

Explaining Digital Financial Security Behavior among University Students: The Roles of Financial Literacy, Digital Security Understanding, and Social Environment

Mehmet Akif ALTUNAY¹

Abstract

Digital financial services have become embedded in everyday financial life; however, adopting these services does not necessarily mean using them securely. While much of the FinTech literature has focused on adoption intention, behavioral intention, and continued use, less attention has been paid to users' security-oriented behavior after adoption. The primary aim of this study is to explain secure post-adoption behavior in digital financial services by examining Financial Literacy, Digital Security Understanding, and Social Environment as antecedents of Digital Financial Security Behavior among university students. Data were collected from 1,781 undergraduate students in Türkiye. Exploratory factor analysis was conducted on one subsample (n = 917), whereas confirmatory factor analysis and structural equation modeling were conducted on an independent subsample (n = 864). Full-collinearity variance inflation factors, measurement invariance analyses, and a multilayer perceptron artificial neural network analysis were used as robustness checks. Financial Literacy was the strongest predictor of Digital Financial Security Behavior ($\beta = .466$; $p < .001$), followed by Digital Security Understanding ($\beta = .319$; $p < .001$). The direct path from Social Environment was positive but not statistically significant ($\beta = .077$; $p = .099$). The model explained 59.9% of the variance in Digital Financial Security Behavior. The ANN analysis yielded the same predictor-importance ordering: Financial Literacy (100.00), Digital Security Understanding (67.29), and Social Environment (7.00). The findings indicate that universities and financial-service providers should combine financial-literacy education with applied digital-security training and emphasize concrete protective routines. By shifting attention from FinTech adoption to secure post-adoption behavior, this study contributes to research on user-side security behavior and fraud prevention in digital financial services.

Keywords: *Digital Financial Security Behavior, Financial Literacy, Digital Security Understanding, Social Environment, FinTech, Artificial Neural Network.*



1. Assoc. Prof. Dr., Süleyman Demirel University, mehmetaltunay@sdu.edu.tr, <https://orcid.org/0000-0002-0729-1686>

<https://doi.org/10.30798/makuiibf.1969028>

Article Type	Application Date	Admission Date
Research Article	June 11, 2026	September 8, 2026

1. INTRODUCTION

Digital financial services have become a central part of modern financial life. Mobile banking, mobile payment systems, contactless payments, digital wallets, and other FinTech applications have transformed how people access, transfer, and manage money. This change has expanded service channels and made financial transactions faster, easier, and less reliant on physical service interactions (Alalwan et al., 2024; Alt et al., 2018; Shaikh et al., 2023). At the same time, digital financial services have increased users' exposure to privacy and data security risks, as well as to cyber and fraud risks. As digital platforms process sensitive personal and financial data, the benefits of convenience and accessibility come with the need for secure and informed use (Alalwan et al., 2024; Amnas et al., 2023; Organisation for Economic Co-operation and Development [OECD], 2025; Sinha et al., 2025).

Much of the existing FinTech literature typically focuses on adoption intention, behavioral intention, intention to continue using, trust, perceived benefit, perceived risk, and privacy concerns. Technology acceptance models have provided a crucial foundation for explaining whether users adopt digital financial technologies and whether they intend to do so. Recent FinTech research continues to draw on these frameworks (Bajunaied et al., 2023; Hassan et al., 2024; Singh et al., 2020). Although this literature has provided valuable insights, adoption and safe use are distinct behavioral issues. Even if a user has adopted mobile banking or digital payments, they may still fail to protect their personal data, spot suspicious requests, or respond appropriately to fraud risks.

This study addresses this limitation by shifting the focus from FinTech adoption to digital financial security behavior. This concept refers to the protective, fraud-preventive, and risk-aware behavior exhibited by users when using digital financial services. The construct captures whether users act cautiously in digital transactions, protect their financial information, and respond prudently to security and fraud risks. Recent studies on digital payment security, digital financial literacy, anti-fraud behavior, and cybersecurity awareness indicate that user-side security behavior needs to be directly addressed empirically (Chanda et al., 2025; OECD, 2025; Pak et al., 2026; Puri et al., 2025).

The primary aim of this study is to explain the antecedents of secure post-adoption behavior in digital financial services. More specifically, it tests whether Financial Literacy, Digital Security Understanding, and Social Environment predict Digital Financial Security Behavior among university students. Financial Literacy is expected to support informed financial judgment and risk assessment in digital environments. Digital Security Understanding is expected to help users recognize cyber threats, privacy risks, and unsafe digital applications. Social Environment is examined as a contextual factor that may influence safe behavior through peer expectations, normative pressure, and socially transmitted practices. By combining these three antecedents, the study treats users not merely as adopters but as active participants in digital financial risk management.

The empirical context comprises university students in Türkiye. This group is significant because young adults are active users of digital technologies and are highly likely to encounter digital financial products early in their financial lives. University students may be familiar with technology, but they may differ in financial literacy, understanding of security, and susceptibility to social influence. Examining this group offers an opportunity to understand the behavioral foundations of safer use of digital financial services among digitally active young users.

This research advances the literature in three respects. First, it conceptualizes Digital Financial Security Behavior as a protective post-adoption outcome that is analytically distinct from adoption intention, behavioral intention, and continued use. Second, it separates Financial Literacy from Digital Security Understanding and evaluates them as related but conceptually distinct antecedents of secure behavior, while also testing the incremental role of general socio-contextual support. Third, it combines independent exploratory and confirmatory subsamples with structural equation modeling, multivariate-outlier sensitivity analysis, measurement invariance testing, and an artificial neural network (ANN) robustness analysis. This design enables the study to evaluate both theory-based structural relationships and the stability of predictor-importance rankings across analytical approaches. Following the literature review and hypothesis development, the paper presents the methodology and results and concludes with theoretical and practical implications.

2. LITERATURE REVIEW AND HYPOTHESIS FORMULATION

2.1. Framing Secure Use as Post-Adoption Protective Behavior

Because adopting a digital financial service is not the same as using it securely, the present study frames secure use as protective post-adoption behavior and draws on three behavioral research streams. First, protection motivation theory argues that people's protective behavior depends on how they judge threats and their own ability to respond (Rogers, 1975, 1983). This study does not test the theory in full. However, the perspective supports the idea that secure behavior needs more than access to technology. Users must see risks and believe protective responses are meaningful and possible. Second, technology threat-avoidance theory distinguishes between technology adoption and threat avoidance. It argues that acceptance-based explanations provide only a partial account of how users respond to malicious information technology threats (Liang & Xue, 2009). This distinction applies to digital financial services, where users might adopt mobile banking or digital payment tools yet still click risky links, use unsafe networks, or fall for fraud. Third, behavioral information security research highlights the role of individual users in protecting information. It urges attention to user security behavior rather than to technical or organizational controls alone (Crossler et al., 2013).

Together, these perspectives provide the theoretical logic for the proposed model. Financial Literacy is expected to strengthen the financial judgment needed to evaluate suspicious claims and risky transactions; Digital Security Understanding represents the cognitive capacity to recognize threats and

understand protective mechanisms; and Social Environment represents a potential source of normative and informational support. Accordingly, H1 and H2 reflect individual-level threat-evaluation and coping resources, whereas H3 tests whether broader socio-contextual support has an additional direct relationship with protective post-adoption behavior.

