-literacy, information-security and technology-adoption perspectives, (b) explicitly models the mediating roles of risk perception, trust and self-efficacy, and (c) is grounded in the digital-payment risk environment and socio-occupational context of salaried women in India is still lacking. The present study addresses this gap by proposing such an integrated framework linking antecedent factors, mediating psychological mechanisms, digital financial security awareness, Secure Digital Financial Behaviour and downstream outcomes (reduced vulnerability to fraud and improved financial well-being), thereby providing a coherent theoretical foundation for future empirical validation using structural equation modelling.

Objectives of the Study

1. To examine the current state of digital financial security awareness among salaried women in India.
2. To identify the key factors influencing digital financial security awareness among salaried women.
3. To propose an integrated conceptual framework depicting the relationship between antecedent factors, mediating variables, and outcomes of digital financial security awareness.
4. To discuss the theoretical, managerial, and policy implications of the proposed framework.
5. To suggest directions for future empirical validation of the framework.

Literature review:

A thorough examination of the literature in the fields of financial literacy, digital banking behaviour, cybersecurity, as well as information security awareness was done to determine the theoretical and empirical foundations of the framework that was suggested. Previous research has examined financial understanding, technology readiness, protection motivation, digital payment security, cyber fraud, and security awareness, particularly regarding digital financial services. These studies provide important information about the factors influencing users' comprehension of digital financial security while also demonstrating the lack of attention given to salaried women as a distinct community. Table 1 summarises the key studies and their important contributions that form the basis of the conceptual framework of the present investigation. Table 1 presents the nine core theoretical and institutional works that form the primary foundation of the framework. The full secondary-data pool used for thematic content analysis comprises these nine works together with twelve additional peer-reviewed and policy sources drawn from the reference list including [Agrawal & Agarwal, 2023](#); [Kulkarni & Ghosh, 2021](#); [World Bank, 2021](#); [Zainuddin et al., 2024](#), yielding a total of twenty-one sources.

Table 1. Summary of Literature Review (Secondary Sources)

Author(s) / Year	Focus Area	Key Contribution / Finding
(OECD & INFE, 2020)	Financial Literacy Framework	Proposed a global framework linking financial knowledge, attitude and behaviour, forming the structural basis for adapting the construct to the digital security context.
(Kaur & Arora, 2021)	Digital Banking Awareness	Found moderate awareness among working women; education and income significantly influence safe digital usage.
(Parasuraman & Colby, 2015) – TRI 2.0	Technology Readiness	Optimism, innovativeness, discomfort and insecurity as determinants of technology adoption; widely applied in recent digital-finance contexts (2017–2025).
(Tsai et al., 2016; Dodge et al., 2023) – PMT	Protection Motivation	Threat appraisal (risk perception) and coping appraisal (self-efficacy) jointly predict protective behaviour; extensively used in recent cybersecurity and digital payment studies.
(Reserve Bank of India, 2023–2025)	Cybersecurity in Banking	Highlights a rising trend of digital fraud incidents and calls for targeted awareness programmes for vulnerable user groups, including women.

Author(s) / Year	Focus Area	Key Contribution / Finding
(Kumari & Devi, 2022)	Gender & Cyber Fraud	Reports that women employees may face elevated exposure to phishing and social-engineering scams, associated in the study with comparatively lower exposure to formal technical training (based on the sample examined).
(Parsons et al., 2017) – HAIS-Q	Security Awareness Measurement	Knowledge–Attitude–Behaviour triad widely used to assess information security awareness in organisational settings.
(NPCI, 2023–2025); (CERT-In 2023–2025)	UPI & Digital Payment Fraud Trends	Reports increasing fraud volumes despite rapid UPI adoption, pointing to a persistent awareness–usage gap.
(National Crime Records Bureau, 2023)	Cyber-crime Against Women	Documents cybercrimes against women and supports examination of digital security issues through a gender-sensitive lens.

Source: Author's own thematic synthesis

To provide a stronger theoretical grounding, the four foundational models that inform the proposed framework are discussed below in relation to the key constructs of the present study. The [OECD/INFE Financial Literacy Framework \(2020\)](#) conceptualizes financial literacy as a combination of knowledge, attitude and behaviour. In the digital financial security context, this framework supplies the structural logic for treating Digital Financial Security Awareness primarily as the knowledge and attitude components, while positioning actual protective actions as a downstream behavioural outcome. Higher levels of financial knowledge and positive attitudes towards safety are expected to support safer digital financial practices among salaried women. The Human Aspects of Information Security Questionnaire (HAIS-Q) developed by [Parsons et al. \(2017\)](#) measures information security awareness through knowledge, attitude and behaviour dimensions. While the original HAIS-Q treats behaviour as part of awareness, the present framework deliberately separates Secure Digital Financial Behaviour as a distinct outcome. This separation allows clearer examination of how knowledge of threats and positive security attitudes translate into concrete protective actions such as enabling two-factor authentication, verifying links and monitoring transaction alerts.

The Technology Readiness Index 2.0 (TRI 2.0), originally developed by [Parasuraman and Colby \(2015\)](#) and still widely applied in recent digital-finance studies, identifies optimism, innovativeness, discomfort and insecurity as key drivers of technology-related beliefs and behaviours. In the present framework, TRI 2.0 supplies the technology-adoption foundation that specifically supports the mediating constructs of Trust in Digital Platforms (linked to lower insecurity and higher optimism) and users' comfort with digital financial tools. Self-efficacy, by contrast, is primarily grounded in Protection Motivation Theory. Users who experience lower insecurity and higher comfort with technology are more likely to develop favourable attitudes towards digital platforms, which supports the overall pathway to Digital Financial Security Awareness and Secure Digital Financial Behaviour. Protection Motivation Theory (PMT), originally proposed and widely applied in recent digital-security research ([Tsai et al., 2016](#); [Dodge et al., 2023](#); [Vafaei-Zadeh et al., 2024](#); [Latif et al., 2025](#); [Hassan et al., 2024](#); [Karayel & Saygılı, 2025](#)), posits that protective behaviour results from threat appraisal (risk perception) and coping appraisal (self-efficacy and response efficacy). In the present framework, PMT provides the motivational logic for two mediating constructs: Risk Perception (threat appraisal of phishing, OTP fraud and fake applications) and Self-Efficacy (coping appraisal of one's ability to act safely). higher risk perception combined with stronger self-efficacy is expected to increase Digital Financial Security Awareness ([Tsai et al., 2016](#); [Al-Emran et al., 2025](#)) and motivate Secure Digital Financial Behaviour.