2.2. Digital Financial Security Behavior

In this study, Digital Financial Security Behavior is an author-synthesized construct developed from research and policy guidance on secure digital payments, digital financial literacy, fraud prevention, and user-side information security (Crossler et al., 2013; OECD, 2025; Pak et al., 2026; Puri et al., 2025). It refers to the protective, fraud-preventive, and risk-aware actions users take when interacting with digital financial services. This behavior includes careful transaction management, safeguarding personal and financial information, avoiding risky digital habits, recognizing signs of fraud, and responding cautiously to suspicious digital financial interactions. Conceptually, this behavior differs from the general FinTech adoption process. While adoption research examines whether users are willing to use digital financial technologies (Bajunaied et al., 2023; Hassan et al., 2024; Singh et al., 2020), Digital Financial Security Behavior concerns how securely they use them. Secure digital financial behavior is not determined solely by platform infrastructure; it also depends on whether users understand the security implications of their own actions. Depending on how they manage passwords, data sharing, network choices, payment requests, and suspicious messages, users can either reduce or increase their risk of falling victim to fraud. Recent studies and policy-focused research emphasize the need for secure digital-payment practices, fraud awareness, and digital financial literacy to protect users in digital financial environments (OECD, 2025; Pak et al., 2026; Puri et al., 2025). Accordingly, Digital Financial Security Behavior is the behavioral outcome assessed in this study.

2.3. Financial Literacy and Digital Financial Security Behavior

Financial literacy provides individuals with the cognitive and behavioral capacity to understand financial information, evaluate financial alternatives, and make prudent decisions under conditions of uncertainty. In this study, following the Organisation for Economic Co-operation and Development/International Network on Financial Education (OECD/INFE) framework, it is operationalized as an applied and multidimensional construct that incorporates financial knowledge, financial behavior, and attitude-related elements. This broader operationalization is appropriate because secure digital financial behavior requires not only factual knowledge of financial concepts but also the capacity to translate such knowledge into prudent financial decisions, disciplined transaction habits, and cautious responses to risky or deceptive digital financial situations.

Recent studies support the argument that financial literacy is closely related to safer behavior in digital financial settings. Pak et al. (2026) link digital financial literacy to the ability to use digital financial services safely and avoid deceptive schemes that exploit digital vulnerabilities. Similarly, the

OECD (2025) argues that higher levels of digital financial literacy can improve users' awareness of digital payment risks and strengthen their capacity to protect themselves online. Puri et al. (2025) also associate digital financial awareness with users' ability to respond effectively to digital financial fraud risks. Sinha et al. (2025) further emphasize that financial literacy is important not only for accessing mobile banking tools but also for making informed decisions in digital financial environments.

From this perspective, Financial Literacy may reduce vulnerability in digital financial transactions by strengthening users' ability to question financial claims, compare alternatives, evaluate risks, and act cautiously in uncertain situations. Therefore, students with higher levels of Financial Literacy are expected to demonstrate stronger digital financial security behavior.

H1: Financial Literacy is positively associated with Digital Financial Security Behavior.

2.4. Digital Security Understanding and Digital Financial Security Behavior

In this study, Digital Security Understanding is an author-synthesized, awareness-oriented construct informed by behavioral information security and cyber-threat-awareness research (Chanda et al., 2025; Crossler et al., 2013; Puri et al., 2025). It refers to users' awareness and understanding of the security risks, protective mechanisms, and vulnerabilities associated with digital financial transactions. The construct captures whether students recognize the function of security controls, understand the importance of two-factor authentication, comprehend the role of data encryption, are aware of the risks of unsecured Wi-Fi networks, and understand the protective value of biometric authentication. It is conceptualized as an understanding-oriented antecedent rather than as a direct measure of general security behavior. A student may understand the importance of two-factor authentication or the risks of unsecured networks yet still fail to review account transactions regularly, recognize phishing messages, or protect financial information in daily practice.

This distinction is important because secure digital financial behavior is not determined solely by platform infrastructure. It also depends on whether users understand the security implications of their own actions. Chanda et al. (2025) emphasize that knowledge of cyber threats can improve individuals' understanding of security vulnerabilities and increase awareness regarding risky actions such as clicking suspicious links or sharing sensitive information. Similarly, Puri et al. (2025) argue that limited technological awareness, including unsafe network use or unsecured third-party access, can increase exposure to digital financial fraud. Alalwan et al. (2024) also note that users of digital payment technologies may become vulnerable to privacy breaches, online fraud, and identity theft when they do not take privacy and security risks seriously.

From this perspective, Digital Security Understanding is expected to strengthen Digital Financial Security Behavior by improving users' ability to recognize threats, evaluate risky transaction contexts, and understand the protective function of security mechanisms. However, the construct is not

treated as identical to the behavioral outcome; rather, it is positioned as a cognitive and awareness-based precursor to secure behavior in digital financial environments.

H2: Digital Security Understanding is positively associated with Digital Financial Security Behavior.

2.5. Social Environment and Digital Financial Security Behavior

The social environment may shape how individuals perceive, learn, and practice security-related behavior in digital financial contexts. In technology adoption research, social influence is commonly used (Venkatesh et al., 2003) to explain whether significant others, such as family members, friends, or peers, affect an individual's intention to use a particular technology. In this tradition, social influence refers to the extent to which individuals perceive that important others believe they should use a given system.

The present study conceptualizes Social Environment as a broader source of perceived social and institutional support. The construct includes family encouragement, peer awareness, university-level information, and social support for saving and financial goals. Therefore, it reflects general socio-contextual support rather than direct social enforcement of secure digital financial behavior.

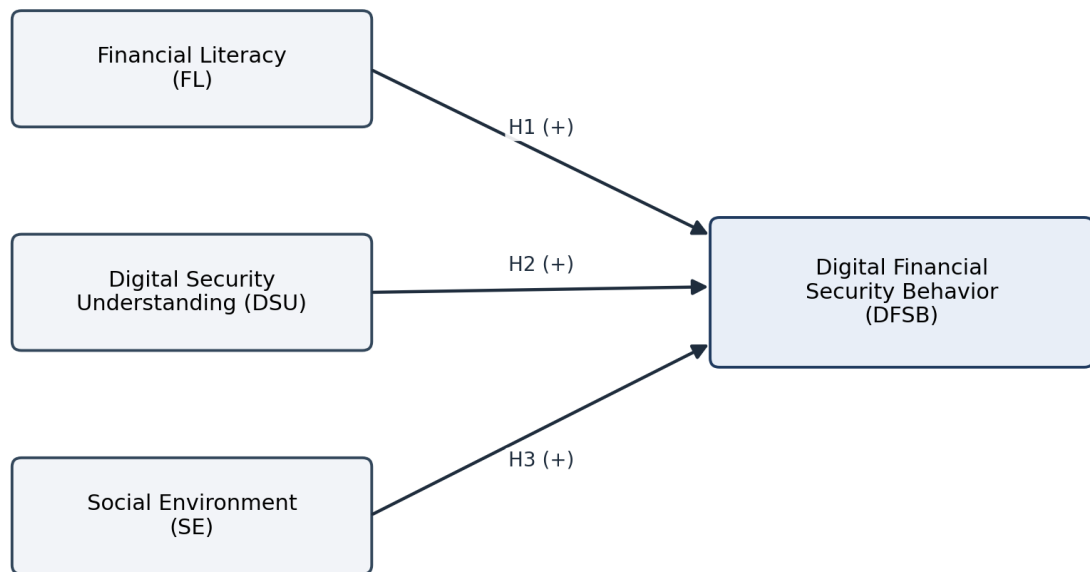
Recent studies provide theoretical support for the relevance of social and normative influences in digital risk contexts. Chanda et al. (2025) associate normative pressure with protecting personal and financial information from unauthorized access, data breaches, and cyber threats. Similarly, Puri et al. (2025) suggest that the social and ethical standards surrounding digital payment platforms may encourage individuals to take reasonable precautions against digital financial fraud. A student-based study by Supu et al. (2025) also indicates that financial literacy, information-system understanding, and social environment may jointly contribute to fraud-mitigation behavior in digital transactions.