Collectively, these four theoretical perspectives highlight important but previously fragmented insights. Financial literacy models emphasise knowledge and attitude; information security models focus on awareness–behaviour linkages; TRI 2.0 ([Parasuraman & Colby, 2015](#); [Boss et al., 2015](#)) (via dimensions such as insecurity and discomfort) helps account for the formation of trust and self-efficacy; and PMT accounts for the motivational role of risk perception. However, an integrated, gender-contextualised framework that simultaneously links antecedent factors, these psychological

mechanisms, Digital Financial Security Awareness (knowledge + attitude), Secure Digital Financial Behaviour and downstream outcomes for salaried women in India has been lacking. The present study addresses this gap by synthesising the above theoretical foundations into a single coherent model. Three recurring patterns emerged from the review of the literature. First, awareness is typically addressed as a composite of understanding, mindset, and behaviour in financial literacy models like the [OECD/INFE \(2020\)](#) framework. The present study adapts this structure by treating knowledge and attitude as the core of Digital Financial Security Awareness, while locating actual safe practices in a separate outcome construct (Secure Digital Financial Behaviour) to avoid conceptual overlap. Second, the available literature on information security, particularly the HAIS-Q model

Thematic Content Analysis of Reviewed Literature

The twenty-one sources indicated in Table 1 were examined through a thematic analysis in order to arrange the secondary data synthesis. Each source revealed seven recurrent subjects about digital financial security. Examples of citations and the occurrence of each topic in the reviewed sources are displayed in Table 2.

Table 2. Thematic Content Analysis of Reviewed Secondary Literature

Theme Identified	Sources Addressing Theme (of 21 reviewed)	Illustrative Sources
Phishing, OTP fraud & fake-app scams	12 / 21	RBI (2023–2025) ; NPCI/CERT-In (2023–2025) ; NCRB (2023) ; Kumari & Devi (2022) ; Ministry of Finance (2024) ; Kulkarni & Ghosh (2021)
Digital literacy gap	9 / 21	OECD/INFE (2020) ; Kaur & Arora (2021) ; Kumari & Devi (2022) ; World Bank (2021) ; Agrawal & Agarwal (2023) ; Zainuddin et al. (2024)
Institutional/workplace training gap	7 / 21	Parsons et al. (2017) ; Kulkarni & Ghosh (2021) ; World Bank (2021) ; Zainuddin et al. (2024) ; Parasuraman & Colby (2015) – TRI 2.0
Trust deficit in digital platforms	7 / 21	Parsons et al. (2017) ; Zainuddin et al. (2024) ; Ali et al. (2024) ; Tsai et al. (2016) ; Dodge et al. (2023) – Protection Motivation Theory
Self-efficacy / psychological barriers	7 / 21	Tsai et al. (2016) ; Dodge et al. (2023) – Protection Motivation Theory; Parasuraman & Colby (2015) – TRI 2.0; Parsons et al. (2017) ; Zainuddin et al. (2024) ; Ali et al. (2024)
Gender-related vulnerability dimensions	9 / 21	Kumari & Devi (2022) ; NCRB (2023) ; RBI (2023–2025) ; Kulkarni & Ghosh (2021) ; World Bank (2021) ; Cabeza-García et al. (2019)
Regulatory/policy response	10 / 21	RBI (2023–2025) ; NPCI/CERT-In (2023–2025) ; NCRB (2023) ; Ministry of Finance (2024) ; OECD/INFE (2020) ; World Bank (2021)

Source: Author's own thematic synthesis

Gender-related dimensions of vulnerability and phishing/OTP-fraud typologies, which appear in nine and twelve of the twenty-one sources respectively, are among the most frequently referred topics in the thematic analysis. It should be noted that available official statistics (e.g., NCRB) document cybercrimes against women but do not always provide fully disaggregated data specifically on cyber-financial fraud by gender. The second is the difference in digital literacy. Psychological mediators like trust and self-efficacy are particularly common in academic and theoretical sources than in sector reports (RBI, NPCI, and NCRB). This implies that though institutional material typically focuses on incidence and enforcement, academic research stresses behavioural processes. The requirement for the integrated structure stipulated in Section 6 is supported by this variance alone.

Trend Analysis of UPI-Related Digital Payment Fraud

The increase in UPI-related fraud over the preceding three fiscal years was examined using publicly accessible data provided by the Ministry of Finance in Parliament and disclosed in the RBI's annual disclosures as an additional layer of secondary-data analysis. This tendency is shown in Table 3 and Figure 1. Trend of UPI Fraud Cases and Amount Involved, FY 2022–23 to FY 2024–25.

Table 3. Trend of UPI-Related Digital Payment Fraud in India (Ministry of Finance, 2024)

Period	UPI Fraud Cases Reported	Amount Involved (₹ Crore)
FY 2022–23	7.25 lakh	573
FY 2023–24	13.42 lakh (↑85% YoY)	1,087
FY 2024–25 (Apr–Sep, provisional)	6.32 lakh	485

Source: Ministry of Finance, Government of India (2024, November 25).

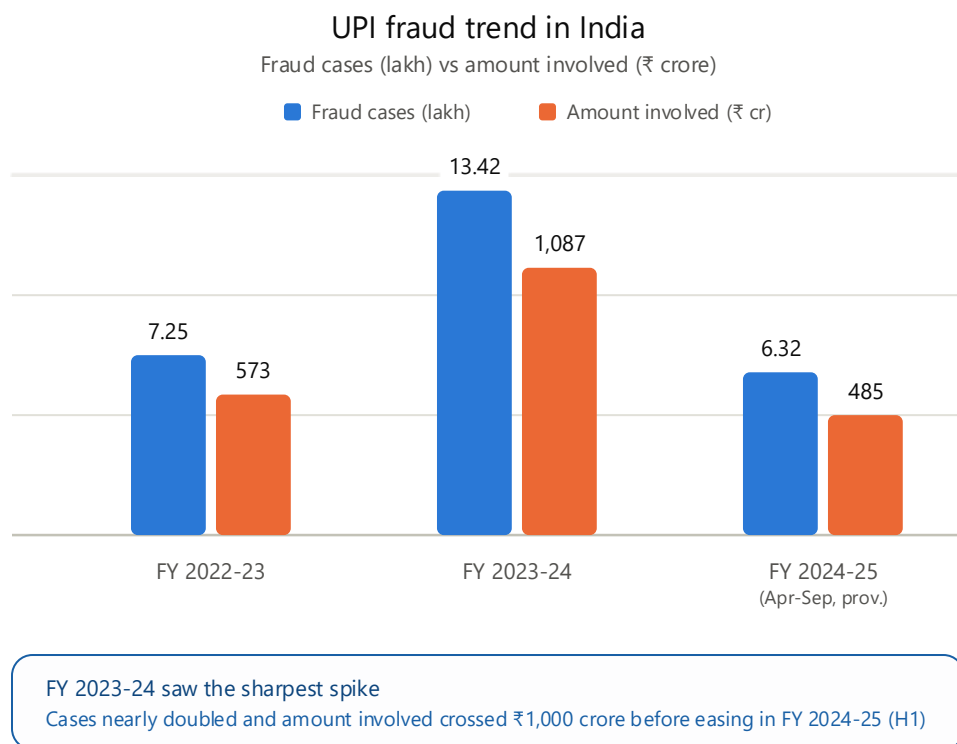


Figure 1. Trend of UPI Fraud Cases and Amount Involved, FY 2022–23 to FY 2024–25

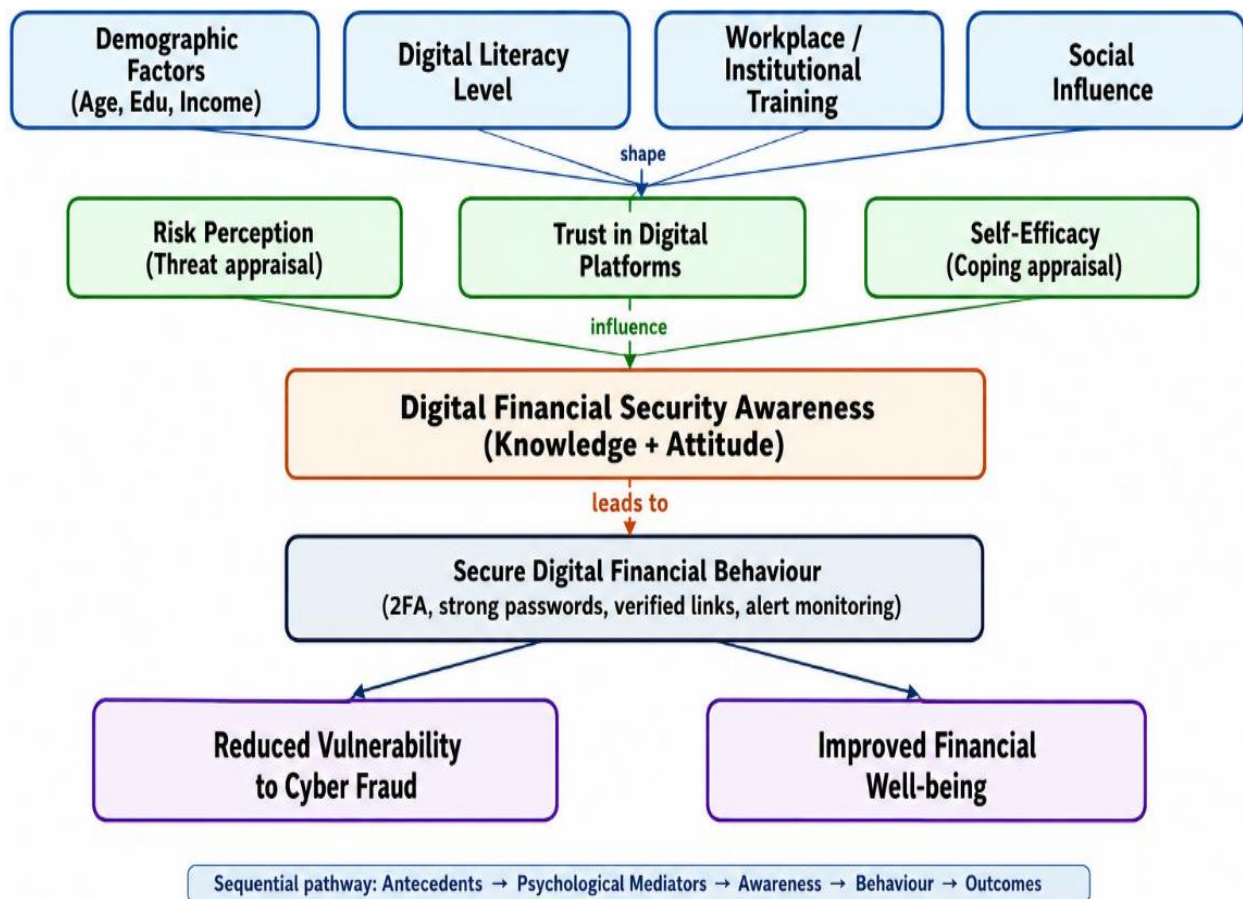
Source: Ministry of Finance, Government of India

The data show an 85% year-on-year increase in reported UPI fraud cases between FY 2022–23 and FY 2023–24, alongside a near-doubling of the amount involved (Ministry of Finance, 2024). The April–September provisional FY 2024–25 data might appear lower in absolute terms, but it is only a partial-year reporting window rather than a real fall. The paper's central claim that digital payment fraud is increasing more quickly than user awareness is supported by this upward trend. Additionally, it highlights how beneficial the suggested conceptual framework is for salaried women who frequently use digital payments (Ministry of Finance, 2024).

4. Proposed Conceptual Framework

This study presents an integrated conceptual framework with four types of constructs: independent (antecedent) variables, mediating variables (psychological mechanisms), the dependent variable (Digital Financial Security Awareness – Knowledge + Attitude), and outcome variables (Secure Digital Financial Behaviour leading to Reduced Vulnerability to Fraud and Financial Well-being). It builds

on the secondary literature that was reviewed. The diagrammatic structure of the proposed model, showing the clear sequential flow, is presented in Figure 2. Conceptual Framework of Digital Financial Security Awareness Among Salaried Women.



Theoretical bases: OECD/INFE (2020) • HAHS © (Parsons et al., 2017) • TRB 2.0 (Parasuraman & Colby, 2015) • PMT (Rogers, 1975)

Figure 2. Conceptual Framework of Digital Financial Security Awareness Among Salaried Women
Source: Author's own conceptualisation based on OECD/INFE (2020), Parsons et al. (2017), recent RBI & NPCI reports (2023–2025), and synthesis of literature 2017–2025.