Nevertheless, direct evidence on the relationship between Social Environment and digital financial security behavior remains less developed than the evidence concerning Financial Literacy and Digital Security Understanding. For this reason, the hypothesis is framed as a theoretically plausible and empirically testable expectation rather than as a strongly established relationship. The study, therefore, examines whether general social and institutional support directly contributes to students' Digital Financial Security Behavior when Financial Literacy and Digital Security Understanding are considered simultaneously.

H3: Social Environment is positively associated with Digital Financial Security Behavior.

The hypothesized relationships are summarized in Figure 1.

Figure 1. Conceptual Research Model



Note: FL = Financial Literacy; DSU = Digital Security Understanding; SE = Social Environment; DFSB = Digital Financial Security Behavior.

3. METHOD

This study employed a cross-sectional and explanatory-correlational quantitative survey design to examine how Financial Literacy, Digital Security Understanding, and Social Environment relate to Digital Financial Security Behavior among undergraduate students. The psychometric structure of the measurement instrument was evaluated using exploratory and confirmatory factor analyses. The hypotheses were tested using structural equation modeling, and a multilayer perceptron artificial neural network analysis was employed as a supplementary robustness check.

3.1. Research Design, Population, Sampling Procedure, and Ethical Considerations

The study population consisted of undergraduate students enrolled in the Faculty of Economics and Administrative Sciences at Süleyman Demirel University during the 2025–2026 academic year. According to the official student distribution by department and year level, the faculty had 5,603 undergraduate students. Therefore, this figure constituted the study's accessible population.

Data were collected between December 2025 and January 2026 using a structured, voluntary questionnaire. Because participation depended on students' voluntary response, and access to the entire population under controlled probability-sampling conditions was not feasible, a non-probability convenience sampling strategy was employed. The study specifically targeted students enrolled in the relevant faculty, whose frequency of digital financial transaction use was subsequently described in the participant profile. Only completed questionnaires were included in the final dataset. The final sample comprised 1,781 undergraduate students, representing approximately 31.8% of the accessible population.

Before data collection, ethical approval was obtained from the Ethics Committee of Süleyman Demirel University, with decision number 179/24 dated 19 November 2025. Participation was entirely voluntary, and no personally identifiable information was collected. Participants were informed about the study's purpose, the questionnaire's anonymity, their right to withdraw at any time, and the use of the data solely for academic research.

3.2. Measurement Instrument Development and Content Validation

Data were collected using a seven-point scale (1 = Strongly Disagree, 7 = Strongly Agree). Rather than being translated from a single pre-existing instrument, the item pool was developed by synthesizing constructs and indicators from research and policy documents on financial literacy, digital financial services, user security behavior, social influence, and fraud prevention (Crossler et al., 2013; OECD, 2025; Puri et al., 2025; Supu et al., 2025; Venkatesh et al., 2003). Supu et al. (2025) provided the closest empirical point of departure by examining financial literacy, accounting-information-system understanding, and social environment as predictors of financial-fraud mitigation in digital transactions. The present instrument reformulated and extended these domains to measure secure post-adoption behavior among a broader university-student sample. The resulting items were therefore author-developed or conceptually adapted rather than direct translations of a single scale.

The initial item pool was constructed by defining the conceptual domain of each construct separately. Digital Financial Security Behavior (DFSb) was designed to capture protective and fraud-preventive behaviors in digital financial transactions, such as checking the security of websites and applications, protecting passwords, recognizing phishing messages, using strong passwords, and monitoring account transactions. Financial Literacy (FL) was operationalized in line with the OECD/INFE approach as a multidimensional construct that includes financial knowledge, financial behavior, and attitude-related elements. Although these indicators cover knowledge-, behavior-, and attitude-related aspects, they were treated as empirically related manifestations of applied financial literacy in this student sample rather than as separate subdimensions. This specification was supported by the exploratory factor analysis (EFA) and confirmatory factor analysis (CFA) results. Accordingly, this dimension covered basic financial concepts, budgeting, saving, impulse control in purchasing, and cost-benefit evaluation of financial products. Digital Security Understanding (DSU) was developed to capture students' understanding of digital security risks and protective mechanisms, including security controls, two-factor authentication, data encryption, unsecured Wi-Fi networks, and biometric login. This construct was therefore treated as an awareness- and understanding-oriented antecedent, whereas Digital Financial Security Behavior was treated as the behavioral outcome reflecting broader protective conduct in digital financial transactions. Social Environment (SE) was designed to reflect perceived social and institutional support, including family encouragement, peer awareness, university-level information, and support for saving and financial goals.

The construct-level item-development map was as follows. DFSB items M1–M5 were conceptually informed by secure-payment, fraud-mitigation, and user-protection guidance (OECD, 2025; Puri et al., 2025; Supu et al., 2025). FL items M6–M10 were informed by the OECD/INFE financial-literacy framework and the financial-literacy indicators discussed by Supu et al. (2025). DSU items M11–M15 drew on information-security controls and digital-security indicators discussed in behavioral information security research (Crossler et al., 2013; Puri et al., 2025) and in Supu et al. (2025). SE items M16–M20 were informed by social-influence and socio-contextual support research (Supu et al., 2025; Venkatesh et al., 2003). These sources defined the conceptual domains; the wording of the items was developed for the present university-student and digital-finance context.

The initial item pool was reviewed by six accounting faculty members with subject-matter expertise. The experts evaluated the items qualitatively in terms of conceptual relevance, clarity, wording, redundancy, and representation of the intended construct. Their review led to minor wording refinements and the revision of items considered repetitive, weakly aligned, or potentially ambiguous before the main data collection. Because the instrument was newly developed, its measurement quality was subsequently evaluated through exploratory factor analysis, confirmatory factor analysis, reliability analysis, and tests of convergent and discriminant validity.

The questionnaire initially had 20 items across four expected dimensions. Following exploratory factor analysis, the reverse-coded M20 item in the Social Environment dimension was removed because it did not fit the factor structure and showed low communality with the construct. Thus, the final measurement structure used in later analyses included four factors and 19 items.

3.3. Data Screening and Psychometric Validation Strategy

Prior to the main analysis, the dataset was screened for missing data, univariate and multivariate outliers, normality, and common method bias. Univariate outliers were assessed using standardized Z-scores, whereas multivariate outliers were examined using Mahalanobis distance (Hair et al., 2019). Because large samples may yield overly sensitive normality test results, the Kolmogorov-Smirnov and Shapiro-Wilk tests were not used as standalone decision criteria. Instead, skewness and kurtosis coefficients were used to evaluate univariate normality (Al-Okaily, 2025; Hair et al., 2019).

The risk of common method bias was assessed in two stages. First, Harman's single-factor test was applied, and the proportion of variance explained by a single factor was examined (Amnas et al., 2023; Podsakoff et al., 2003). Second, because Harman's test alone is not sufficient to rule out common method bias, full-collinearity variance inflation factor (VIF) values were calculated (Bouteraa, 2024; Chanda et al., 2025). For this purpose, Digital Financial Security Behavior, Financial Literacy, Digital Security Understanding, and Social Environment were included in the same model, and the VIF values were compared against the threshold of 3.3 (Kock, 2015).

To reduce the risk of model overfitting arising from exploring and validating the factor structure on the same data, the dataset was split into two independent subsamples. Exploratory factor analysis (EFA) was conducted on the EFA subsample comprising 917 observations, whereas confirmatory factor analysis (CFA) and structural equation modeling (SEM) were conducted on the CFA/SEM subsample comprising 864 observations. Thus, the factor structure was first explored in one subsample and subsequently validated in another.