The sequential flow of the proposed conceptual framework is as follows: Antecedent Factors (Demographic Factors, Digital Literacy Level, Workplace/Institutional Training, and Social Influence) influence the Psychological Mechanisms (Risk Perception, Trust in Digital Platforms, and Self-Efficacy). These mediating mechanisms, in turn, shape Digital Financial Security Awareness (conceptualised as Knowledge + Attitude). Higher awareness then leads to Secure Digital Financial Behaviour (actual protective practices). Finally, Secure Digital Financial Behaviour contributes to the Outcomes of Reduced Vulnerability to Cyber Fraud and Improved Financial Well-being.

4.1 Description of Framework Constructs

Table 4 provides a detailed description of each construct included in the proposed framework, along with representative indicators and the supporting secondary literature that could be used for subsequent empirical measurement.

Table 4. Constructs and Indicators of the Proposed Framework

Category	Variable	Description / Indicators	Supporting Literature
Independent	Demographic Factors	Age, education level, income, job sector/designation	OECD/INFE (2020)
Independent	Digital Literacy Level	Familiarity with apps, devices, online transaction procedures	Kaur & Arora (2021)
Independent	Workplace/Institutional Training	Exposure to cybersecurity training by employer, bank, or government bodies	RBI (2023–2025)
Independent	Social Influence	Guidance/warnings from family, peers, and media exposure	Kumari & Devi (2022)
Mediating	Risk Perception	Perceived likelihood and severity of falling victim to digital fraud	Tsai et al. (2016) ; Dodge et al. (2023) ; Vafaei-Zadeh et al. (2024) – PMT
Mediating	Trust in Digital Platforms	Confidence in banks, payment apps, and regulatory safeguards	Parasuraman & Colby (2015) ; Boss et al. (2015) – TRI 2.0
Mediating	Self-Efficacy	Confidence in one's own ability to use digital finance tools safely	Tsai et al. (2016) ; Dodge et al. (2023) ; Latif et al. (2025) – PMT
Dependent	Digital Financial Security Awareness	Composite of knowledge of digital threats/safe practices and attitude towards digital financial security	Parsons et al. (2017) ; Latif et al. (2025)
Outcome	Secure Digital Financial Behaviour	Use of 2FA, strong passwords, verified links, alert monitoring	Parsons et al. (2017) ; Al-Emran et al. (2025)
Outcome	Reduced Vulnerability to Fraud	Lower incidence of phishing/OTP/UPI fraud victimisation	NPCI (2023–2025) ; CERT-In (2023–2025) ; Ministry of Finance (2024)
Outcome	Financial Well-being	Sense of financial security and independence in digital transactions	World Bank (2021) ; Choung et al. (2023) ; Zainuddin et al. (2024)

Source: Author's own thematic synthesis

Independent Variables

It is predicted that demographic variables including age, education, income level, and employment sector will have an impact on baseline awareness levels. This is consistent with research on financial literacy ([OECD/INFE, 2020](#); [Maina & Györke, 2025](#)) that shows increased digital and financial literacy are associated with higher income and education levels. One important indicator of working women's safe usage of digital banking is their level of digital literacy, which gauges their familiarity with digital tools and processes ([Kaur and Arora, 2021](#)). The [RBI \(2023–2025\)](#) survey, which gauges the degree to which businesses, banks, or governmental organisations provide systematic cybersecurity training, repeatedly revealed shortcomings in workplace or institutional training. According to [Kumari and Devi \(2022\)](#), social influence encompasses the informal channels family, peers, and the

media through which women frequently obtain helpful advice on safe digital practices. This pathway is especially important given that women employees have fewer formal technical skills.

Mediating Variables

Risk perception, trust in digital platforms, and self-efficacy are proposed as mediating variables that translate antecedent factors into actual awareness and behaviour. Drawing from Protection Motivation Theory (Tsai et al., 2016; Dodge et al., 2023; Vafaei-Zadeh et al., 2024; Latif et al., 2025), higher risk perception combined with higher self-efficacy is expected to be associated with stronger adoption of protective digital behaviours. Trust in digital platforms, shaped by both institutional reputation and experience (Parasuraman & Colby, 2015; Boss et al., 2015), is expected to influence the extent to which awareness translates into actual usage confidence (Parasuraman & Colby, 2015).

Dependent Variable: Digital Financial Security Awareness

According to the HAIS-Q (Parsons et al., 2017; Latif et al., 2025) and OECD/INFE (2020) models, digital financial security awareness is conceptualised as a composite construct comprising two core dimensions: knowledge (of digital threats and recommended safe practices) and attitude (perceived importance of digital safety). Although the original HAIS-Q framework includes a behavioural component, the present study deliberately separates actual protective actions into a distinct outcome variable—Secure Digital Financial Behaviour—to avoid conceptual overlap and to enable clearer examination of the awareness–behaviour pathway. Resilience (the ability to recognise, respond to, and recover from fraud attempts) is viewed as an advanced outcome that builds upon awareness and is reflected in secure behavioural practices (CERT-In, 2023–2025). These distinctions are depicted in Figure 3. Layered Dimensions of Digital Financial Security Awareness (Zainuddin, A., Aziz, F. M. M., Harith, N. H. M., Rahim, M. A., & Yusoff, B., 2024).