Reliability analysis, exploratory factor analysis, normality assessment, and common method bias diagnostics were conducted using IBM SPSS Statistics 30. Confirmatory factor analysis, structural equation modeling, and measurement invariance analyses were carried out using AMOS 22. Convergent and discriminant validity were assessed using composite reliability, average variance extracted, the Fornell-Larcker criterion, and the heterotrait-monotrait (HTMT) ratio. The research hypotheses were tested using a structural equation model. The ANN-based robustness analysis was conducted in Google Colab using Python and scikit-learn.

3.4. Measurement Invariance Analysis

To assess the cross-group stability of the measurement structure, measurement invariance analyses were conducted using multi-group confirmatory factor analysis across gender, year level, and broad academic field groups. Configural, metric, and scalar models were tested sequentially. In model comparisons, the criteria of $\Delta CFI \leq .010$ and $\Delta RMSEA \leq .015$ were adopted (Chen, 2007; Cheung & Rensvold, 2002).

The department variable was not tested within a multi-group CFA framework across 13 separate category levels due to the large number of categories and the relatively small sizes of some departmental groups. Instead, departments were reclassified into two macro-academic fields based on their exposure to economic-financial and analytical courses in the compulsory course plans. Labor Economics and Industrial Relations, Econometrics, Finance and Banking, Economics, Business Administration, Public Finance, Health Management, and International Trade and Logistics were classified as the “high-medium economic-financial/analytical exposure” group. Human Resource Management, Political Science and Public Administration, Social Work, Tourism Administration, and International Relations were classified as the “mixed-low social-management/service exposure” group. Measurement invariance was then assessed across these two macro-academic field groups.

3.5. ANN-Based Robustness Check

As a complementary robustness check, a multilayer perceptron ANN was estimated in Google Colab using Python/scikit-learn on the CFA/SEM subsample. Construct-level mean scores for Financial Literacy, Digital Security Understanding, and Social Environment were used to predict Digital Financial Security Behavior. Predictor variables were standardized, and model performance was evaluated using repeated 10-fold cross-validation. Permutation importance based on R^2 reduction was used to assess

relative predictor importance. The ANN analysis was used as a supplementary non-linear robustness check, not as a replacement for the theory-based SEM model.

4. FINDINGS

4.1. Participant Profile and Data Pre-checks

Table 1 summarizes the demographic characteristics of the participants.

Table 1. Demographic Characteristics of Participants

Variable	Group	n	%
Gender	Female	1260	70.7
	Male	521	29.3
Departments	Labor Economics and Industrial Relations	100	5.6
	Econometrics	62	3.5
	Finance and Banking	189	10.6
	Economics	123	6.9
	Human Resource Management	167	9.4
	Business Administration	261	14.7
	Public Finance	201	11.3
	Health Management	160	9.0
	Political Science and Public Administration	211	11.8
	Social Work	48	2.7
	Tourism Administration	111	6.2
	International Relations	101	5.7
	International Trade and Logistics	47	2.6
Year	First year	508	28.5
	Second year	497	27.9
	Third year	346	19.4
	Fourth year	430	24.1
Frequency of Use of Digital Financial Transactions	Very rarely	50	2.8
	A few times a month	65	3.6
	A few times a week	205	11.5
	Once a day	159	8.9
	A few times a day	1302	73.1

A total of 1,781 participants were included in the study. Of the participants, 70.7% were female, and 29.3% were male. When the departmental distribution was examined, the highest participation came from the Business Administration (14.7%), Political Science and Public Administration (11.8%), Public Finance (11.3%) and Finance and Banking (10.6%) departments.

The distribution of participants by year level was relatively balanced; 28.5% of the sample consisted of first-year students, 27.9% of second-year students, 19.4% of third-year students and 24.1% of fourth-year students. In terms of the frequency of digital financial transactions, it is evident that a significant proportion of participants are in frequent contact with such transactions. Among the participants, 73.1% stated that they carried out digital financial transactions several times a day. This

finding indicates that the research sample consists of a group of students with a high level of experience in digital financial transactions.

Table 2. Data Preparation, Preliminary Analyses and Common Method Bias Checks

Analysis / Check	Criterion	Result	Assessment
Missing data check	Valid N for M1–M20	No missing data	Acceptable
Univariate outlier	$ Z > 3.29$	0	No outliers
Multivariate outlier	Mahalanobis $D^2 > \chi^2(20) = 45.315$; $p < .001$	124	Flagged for sensitivity analysis
Observation within normal range	Mahalanobis $D^2 \leq 45.315$	1657	Acceptable
Normality - all data	Skewness $ 2 $; kurtosis $ 2 $	Skewness: $-.993$ to $.422$; kurtosis: -1.407 to $-.360$	Acceptable
Normality - after outliers were excluded	Skewness $ 2 $; kurtosis $ 2 $	Skewness: $-.957$ to $.399$; kurtosis: -1.372 to $-.404$	Acceptable
Harman single-factor test	Single-factor variance $< 50\%$	44.222%	No indication of serious common method bias
Harman test KMO	$> .60$	.951	Acceptable
Harman Bartlett test	$p < .05$	$\chi^2 = 21,791.855$; $df = 190$; $p < .001$	Acceptable
Full collinearity VIF - Digital Financial Security Behavior	VIF < 3.3	Tolerance = $.486$; VIF = 2.057	Acceptable
Full collinearity VIF - Financial Literacy	VIF < 3.3	Tolerance = $.479$; VIF = 2.088	Acceptable
Full collinearity VIF - Digital Security Understanding	VIF < 3.3	Tolerance = $.442$; VIF = 2.260	Acceptable
Full collinearity VIF - Social Environment	VIF < 3.3	Tolerance = $.519$; VIF = 1.927	Acceptable
EFA subsample	Data splitting	$n = 917$; 51.5%	Acceptable
CFA subsample	Data splitting	$n = 864$; 48.5%	Acceptable

Note: The value $\chi^2(20) = 45.315$ represents the Mahalanobis distance critical value at $p < .001$. Normality was evaluated using skewness and kurtosis. Harman's single-factor test was conducted as an unrotated single-factor solution, and full collinearity VIF values were used as an additional common method bias diagnostic. EFA = Exploratory Factor Analysis; CFA = Confirmatory Factor Analysis.

Data screening and common method bias diagnostics followed established recommendations for outlier detection, normality assessment and common method bias control (Bouteraa, 2024; Chanda et al., 2025; Hair et al., 2019; Podsakoff et al., 2003). Data screening indicated no missing data and no univariate outliers. Mahalanobis distance identified 124 multivariate outliers, which were retained in the main analyses and later examined through sensitivity analysis. Skewness and kurtosis values were within acceptable limits both before and after excluding these cases. Harman's single-factor test explained 44.222% of the variance, and all full collinearity VIF values were below 3.3, suggesting that common method bias was unlikely to distort the substantive findings.

4.2. Exploratory Factor Analysis and Reliability

The dataset was divided into two subsamples for use in the psychometric validation process. Exploratory factor analysis was conducted on the EFA subsample comprising 917 observations, while

confirmatory factor analysis was carried out on the CFA subsample comprising 864 observations. This approach was chosen to reduce the risk of model overfitting that could arise from both discovering and validating the factor structure on the same data.