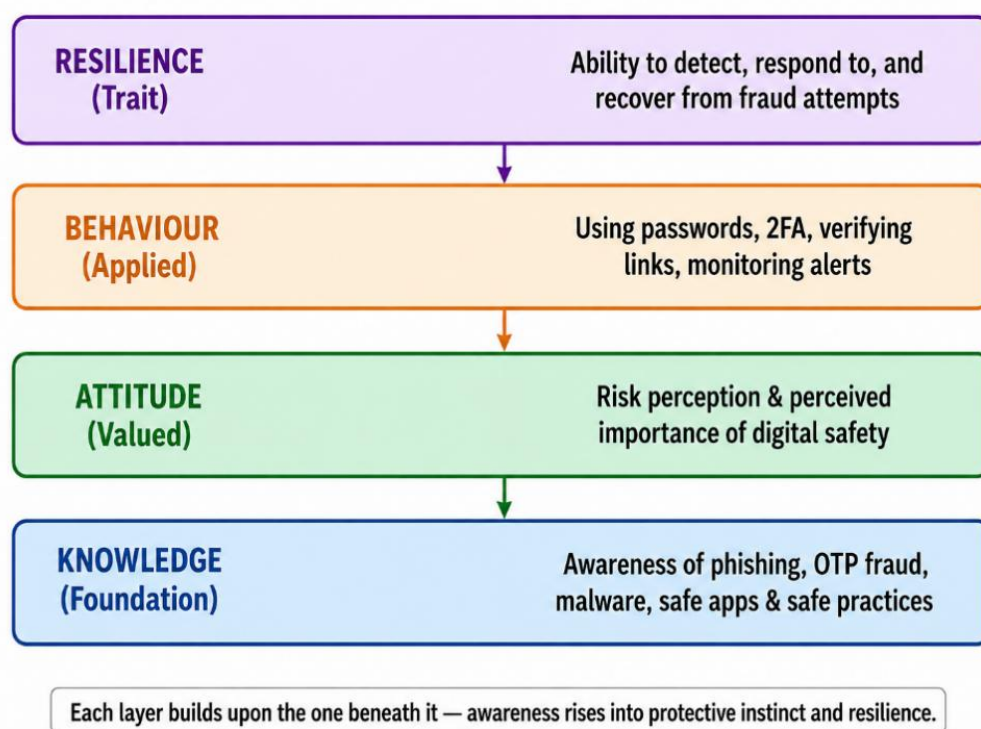


Figure 3. Layered Dimensions of Digital Financial Security Awareness

Source: Adapted and extended by the authors from the Knowledge–Attitude–Behaviour structure

Outcome Variables

According to the framework, higher Digital Financial Security Awareness (knowledge and attitude) is expected to lead to three main outcomes: adoption of Secure Digital Financial Behaviour (actual protective practices such as using strong passwords, two-factor authentication, and checking links before clicking) (Parsons et al., 2017); decreased susceptibility to digital fraud, in line with reports of decreased victimization in areas where awareness interventions have been put into place (NPCI, 2023–2025; CERT-In, 2023–2025); and, eventually, improved financial well-being through increased self-assurance and autonomy in handling digital finances (World Bank, 2021).

Theoretical Underpinnings

The proposed framework draws upon and integrates constructs from several established theoretical models, as summarised in Table 5

Table 5. Theoretical Models Informing the Proposed Framework

Model	Origin/Domain	Relevance to Present Framework
OECD/INFE Financial Literacy Model (2020)	Financial Education	Provides the Knowledge–Attitude structure adapted for Digital Financial Security Awareness; actual behaviour is modelled as a separate downstream outcome.
HAIS-Q (Parsons et al., 2017; Latif et al., 2025)	Information Security	Provides the knowledge–attitude foundation for awareness; the behavioural component is treated as a separate outcome in the present framework to avoid conceptual overlap.
Technology Readiness Index 2.0 – TRI 2.0 (Parasuraman & Colby, 2015; Boss et al., 2015)	Technology Adoption	Source: Parasuraman & Colby (2015). Provides the technology-adoption foundation (optimism, innovativeness, discomfort, insecurity) that supports Trust in Digital Platforms and comfort with digital financial technologies in the present framework.
Protection Motivation Theory – PMT (Tsai et al., 2016; Dodge et al., 2023)	Health/Risk Behaviour	Explains the role of risk perception (threat appraisal) and self-efficacy (coping appraisal) as mediators that drive Digital Financial Security Awareness and Secure Digital Financial Behaviour.

Source: OECD/INFE (2020); Parsons et al. (2017) – HAIS-Q; Parasuraman & Colby (2015) – TRI 2.0; Tsai et al. (2016), Dodge et al. (2023), Vafaei-Zadeh et al. (2024), Latif et al. (2025) – Protection Motivation Theory (PMT)

Implications of the Framework

1. Theoretical Implications

The proposed framework contributes to the literature by integrating financial literacy (OECD/INFE, 2020; Maina & Györke, 2025), information security and technology adoption perspectives into a single, gender-contextualised model. It extends existing awareness models by explicitly incorporating mediating psychological mechanisms grounded in Protection Motivation Theory, offering a more nuanced explanation of how awareness translates into protective behaviour among salaried women specifically (Parsons et al., 2017).

2. Managerial and Policy Implications

1. Banks and fintech companies can use the framework to design targeted, women-focused digital safety campaigns that address trust and self-efficacy gaps, not just knowledge gaps
2. Employers can integrate structured cybersecurity training into workplace induction and periodic training programmes for salaried employees, addressing the training gap noted in RBI (2023–2025) reports.
3. Policymakers and regulators (RBI, NPCI, CERT-In) can use the framework to design awareness metrics that go beyond knowledge testing to assess actual behavioural outcomes.

4. Community and family-based awareness channels should be leveraged, given the significant role of social influence identified by [Kumari and Devi \(2022\)](#) in the framework.

METHOD

Research Methodology

This study adopts a purely conceptual and descriptive research design based exclusively on secondary data. No primary data were collected, and no statistical hypothesis testing was performed. The purpose of the methodology is to systematically review, synthesise, and integrate existing theoretical and empirical literature in order to develop a coherent conceptual framework of digital financial security awareness among salaried women in India.

Sources of Secondary Data

1. Peer-reviewed journal articles and conference papers (Google Scholar, ResearchGate, ScienceDirect)
2. Reports published by the Reserve Bank of India ([RBI, 2023–2025](#); [RBI, 2024](#)) on financial literacy and digital payment security
3. National Payments Corporation of India ([NPCI, 2023–2025](#); [NPCI, 2024](#)) transaction and fraud trend reports
4. Cybersecurity bulletins and advisories issued by CERT-In ([Indian Computer Emergency Response Team, 2023–2025](#))
5. National Crime Records Bureau ([NCRB, 2023](#)) data on cybercrime against women
6. [OECD/INFE \(2020\)](#) financial literacy framework publications
7. Global Findex Database ([World Bank, 2021](#); [World Bank, 2022](#)) on financial inclusion and digital payments
8. Parliamentary replies and press releases of the [Ministry of Finance, Government of India \(2024\)](#), on UPI-related fraud trends

Approach

1. Source Selection Procedure

Relevant literature was identified through structured searches on Google Scholar, ResearchGate, ScienceDirect and official websites of RBI, NPCI, CERT-In, NCRB, OECD and the World Bank. Search terms included combinations of “digital financial security”, “cyber fraud”, “UPI fraud”, “financial literacy”, “information security awareness”, “technology readiness”, “protection motivation”, “women” and “India”. Inclusion criteria focused on peer-reviewed journal articles, theoretical models, and authentic institutional reports published mainly between 2017 and 2025 that addressed financial literacy, information security awareness, technology adoption or digital payment fraud. Preference was given to sources that either provided theoretical constructs or reported empirical/policy evidence relevant to the Indian digital financial ecosystem and women’s experiences. The search was conducted between January 2024 and December 2025. An initial pool of approximately 85 records was identified. After title and abstract screening for relevance to digital financial security, cyber fraud, financial literacy or technology adoption in the Indian context, 42 sources were retained for full-text review. Following full-text screening against the inclusion criteria, 21 sources were finally selected for the thematic content analysis and framework development: nine core theoretical and institutional works (summarised in Table 1) and twelve additional peer-reviewed and policy sources drawn from the reference list.

2. Literature Synthesis Procedure

The selected sources were synthesised using a concept-centric approach. First, key constructs (demographic factors, digital literacy, training, social influence, risk perception, trust, self-efficacy,

awareness and protective behaviour) were extracted from each major theoretical model and empirical study. Second, overlapping and complementary constructs were mapped across the OECD/INFE framework, HAIS-Q, TRI 2.0 and Protection Motivation Theory. Third, the mapped constructs were arranged into antecedent, mediating, dependent and outcome categories to form the proposed integrated framework. All relationships proposed in the framework are therefore derived from logical synthesis of existing literature rather than from new primary data.

3. Thematic Analysis Procedure

A focused thematic content analysis was conducted on the twenty-one core sources listed in Table 1. Each source was examined for recurring themes related to digital financial security (phishing and OTP fraud, digital literacy gaps, institutional training, trust, self-efficacy, gender-related vulnerability dimensions and policy responses). Themes were coded inductively by reading each source for explicit and implicit references to digital financial security issues; codes were then grouped into seven overarching themes and tabulated to show frequency of occurrence across the twenty-one reviewed sources (see Table 2). This thematic mapping helped identify the most salient issues and confirmed the theoretical and practical relevance of the constructs retained in the final conceptual framework.

4. Overall Analytical Approach

The paper follows a conceptual-analytical approach wherein constructs and relationships identified in established models, namely the [OECD/INFE Financial Literacy Framework \(2020\)](#), the Human Aspects of Information Security Questionnaire (HAIS-Q; [Parsons et al., 2017](#)), the Technology Readiness Index 2.0 ([TRI 2.0; Parasuraman & Colby, 2015](#)), and Protection Motivation Theory are systematically synthesised into the proposed integrated conceptual framework.

Future Scope

The suggested methodology should be empirically tested in further studies using primary data gathered from structured questionnaires given to salaried women in various industries, income brackets, and geographical areas. The proposed correlations between independent, mediating, and outcome factors might be statistically validated using structural equation modelling (SEM). ([Hair et al., 2022](#)). Comparative studies across different demographic segments, age groups, urban versus rural, and public versus private sector employees would further strengthen the generalizability of the framework.

RESULTS AND DISCUSSION

Results

The synthesis of secondary literature yields the following key findings. First, demographic factors, digital literacy level, workplace/institutional training and social influence emerge as the main antecedent factors associated with digital financial security awareness. Second, the thematic content analysis of the twenty-one core sources (Table 2) shows that phishing, OTP fraud, fake payment applications, gender-related vulnerability dimensions and digital literacy gaps are the most frequently recurring themes. Third, the trend analysis of UPI-related fraud (Table 3) records a substantial rise in reported cases and amounts between the two complete financial years FY 2022–23 and FY 2023–24; the provisional six-month figures for FY 2024–25 is reported for completeness but are not used for year-on-year comparison. Fourth, risk perception, trust in digital platforms and self-efficacy are identified as the principal mediating mechanisms linking the antecedents to Digital Financial Security Awareness (knowledge + attitude). Finally, the proposed framework positions Secure Digital Financial Behaviour, reduced vulnerability to cyber fraud and improved financial well-being as the expected downstream outcomes of higher awareness.

Discussion

Interpretation of these findings suggests that digital financial security awareness cannot be reduced to financial literacy alone; it requires the joint operation of technological knowledge, security-related attitudes and psychological readiness. By integrating the OECD/INFE framework, HAIS-Q, TRI 2.0 and Protection Motivation Theory, the proposed model offers a coherent account of how antecedent factors shape risk perception, trust and self-efficacy, which in turn influence awareness and, subsequently, actual protective behaviour. The documented rise in UPI fraud between the two full financial years reinforces the practical urgency of such a model for frequent digital-payment users, including salaried women. Importantly, the framework implies that interventions limited to knowledge transfer are likely to be insufficient; programmes must also address trust deficits, risk perception and self-efficacy if they are to convert awareness into sustained Secure Digital Financial Behaviour.

Implications

The proposed conceptual framework offers important theoretical, managerial, and policy implications. For policymakers and regulators, it provides guidance for designing gender-sensitive digital financial security awareness programmes. Financial institutions and fintech companies can utilise the framework to develop customised awareness campaigns that emphasise secure digital practices and fraud prevention. Employers may incorporate regular cybersecurity training into workplace development programmes to strengthen employees' digital financial competencies. Educational institutions can integrate digital financial security topics into financial literacy curricula, thereby preparing future users to recognise and respond to cyber-financial threats effectively.

Research Contribution

This study contributes to the literature by proposing an integrated conceptual framework that combines financial literacy, information security awareness, and technology adoption theories within a single model. Unlike previous studies that examine these constructs separately, the present framework explains the interrelationships among antecedent factors, mediating variables, digital financial security awareness, and behavioural outcomes specifically for salaried women. It also provides a theoretical foundation for future empirical validation using Structural Equation Modelling (SEM) and contributes to the limited literature on gender-contextualised digital financial security awareness among salaried women in India.

Limitations of the Study

1. The framework is conceptual in nature and has been developed entirely from secondary data and literature synthesis; it has not yet been empirically tested or statistically validated.
2. The relationships proposed between constructs are based on theoretical reasoning and prior secondary studies in related domains, and actual relationships may vary across regions and demographic groups.
3. Being based entirely on secondary sources, the study is subject to the limitations, scope, and currency of the reports and literature reviewed ([RBI, 2023–2025](#); [NPCI, 2023–2025](#)).
4. The thematic content analysis (Table 2) and fraud-trend analysis (Table 3, Figure 1. Trend of UPI Fraud Cases and Amount Involved, FY 2022–23 to FY 2024–25) are both derived from secondary sources and are illustrative of broader patterns rather than a statistically validated or exhaustive analysis; the FY 2024–25 figures are provisional and cover only part of the financial year.