Table 3. Results of Exploratory Factor Analysis

Factor	Item	Factor load
DFSB - Digital Financial Security Behavior	M1. I ensure the security of websites and apps	.600
	M2. I do not share my bank or e-wallet password with anyone	.890
	M3. I can recognize phishing messages	.771
	M4. I use different and strong passwords	.675
	M5. I check my account transactions regularly	.780
DSU - Digital Security Understanding	M11. I understand the role of security controls in protecting digital financial transactions.	.738
	M12. I am familiar with the 2FA security feature and understand its importance	.928
	M13. I understand the meaning and importance of data encryption	.866
	M14. I avoid carrying out financial transactions on public Wi-Fi	.450
	M15. I actively use 2FA / biometric login	.708
FL - Financial Literacy	M6. I understand concepts such as interest, inflation and investment risk	.604
	M7. I draw up a budget and try to stick to it	.808
	M8. I save regularly from my income	.743
	M9. I think before making an impulse purchase	.635
	M10. I compare the costs and benefits of financial products	.722
SE - Social Environment	M16. My family encourages me to be financially aware and secure	.673
	M17. My friends are aware of digital security	.786
	M18. My university provides financial security training or information	.742
	M19. My social environment supports saving and financial goals	.804

Note. EFA was conducted on the EFA subsample ($n = 917$). The extraction method was Principal Axis Factoring, and the rotation method was Promax. $KMO = .949$; Bartlett's $\chi^2(171) = 11,113.802$; $p < .001$; total variance explained = 62.143%. The factor loadings reported in the table are taken from the pattern matrix. The reverse-coded M20 item, which was initially included in the Social Environment dimension, was removed because it did not align with the expected factor structure and showed low communality with the relevant construct. Therefore, the final EFA solution consisted of four factors and 19 items.

Principal Axis Factoring produced the expected four-factor structure, and the reverse-coded M20 was removed for low communality with Social Environment (Hair et al., 2019).

Table 4. Reliability Analysis Results

Construct	Number of Items	Cronbach's alpha	Corrected item-total correlation range	Assessment
DFSB - Digital Financial Security Behavior	5	.883	.676–.763	Reliable
DSU - Digital Security Understanding	5	.894	.640–.791	Reliable
FL - Financial Literacy	5	.871	.652–.749	Reliable
SE - Social Environment	4	.871	.673–.788	Reliable

Note. The reliability analysis was conducted on the EFA subsample ($n = 917$). The reverse-coded M20 item was excluded from the reliability analysis because it had been removed from the scale structure following the EFA. Cronbach's alpha coefficients of .70 and above were considered acceptable indicators of internal consistency (Hair et al., 2019).

Cronbach's alpha coefficients ranged from .871 to .894, exceeding the commonly accepted .70 threshold for all constructs (Hair et al., 2019). Adjusted item-total correlations were positive and adequate, indicating that the items contributed consistently to their intended dimensions (Netemeyer et al., 2003). Therefore, the reliability analysis did not indicate the need to remove any additional items.

4.3. Confirmatory Measurement Model

Table 5 reports the confirmatory factor analysis fit indices.

Table 5. Confirmatory Factor Analysis Model Fit Indices

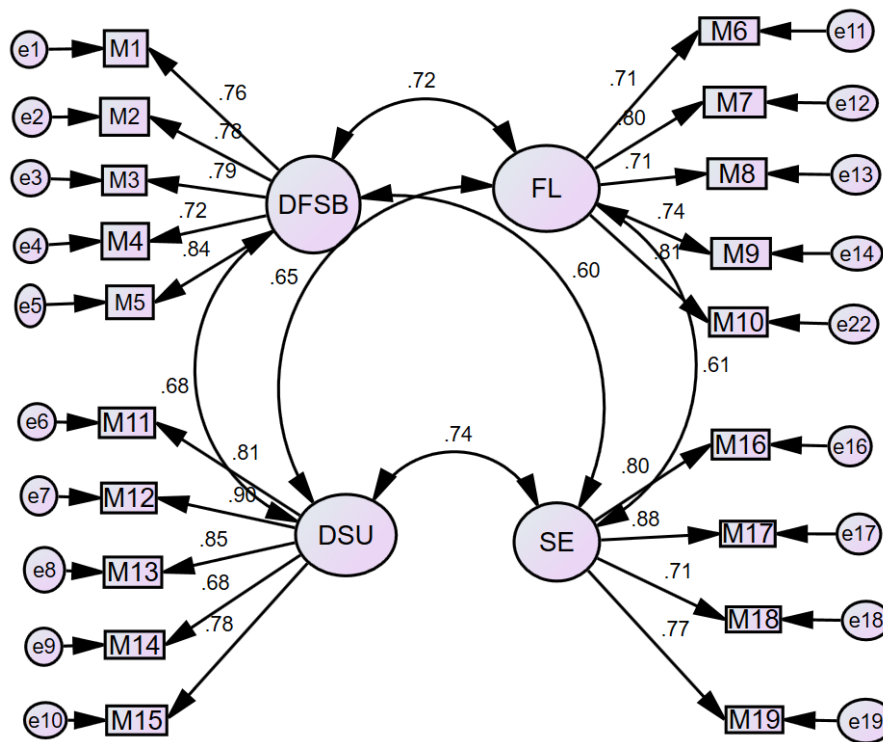
Fit index	Result	Acceptance criterion	Assessment
χ^2	626.571	-	Significance may be expected with a large sample size
df	146	-	-
χ^2/df	4.292	< 5	Acceptable
GFI	.925	> .90	Good
AGFI	.902	> .90	Good
NFI	.941	> .90	Good
IFI	.954	> .90 / > .95	Good
TLI	.946	> .90	Acceptable
CFI	.954	> .95	Good
RMSEA	.062	< .08	Acceptable
RMSEA 90% CI	.057–.067	< .08	Acceptable
Bollen-Stine bootstrap p	< .001	-	The hypothesis of perfect fit has been rejected

Note. CFA was conducted on the CFA/SEM subsample (n = 864) using Maximum Likelihood estimation. Because multivariate normality was not fully satisfied, the Bollen-Stine bootstrap test was applied with 2,000 bootstrap samples. Although the exact-fit hypothesis was rejected, the model was assessed as having adequate practical fit because the approximate fit indices were within acceptable limits. Model fit was evaluated using χ^2/df , CFI, TLI, GFI, AGFI, NFI, IFI and RMSEA together (Hair et al., 2019; Hu & Bentler, 1999). The acceptance criteria reported in Table 5 were based on Hair et al. (2019) and Hu and Bentler (1999).

The four-factor, 19-item structure obtained from the EFA was tested using CFA on the CFA/SEM subsample. The model showed acceptable practical fit, with $\chi^2/df = 4.292$, CFI = .954, TLI = .946 and RMSEA = .062. Although the Bollen-Stine bootstrap test rejected the exact-fit hypothesis, the approximate fit indices supported the adequacy of the measurement model given the sample size and Likert-type data structure (Bollen & Stine, 1992; Hair et al., 2019; Hu & Bentler, 1999).

The standardized CFA measurement model is presented in Figure 2, next page. As shown in Figure 2, all retained items loaded positively on their intended latent constructs. Table 6 reports the standardized factor loadings, composite reliability values and average variance extracted values.

Figure 2. Confirmatory Factor Analysis Measurement Model



Note. Standardized estimates are reported. DFSB = Digital Financial Security Behavior; FL = Financial Literacy; DSU = Digital Security Understanding; SE = Social Environment.

Table 6. CFA Factor Loadings, CR and AVE Results

Factor	Item	Standardized Factor Loading	R ²	CR	AVE	√AVE
DFSB - Digital Financial Security Behavior	M1	.760	.577	.885	.607	.779
	M2	.776	.602			
	M3	.792	.628			
	M4	.719	.517			
	M5	.844	.712			
DSU - Digital Security Understanding	M11	.815	.664	.903	.653	.808
	M12	.897	.805			
	M13	.853	.727			
	M14	.676	.458			
	M15	.783	.613			
FL - Financial Literacy	M6	.710	.504	.869	.572	.756
	M7	.803	.644			
	M8	.711	.506			
	M9	.738	.545			
	M10	.812	.659			
SE - Social Environment	M16	.804	.647	.870	.627	.792
	M17	.877	.770			
	M18	.713	.509			
	M19	.765	.586			

Note. CFA was conducted on the CFA/SEM subsample (n = 864). CR = Composite Reliability; AVE = Average Variance Extracted. √AVE values were used to assess discriminant validity. Standardized factor loadings and R² values were taken from the AMOS output. CR and AVE values were calculated based on the standardized factor loadings. CR and AVE values were used to assess convergent validity; thresholds of .70 for CR and .50 for AVE were considered (Fornell & Larcker, 1981; Hair et al., 2019).

Standardized factor loadings ranged from .676 to .897, and all retained items loaded adequately on their intended constructs. CR values ranged from .869 to .903, and AVE values ranged from .572 to .653, supporting internal consistency and convergent validity. Taken together, these results indicate that the four-factor measurement model was psychometrically adequate.

Table 7. Fornell-Larcker and HTMT Discriminant Validity Results

Panel A. Fornell-Larcker Criteria					Panel B. HTMT Results				
Factor	DFSB	DSU	FL	SE	Factor	DFSB	DSU	FL	SE
DFSB	.779				DFSB	-			
DSU	.679	.808			DSU	.692	-		
FL	.721	.650	.756		FL	.722	.667	-	
SE	.599	.741	.613	.792	SE	.605	.755	.624	-

Note. In Panel A, the diagonal values represent the square root of the AVE, while the values below the diagonal represent the intercorrelations between factors. In Panel B, the HTMT values are reported. HTMT values were calculated based on item correlations in the CFA subsample (n = 864). DFSB = Digital Financial Security Behavior; DSU = Digital Security Understanding; FL = Financial Literacy; SE = Social Environment.

Discriminant validity was assessed using the Fornell-Larcker criterion and the HTMT ratio. In the Fornell-Larcker results, the $\sqrt{\text{AVE}}$ value for each construct exceeded its correlations with the other constructs. The HTMT values were also below the .85 and .90 thresholds, with the highest value observed between Digital Security Understanding and Social Environment (HTMT = .755). These findings support discriminant validity (Fornell & Larcker, 1981; Henseler et al., 2015).

4.4. Descriptive Statistics and Correlations

Table 8 presents descriptive statistics and correlations for the dimensions.

Table 8. Descriptive Statistics and Correlations for the Dimensions

Variable	Mean	SD	1	2	3	4
DFSB	4.8828	1.7637	1			
FL	4.1246	1.6949	.659**	1		
DSU	5.0831	1.6558	.618**	.609**	1	
SE	4.8119	1.7115	.528**	.562**	.660**	1

Note. N = 1,781. DFSB = Digital Financial Security Behavior; FL = Financial Literacy; DSU = Digital Security Understanding; SE = Social Environment; SD = Standard deviation. **p < .01.

The construct means ranged from 4.1246 for Financial Literacy to 5.0831 for Digital Security Understanding. All inter-construct correlations were positive and statistically significant. Digital Financial Security Behavior was correlated with Financial Literacy (r = .659), Digital Security Understanding (r = .618) and Social Environment (r = .528).

4.5. Structural Model and Hypothesis Testing

Following the validation of the measurement model, the structural model was tested. Direct structural paths were specified from Financial Literacy, Digital Security Understanding and Social Environment to Digital Financial Security Behavior, and covariances between the exogenous variables

were permitted. Because the structural model retained the validated measurement model and was statistically equivalent to the CFA model in terms of global fit, the model fit indices are not repeated here. Instead, the structural model is evaluated based on the path coefficients, their statistical significance and the explained variance in Digital Financial Security Behavior.

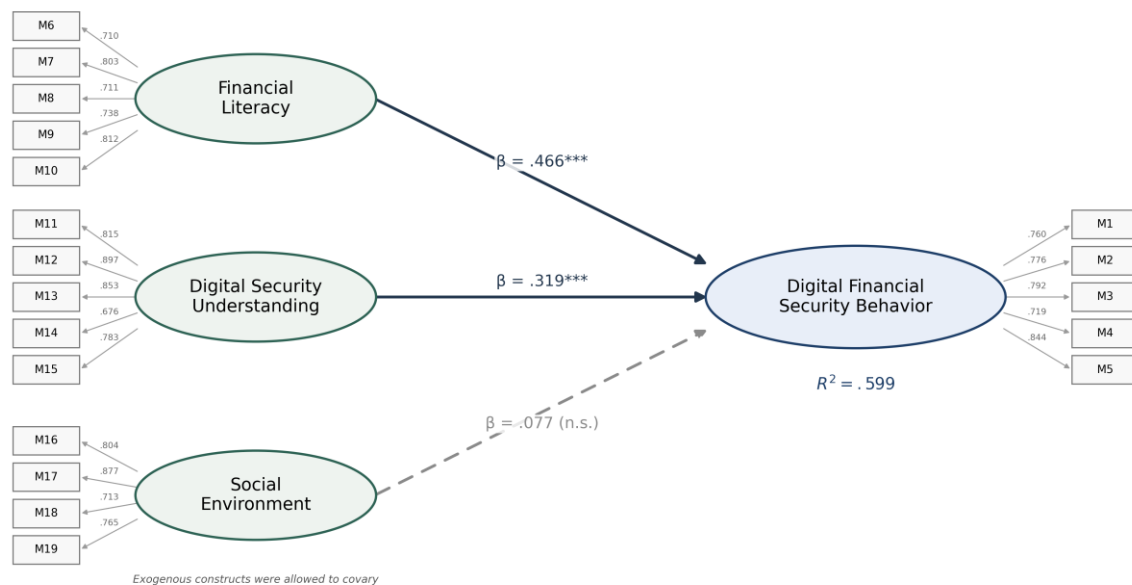
Table 9. Results of the Structural Model Hypothesis Test and Explained Variance

Hypothesis	Path	Standardized β	S.E.	C.R.	p	Conclusion
H1	FL $\rightarrow$ DFSB	.466	.053	10.316	< .001	Supported
H2	DSU $\rightarrow$ DFSB	.319	.051	6.449	< .001	Supported
H3	SE $\rightarrow$ DFSB	.077	.048	1.649	.099	Not supported
R^2 for DFSB						.599

Note. DFSB = Digital Financial Security Behavior; FL = Financial Literacy; DSU = Digital Security Understanding; SE = Social Environment. The β values represent standardized path coefficients. S.E. = Standard error; C.R. = Critical Ratio. The R^2 value indicates the combined explanatory power of FL, DSU and SE for DFSB.

The structural model with standardized estimates is presented in Figure 3.

Figure 3. Structural Model with Standardized Path Estimates



Note: Standardized measurement loadings and structural path estimates are reported. Error terms are omitted for visual clarity, and the exogenous constructs were allowed to covary. *** $p < .001$; n.s. = not significant. Estimates are based on the CFA/SEM subsample ($n = 864$).

The SEM results supported H1 and H2, whereas H3 was not supported. Although Social Environment was positively correlated with Digital Financial Security Behavior at the bivariate level, its direct effect weakened to non-significance once Financial Literacy and Digital Security Understanding were included. Financial Literacy was the strongest predictor of Digital Financial Security Behavior, followed by Digital Security Understanding, and the model explained 59.9% of the

variance. The sensitivity analysis excluding Mahalanobis outliers reproduced the same substantive pattern, indicating that the main findings were stable.

Table 10. Sensitivity Analysis Excluding Mahalanobis Multivariate Outliers

Panel A. Structural paths

Path	Main SEM β	Main SEM p	Sensitivity SEM B	S.E.	C.R.	Sensitivity SEM β	Sensitivity SEM p	Conclusion
FL $\rightarrow$ DFSB	.466	< .001	.580	.053	11.040	.489	< .001	Stable
DSU $\rightarrow$ DFSB	.319	< .001	.321	.053	6.023	.303	< .001	Stable
SE $\rightarrow$ DFSB	.077	.099	.074	.049	1.487	.071	.137	Not significant

Panel B. Explained variance

Model	N	R ² for DFSB
Main SEM model	864	.599
Sensitivity SEM excluding Mahalanobis outliers	802	.610

Note: FL = Financial Literacy; DSU = Digital Security Understanding; SE = Social Environment; DFSB = Digital Financial Security Behavior. The sensitivity model was estimated with 802 cases after excluding 62 cases flagged as multivariate outliers within the CFA/SEM subsample. p values are reported directly. B = unstandardized estimate; β = standardized estimate.