Suggestions

Future research should empirically validate the proposed conceptual framework using primary data collected from salaried women across different sectors and regions of India ([Ali et al., 2024](#); [Garg & Mehrotra, 2026](#); [Chanda & Joshi, 2026](#)). Structural Equation Modelling (SEM) may be employed to

examine the relationships among antecedent, mediating, and outcome variables (Hair et al., 2022). Comparative studies involving urban and rural women, public and private sector employees, and different income groups may provide broader insights into digital financial security awareness. Policymakers, employers, banks, fintech organisations, and educational institutions should collaborate to develop continuous, gender-responsive digital financial security awareness programmes that combine financial literacy, cybersecurity education, and behavioural interventions to minimise cyber-financial fraud and improve financial well-being (Desai et al., 2023; Bothara & Khaire, 2025; Maina & Györke, 2025).

CONCLUSION.

This conceptual study makes a focused contribution by proposing an integrated framework that links antecedent factors, psychological mediators (risk perception, trust and self-efficacy), Digital Financial Security Awareness (knowledge and attitude), Secure Digital Financial Behaviour, and downstream outcomes for salaried women in India. By synthesising the OECD/INFE financial literacy model, HAIS-Q, Technology Readiness Index 2.0 (TRI 2.0) and Protection Motivation Theory, the framework offers a coherent theoretical foundation that was previously fragmented across separate streams of literature. The main contribution therefore lies in providing a clear, sequential and gender-contextualised model that can guide both future empirical testing and the design of more effective awareness interventions.

The study has important limitations. It is purely conceptual and relies entirely on secondary literature; the proposed relationships have not been statistically tested. The thematic analysis and fraud-trend observations are illustrative rather than exhaustive, and fully gender-disaggregated official data on cyber-financial fraud remain limited. Consequently, the framework should be regarded as a theoretically grounded proposition rather than an empirically confirmed model.

Future research should empirically validate the framework using primary data collected from salaried women across different sectors, income groups and regions of India. Structural Equation Modelling (SEM) is recommended to test the sequential relationships among antecedents, mediators, Digital Financial Security Awareness, Secure Digital Financial Behaviour and outcomes. Comparative studies (urban–rural, public–private sector) would further enhance the generalisability of the model and strengthen its practical utility for policymakers, employers and financial institutions.

ACKNOWLEDGMENT

The author expresses her heartfelt gratitude to her research guide, Dr. Dineshkumar R. Chavda, Assistant Professor, Department of Commerce and Management, Bhakta Kavi Narsinh Mehta University, Junagadh, for his continuous guidance, valuable suggestions, and constant encouragement throughout the preparation of this conceptual paper. The author also wishes to express her deepest gratitude to her beloved parents, Mr. Dineshbhai Vikrambhai Suva and Mrs. Manjuben Dineshbhai Suva, for their unconditional love, constant support, inspiration, and encouragement, which have been the greatest source of strength throughout her academic journey. Finally, the author sincerely thanks the Department of Commerce and Management, Bhakta Kavi Narsinh Mehta University, Junagadh, for providing a supportive academic environment for completing this study. The author declares that no external financial support or research funding was received for this study.

AUTHOR CONTRIBUTION STATEMENT

HS: Contributed to the conceptualisation of the study, conducted the literature review, developed the conceptual framework, drafted the manuscript, revised and edited the content, and finalised the manuscript for submission. DRC: Provided overall supervision and conceptual guidance, reviewed

the manuscript critically for intellectual content, offered valuable suggestions for improvement, edited the manuscript, and approved the final version for publication.

REFERENCES

- Agrawal, V., & Agarwal, M. (2023). Evaluating financial literacy among working women in Pune: A gender-sensitive approach. In E. L. Eijdenberg, M. Mukherjee, & J. Wood (Eds.), *Innovation-driven business and sustainability in the tropics* (pp. 419–430). Springer. https://doi.org/10.1007/978-981-99-2909-2_24
- Al-Emran, M., Yousuf, H., Al-Sharafi, M. A., & Shaalan, K. (2025). Examining the factors influencing cybersecurity behaviours in m-payment contactless technologies using SEM–ANN approach. *Journal of Financial Services Marketing*, 30(3). <https://doi.org/10.1057/s41264-025-00314-x>
- Ali, U., Fatima, H., Rehman, J., & Baloch, S. (2024). Evaluating the impact of financial literacy on investment decisions: A case study of Balochistan, Pakistan. *Journal of Entrepreneurship, Management, and Innovation*, 6(1), 35–56. <https://doi.org/10.52633/jemi.v6i1.376>
- Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours. *MIS Quarterly*, 39(4), 837–864. <https://doi.org/10.25300/MISQ/2015/39.4.5>
- Bothara, S. S., & Khaire, R. J. (2025). Empowering women in the digital workplace: Evaluating cyber resilience frameworks in Mumbai. *EPJ Web of Conferences*, 328, 01005. <https://doi.org/10.1051/epjconf/202532801005>
- Cabeza-García, L., Del Brio, E. B., & Oscanoa-Victorio, M. L. (2019). Female financial inclusion and its impacts on inclusive economic development. *Women's Studies International Forum*, 77, 102300. <https://doi.org/10.1016/j.wsif.2019.102300>
- CERT-In. (2023–2025). *Cybersecurity advisories and bulletins*. Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, Government of India. <https://www.cert-in.org.in/s2cMainServlet?pageid=PUBADVLIST02&year=2025>
- Chanda, A., & Joshi, P. (2026). Bridging the confidence gap: An empirical study of digital financial literacy and women's economic empowerment in urban India.
- Chen, X., Chen, L., & Wu, D. (2018). Factors that influence employees' security policy compliance: An awareness-motivation-capability perspective. *Journal of Computer Information Systems*, 58(4), 312–324. <https://doi.org/10.1080/08874417.2016.1258679>
- Choung, Y., Chatterjee, S., & Pak, T.-Y. (2023). Digital financial literacy and financial well-being. *Finance Research Letters*, 58, 104438. <https://doi.org/10.1016/j.frl.2023.104438>
- Desai, P. S., Pannerselvam, S., & Chandawarkar, M. (Eds.). (2023). *Women empowerment and financial literacy*. National Press Associates.
- Dodge, C. E., Fisk, N., Burruss, G. W., Moule, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy*, 22(4), 849–868. <https://doi.org/10.1111/1745-9133.12641>
- Garg, S., & Mehrotra, V. (2026). Financial literacy and retirement preparedness: A study of salaried women in Haryana. *Advances in Consumer Research*, 3(4), 386–391. <https://acr-journal.com/article/financial-literacy-and-retirement-preparedness-a-study-of-salaried-women-in-haryana-2958/>
- Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). *A primer on partial least squares structural equation modeling (PLS-SEM)* (3rd ed.). SAGE Publications. <https://us2.sagepub.com/en-us/nam/a-primer-on-partial-least-squares-structural-equation-modeling-pls-sem/book270548>