4.6. ANN-Based Robustness Analysis

Table 11 reports the ANN results.

Table 11. ANN-Based Robustness Analysis: Predictor Importance and Model Performance

Panel A. Predictor Importance

Predictor	Mean importance	SD	Normalized importance (%)
Financial Literacy	.435	.089	100.00
Digital Security Understanding	.293	.118	67.29
Social Environment	.030	.026	7.00

Panel B. Predictive Performance

Measure	Mean	SD
Training RMSE	1.174	.013
Testing RMSE	1.224	.119
Training R ²	.553	.011
Testing R ²	.500	.111

Note: The ANN analysis was conducted on the CFA/SEM subsample using construct-level mean scores for Financial Literacy, Digital Security Understanding and Social Environment as predictors of Digital Financial Security Behavior. The model was estimated in Google Colab using Python/scikit-learn's MLPRegressor. Model performance was evaluated using a 10-repeated 10-fold cross-validation procedure, producing 100 train-test iterations. Predictor importance was estimated using permutation importance based on R² reduction, with 30 permutations in each test fold. Normalized importance values were scaled relative to the most important predictor. RMSE = root mean square error. The ANN-based R² values refer to predictive performance and should not be interpreted as equivalent to SEM-based explained variance. The network used one hidden layer with three neurons, hyperbolic tangent activation, the L-BFGS solver, $\alpha = .0001$, and a maximum of 2,000 iterations.

Consistent with prior SEM–ANN applications in cybersecurity and fraud-safe behavior research (Chanda et al., 2025; Puri et al., 2025), the ANN results were used as a supplementary robustness check and were broadly consistent with the SEM findings. Financial Literacy had the highest normalized

importance score (100.00), followed by Digital Security Understanding (67.29), whereas Social Environment showed a much weaker contribution (7.00).

4.7. Measurement Invariance Analyses

As a psychometric robustness check, measurement invariance was assessed across gender, year level, and macro-academic field groups using multi-group CFA. Configural, metric, and scalar models were tested sequentially, and model comparisons were evaluated using $\Delta CFI \leq .010$ and $\Delta RMSEA \leq .015$. As shown in Table 12, scalar invariance was achieved across all three grouping variables, supporting the cross-group stability of the measurement structure. Measurement invariance was not tested across the original 13 department categories because of the large number of groups and the relatively small size of some departments.

Table 12. Summary of Measurement Invariance Results

Grouping variable	Highest level achieved	ΔCFI range	$\Delta RMSEA$ range	Decision
Macro-academic field	Scalar	.000 to -.001	-.001 to -.001	Achieved
Gender	Scalar	.000 to .007	.002 to .002	Achieved
Year level	Scalar	.000 to .004	.001 to .000	Achieved

Note: Measurement invariance was tested sequentially through configural, metric and scalar models using multi-group CFA. Model comparisons were evaluated using $\Delta CFI \leq .010$ and $\Delta RMSEA \leq .015$.

5. DISCUSSION AND CONCLUSION

This study examined Digital Financial Security Behavior as a protective post-adoption outcome rather than merely an extension of FinTech adoption intention. The findings show that secure digital financial behavior is mainly associated with Financial Literacy and Digital Security Understanding, whereas Social Environment does not have a statistically significant direct effect once these individual-level antecedents are considered simultaneously. This pattern supports the study's central conceptual distinction: adopting a digital financial service and using it securely are related but analytically different behavioral questions. The result is consistent with the Technology Threat-Avoidance Theory distinction between technology acceptance and threat-avoidance behavior and with behavioral information security research that treats users as active components of the security system.

The stronger role of Financial Literacy suggests that secure digital financial behavior is not merely a technical security issue. Many risky digital financial situations require financial judgment before a technical response is needed. Suspicious investment offers, misleading payment requests, impulsive online purchases, and fraud-related messages often exploit users' financial expectations rather than only their technical weaknesses. Students with stronger Financial Literacy may therefore be better positioned to question the economic logic of such situations before deciding how to act.

Digital Security Understanding also provides an important cognitive basis for secure behavior. Students may know how to use digital financial services, but safe use requires understanding security mechanisms, data protection, two-factor authentication, unsecured networks, and suspicious digital

interactions. At the same time, understanding a security mechanism does not automatically imply that users consistently engage in protective behavior; this distinction supports the study's separation of Digital Security Understanding from Digital Financial Security Behavior.

The non-significant direct path from Social Environment suggests that general social and institutional support may not be sufficient to produce secure digital financial behavior unless it is translated into concrete security norms, repeated warnings, practical guidance, or peer-level routines. This result does not rule out an indirect or conditional role for Social Environment, but it indicates that its direct contribution is weak when Financial Literacy and Digital Security Understanding are modeled simultaneously.

These findings align with work linking financial and digital financial literacy to safer digital financial conduct (OECD, 2025; Pak et al., 2026; Puri et al., 2025). They extend Sinha et al. (2025), whose outcome was service use rather than secure use, by showing that applied Financial Literacy predicts security-oriented behavior after adoption. The emergence of Financial Literacy as the strongest predictor likely reflects its judgment-based content, which helps students question suspicious claims, deceptive offers, and risky transaction contexts.

The positive role of Digital Security Understanding is consistent with protection-motivation, behavioral information security, and threat-avoidance perspectives (Crossler et al., 2013; Liang & Xue, 2009; Rogers, 1975, 1983). It also aligns with evidence that cyber-threat awareness and privacy/security concerns matter in digital payment contexts (Alalwan et al., 2024; Chanda et al., 2025). The partial divergence from Puri et al. (2025) may reflect differences in model structure, dependent variable, and construct operationalization.

The non-significant direct path from Social Environment requires careful interpretation. In technology acceptance research, social influence is commonly linked to behavioral intention, particularly under moderating conditions such as voluntariness, age, gender, and experience (Venkatesh et al., 2003). The present study instead examines protective post-adoption behavior among students who already frequently use digital financial services. This also contrasts with Supu et al. (2025), who identified a significant role of the social environment in financial fraud mitigation among accounting students, possibly due to differences in sample composition, measurement, and modeling strategies. Here, a broader faculty-level sample was used, and Financial Literacy, Digital Security Understanding, and Social Environment were modeled as latent constructs. Once individual cognitive and security-related predictors were included, Social Environment showed only a weak and non-significant direct path. This does not rule out an indirect or conditional role for Social Environment; rather, it suggests that future research should examine whether social support works through Financial Literacy, Digital Security Understanding, peer-level security norms, or institutional warning mechanisms.

Robustness checks supported the credibility of the findings: the ANN ranking reproduced the SEM order, the Mahalanobis sensitivity analysis showed that the pattern was not driven by outliers, and measurement invariance supported the cross-group stability of the measurement structure. Overall, the study contributes by treating secure post-adoption behavior as a distinct outcome and by testing Financial Literacy, Digital Security Understanding, and Social Environment within an integrated EFA–CFA–SEM framework.

The findings also have practical implications. Universities, financial institutions, and policymakers should not assume that frequent use of digital financial services automatically leads to safe use. Educational interventions should integrate financial literacy and digital security training rather than treating them as separate domains. Programs targeting young users should include practical modules on recognizing phishing, managing passwords, enabling two-factor authentication, using networks securely, protecting data privacy, and monitoring transactions. Social and institutional messaging should also move beyond general encouragement and provide clearer behavioral guidance regarding responsible digital financial practices.