- Hassan, S., Ahmad, R., Katuk, N., Ghazali, N. N., Aripin, J. A., & Ali, F. (2024). Staying one step ahead: Exploring protection motivation theory to combat cyber-fraud among e-services users. *Procedia Computer Science*, 234, 1364–1371. <https://doi.org/10.1016/j.procs.2024.04.011>
- Jain, S., & Patel, R. (2024). Cyber fraud targeting women in digital banking: Socio-legal perspectives. *The Scientific Temper*.
- Jainy Rahulkumar, S., & Patel, K. (2025). Assessing the financial well-being of working women in Gujarat: The role of financial literacy and investment decisions. *Advances in Consumer Research*, 2(4), 5511–5520. <https://acr-journal.com/article/assessing-the-financial-well-being-of-working-women-in-gujarat-the-role-of-financial-literacy-and-investment-decisions-1889/>
- Karayel, T., & Saygılı, M. (2025). Understanding smartphone security behavior through the core constructs of protection motivation theory: A comparative study of iOS and Android users. *Computers & Security*, 158, 104652. <https://doi.org/10.1016/j.cose.2025.104652>
- Kaur, H., & Arora, S. (2021). Digital banking awareness among working women: An empirical study. *Journal of Financial Literacy Studies*, 8(2), 45–58.
- Klapper, L., & Arora, T. (2022, October 12). Improving women’s access to credit in India. *World Bank Blogs*. <https://blogs.worldbank.org/en/allaboutfinance/improving-womens-access-credit-india>
- Kulkarni, L., & Ghosh, A. (2021). Gender disparity in the digitalisation of financial services: Challenges and promises for women’s financial inclusion in India. *Gender, Technology and Development*, 25(2), 233–250. <https://doi.org/10.1080/09718524.2021.1911022>
- Kumar, S. (2023). Financial inclusion of women: Current evidence from India. *Observer Research Foundation*. <https://www.orfonline.org/research/financial-inclusion-of-women-current-evidence-from-india>
- Kumari, P., & Devi, R. (2022). Gender differentials in vulnerability to cyber-financial fraud. *International Journal of Cyber Studies*, 5(1), 22–34.
- Latif, S. F. A., Sulaiman, N. S., Aziz, N. S. A., Yacob, A., & Nasir, A. (2025). Development of cybersecurity awareness model based on protection motivation theory (PMT) for digital IR 4.0 in Malaysia. *International Journal of Advanced Computer Science and Applications*, 16(3). <https://doi.org/10.14569/IJACSA.2025.01603117>
- Maina, C. W., & Györke, D. K. (2025). A selective systematic review and bibliometric analysis of gender and financial literacy research in developing countries. *Journal of Risk and Financial Management*, 18(3), 145. <https://doi.org/10.3390/jrfm18030145>
- Ministry of Finance, Government of India. (2023). *Pradhan Mantri Jan-Dhan Yojana (PMJDY) progress report*. <https://www.pmjdy.gov.in/account/>
- Ministry of Finance, Government of India. (2024, November 25). Response to unstarred question on domestic UPI-related frauds. Lok Sabha, Winter Session. <https://www.medianama.com/2024/11/223-upi-fraud-up-85-per-cent-fy2023-24-finance-ministry-data/>
- National Crime Records Bureau. (2023). Crime in India 2023: Crime against women/cybercrime statistics. Ministry of Home Affairs, Government of India. <https://ncrb.gov.in/>
- National Payments Corporation of India. (2024). *Unified Payments Interface (UPI) product statistics*. <https://www.npci.org.in/product/upi/product-statistics>
- OECD. (2020). *OECD/INFE 2020 international survey of adult financial literacy*. OECD Publishing. <https://doi.org/10.1787/145f5607-en>
- OECD. (2022). *Digital financial literacy for women*. Organisation for Economic Co-operation and Development.

- Parasuraman, A., & Colby, C. L. (2015). An updated and streamlined technology readiness index: TRI 2.0. *Journal of Service Research*, 18(1), 59–74. <https://doi.org/10.1177/1094670514539730>
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
- Patel, P., Kolte, H., & Satish, R. (2025). Financial literacy and its determinants among tribal women: Evidence from Raigarh District, Chhattisgarh, India. *Advancement in Management and Technology*, 6(2), 8–16. <https://doi.org/10.46977/amt.2025.v06i02.002>
- Reserve Bank of India. (2024). *Annual report 2023–24*. <https://www.rbi.org.in/scripts/AnnualReportPublications.aspx?Id=1399>
- Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, 59, 138–150. <https://doi.org/10.1016/j.cose.2016.02.009>
- Vafaei-Zadeh, A., Nikbin, D., Teoh, K. Y., & Hanifah, H. (2024). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. *International Journal of Bank Marketing*, 43(3), 476–505. <https://doi.org/10.1108/IJBM-03-2024-0138>
- World Bank. (2021). *The Global Findex Database 2021: Financial inclusion, digital payments, and resilience in the age of COVID-19*. World Bank. <https://doi.org/10.1596/978-1-4648-1897-4>
- World Bank. (2022). *The Global Findex Database 2021*. World Bank Group.
- Yohana, E., & Masdupi, E. (2023). The influence of financial knowledge on tax literacy with individual financial management behaviour as a mediation variable. *Advances in Economics, Business and Management Research*, 250, 57–73. https://doi.org/10.2991/978-94-6463-158-6_6
- Youssof, K. B., Abd Razak, N., Mohd Idris, S. M. B., & Mohd Shahren, N. B. (2024). Ontology of Protection Motivation Theory on digital risk—A systematic literature review. *Information Management and Business Review*, 16(4S[I]), 426–432. [https://doi.org/10.22610/imbr.v16i4\(S\)I.4282](https://doi.org/10.22610/imbr.v16i4(S)I.4282)
- Zainuddin, A., Mahamad Aziz, F. M., Mohamed Harith, N. H., Abdul Rahim, M., & Yusoff, B. (2024). Financial literacy in improving financial well-being among female civil servants: A study in Putrajaya. *Pakistan Journal of Life and Social Sciences*, 22(2), 4831–4846. <https://doi.org/10.57239/PJLSS-2024-22.1.00356>
- Zainuddin, A., Abdul Rahim, M., Mohamed Harith, N. H., & Shaiful Nizam, S. N. (2025). Domains of financial literacy among women in public sector: A systematic literature review. *Pegem Journal of Education and Instruction*, 15(2), 105–115. <https://doi.org/10.47750/pegegog.15.02.11>