This study has limitations. Its cross-sectional design prevents causal inference and does not rule out reverse causality; future studies should use longitudinal, experimental, or causal-inference designs. The higher proportion of female participants and voluntary sampling should be considered in generalizing the findings, although gender invariance and the absence of a gender difference in DFSB support interpretability. Department-level results remain exploratory because invariance was not tested across all 13 departments. Finally, although discriminant validity was supported, some Digital Security Understanding items border on enacted behavior; future research should more sharply separate knowledge-, awareness-, and behavior-based indicators and test alternative Financial Literacy specifications.

Overall, the study treats secure post-adoption behavior as a distinct outcome and tests the three antecedents within one framework integrating EFA, CFA, SEM, measurement invariance, sensitivity, and ANN robustness checks.

Ethics committee approval was obtained from the Ethics Committee of Süleyman Demirel University (Decision No. 179/24, 19 November 2025).

The author declares that the study was conducted in accordance with research and publication ethics.

The author confirms that AI tools were used only for language editing and translation purposes and were not involved in the generation of the study's scientific content.

The author declares that there are no financial conflicts of interest involving any institution, organization, or individual associated with this article.

REFERENCES

- Alalwan, A. A., Baabdullah, A. M., Al-Debei, M. M., Raman, R., Alhitmi, H. K., Abu-ElSamen, A. A., & Dwivedi, Y. K. (2024). Fintech and contactless payment: Help or hindrance? The role of invasion of privacy and information disclosure. *International Journal of Bank Marketing*, 42(1), 66–93. <https://doi.org/10.1108/IJBM-08-2022-0339>
- Ali, M., Raza, S. A., Khamis, B., Puah, C. H., & Amin, H. (2021). How perceived risk, benefit and trust determine user Fintech adoption: A new dimension for Islamic finance. *Foresight*, 23(4), 403–420. <https://doi.org/10.1108/FS-09-2020-0095>
- Al-Okaily, M. (2025). So what about the post-COVID-19 era?: Do users still adopt FinTech products? *International Journal of Human–Computer Interaction*, 41(2), 876–890. <https://doi.org/10.1080/10447318.2024.2305992>
- Alt, R., Beck, R., & Smits, M. T. (2018). FinTech and the transformation of the financial industry. *Electronic Markets*, 28(3), 235–243. <https://doi.org/10.1007/s12525-018-0310-9>
- Amnas, M. B., Selvam, M., Raja, M., Santhoshkumar, S., & Parayitam, S. (2023). Understanding the determinants of FinTech adoption: Integrating UTAUT2 with trust theoretic model. *Journal of Risk and Financial Management*, 16(12), 505. <https://doi.org/10.3390/jrfm16120505>
- Bajunaied, K., Hussin, N., & Kamarudin, S. (2023). Behavioral intention to adopt FinTech services: An extension of unified theory of acceptance and use of technology. *Journal of Open Innovation: Technology, Market, and Complexity*, 9(1), Article 100010. <https://doi.org/10.1016/j.joitmc.2023.100010>
- Bollen, K. A., & Stine, R. A. (1992). Bootstrapping goodness-of-fit measures in structural equation models. *Sociological Methods & Research*, 21(2), 205–229. <https://doi.org/10.1177/0049124192021002004>
- Bouteraa, M. (2024). Mixed-methods approach to investigating the diffusion of FinTech services: Enriching the applicability of TOE and UTAUT models. *Journal of Islamic Marketing*, 15(8), 2036–2068. <https://doi.org/10.1108/JIMA-12-2022-0343>
- Chanda, R. C., Vafaei-Zadeh, A., Hanifah, H., & Nikbin, D. (2025). Assessing cybersecurity awareness among bank employees: A multi-stage analytical approach using PLS-SEM, ANN, and fsQCA in a developing country context. *Computers & Security*, 149, Article 104208. <https://doi.org/10.1016/j.cose.2024.104208>
- Chen, F. F. (2007). Sensitivity of goodness of fit indexes to lack of measurement invariance. *Structural Equation Modeling: A Multidisciplinary Journal*, 14(3), 464–504. <https://doi.org/10.1080/10705510701301834>
- Cheung, G. W., & Rensvold, R. B. (2002). Evaluating goodness-of-fit indexes for testing measurement invariance. *Structural Equation Modeling: A Multidisciplinary Journal*, 9(2), 233–255. https://doi.org/10.1207/S15328007SEM0902_5
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90–101. <https://doi.org/10.1016/j.cose.2012.09.010>
- Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50. <https://doi.org/10.2307/3151312>
- Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage.
- Hassan, Md. S., Islam, Md. A., Abdullah, A. B. M., & Nasir, H. (2024). End-user perspectives on fintech services adoption in the Bangladesh insurance industry: The moderating role of trust. *Journal of Financial Services Marketing*, 29(4), 1377–1395. <https://doi.org/10.1057/s41264-024-00268-6>
- Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115–135. <https://doi.org/10.1007/s11747-014-0403-8>
- Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, 6(1), 1–55. <https://doi.org/10.1080/10705519909540118>
- Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration*, 11(4), 1–10. <https://doi.org/10.4018/ijec.2015100101>

- Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly*, 33(1), 71–90. <https://doi.org/10.2307/20650279>
- Netemeyer, R. G., Bearden, W. O., & Sharma, S. (2003). *Scaling procedures: Issues and applications*. Sage.
- Organisation for Economic Co-operation and Development. (2025). *Supporting informed and safe use of digital payments through digital financial literacy*. <https://doi.org/10.1787/21de47d1-en>
- Pak, T.-Y., Chatterjee, S., & Choung, Y. (2026). Navigating digital finance: How digital financial literacy influences digital financial services use and benefits in Korea. *Financial Innovation*, 12, Article 42, 1–33. <https://doi.org/10.1186/s40854-025-00820-w>
- Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879–903. <https://doi.org/10.1037/0021-9010.88.5.879>
- Puri, L., Kumar, A., & Singh, R. (2025). What drives or discourages fraud-safe behavior in digital transactions? A BRT perspective. *Acta Psychologica*, 260, Article 105675, 1–12. <https://doi.org/10.1016/j.actpsy.2025.105675>
- Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93–114. <https://doi.org/10.1080/00223980.1975.9915803>
- Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook* (pp. 153–176). Guilford Press.
- Shaikh, A. A., Glavee-Geo, R., Karjaluo, H., & Hinson, R. E. (2023). Mobile money as a driver of digital financial inclusion. *Technological Forecasting and Social Change*, 186, Article 122158, 1–14. <https://doi.org/10.1016/j.techfore.2022.122158>
- Singh, S., Sahni, M. M., & Kovid, R. K. (2020). What drives FinTech adoption? A multi-method evaluation using an adapted technology acceptance model. *Management Decision*, 58(8), 1675–1697. <https://doi.org/10.1108/MD-09-2019-1318>
- Sinha, G. R., Mehta, R. C., Kaattila, A., & Viitasalo, K. (2025). Factors and patterns in mobile banking and payment services use in the United States. *Journal of Financial Services Marketing*, 30, Article 26, 1–11. <https://doi.org/10.1057/s41264-025-00319-6>
- Supu, I. S., Karamoy, H., & Tangkuman, S. J. (2025). Pengaruh literasi keuangan, pemahaman SIA, dan lingkungan sosial terhadap mitigasi penipuan keuangan pada penggunaan transaksi digital mahasiswa akuntansi Universitas Sam Ratulangi Manado. *Manajemen Bisnis dan Keuangan Korporat*, 3(2), 554–567. <https://doi.org/10.58784/mbkk.393>
- Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 27(3), 425–478. <https://doi.org/10.2307/30036540>