How digital financial literacy helps mobile money users avoid fraud in Tanzania: A user survey and a practical framework for building resilience

Kelvin Andrew Mbuya

kevnps@gmail.com

College of Business Education, Tanzania

https://doi.org/10.51867/ajernet.7.4.121

ABSTRACT

Mobile money has deepened financial inclusion in Tanzania but has also exposed users to fraud, and because the user usually authorises the transaction, the user's own literacy and habits are the first line of defence. This study examined which digital-financial-literacy factors help mobile money users resist fraud and how that resilience can be built. This study is guided principally by theories of protective behaviour, Technology threat-avoidance theory and theory of planned behaviour. Using a cross-sectional quantitative survey with a design-science component, data from 650 mobile money users across urban and rural areas were analysed by reliability analysis, exploratory factor analysis, correlation and multiple linear regression. The instrument was reliable (Cronbach's alpha = 0.896), the data were factorable (Kaiser-Meyer-Olkin = 0.883; Bartlett's test, $p < 0.001$), and eleven factors explained 73.5% of the variance. Regression explained 15.9% of the variance in fraud resilience (adjusted R-squared = 0.146; $F(10, 639) = 12.11$, $p < 0.001$), with fraud awareness, social influence, security behaviour and self-efficacy as the significant predictors; information access and social influence were the lowest-scoring areas. The study concludes that the factors that most protect users, awareness and safe behaviour, are also among those users possess least, revealing an actionable gap. It recommends that providers, regulators, agents and educators deliver continuous, easy-to-reach fraud-awareness education and just-in-time safety reminders, especially for rural, older and less-literate users, alongside a practical user-resilience framework proposed by the study.

Keywords: Digital financial literacy, Mobile money fraud, Fraud awareness, User resilience, Financial inclusion, Tanzania

I. INTRODUCTION

Mobile money has transformed daily life in Tanzania, allowing millions to send, receive, save and spend money using a basic mobile phone (GSM Association [GSMA], 2024). Tanzania is among the regional leaders in this shift: mobile money accounts now outnumber traditional bank accounts, and the service has become the principal channel through which most Tanzanians, including previously unbanked rural and low-income households, participate in the formal financial system. This growth has brought genuine gains in financial inclusion, convenience and economic participation, and it is against this backdrop of rapid, large-scale adoption that the present study is set.

The same growth has, however, exposed users to fraud. Scams such as subscriber identity module (SIM) swap, in which a fraudster takes over a person's phone number, fake reversal messages, deceptive phone calls and dishonest agents increasingly target ordinary users (Pallangyo, 2022). A recent Tanzanian survey of 231 active mobile money users in Dar es Salaam and Kibaha found that 72.3% had been targeted by impersonation-based fraud attempts, and that 86.2% of those targeted were targeted repeatedly (Aloyce et al., 2026), evidence that fraud exposure is not a marginal concern but a routine feature of using mobile money in Tanzania today. Because the user initiates the transaction and holds the personal identification number (PIN) and one-time password (OTP), the user is usually the point the fraudster tries to exploit, which is precisely why this study approaches the problem from the user's side rather than from the provider's or the regulator's.

This places the user's own knowledge and habits at the centre of staying safe. People who understand money manage it better (Lusardi & Mitchell, 2014), and in a digital economy that understanding must extend to digital financial literacy: how digital services work, what they cost, and how to use them safely (Morgan et al., 2019; Organisation for Economic Co-operation and Development [OECD], 2020). Whether a person behaves safely also depends on how serious they judge the threat and how capable they feel of protecting themselves, as protection-motivation and threat-avoidance theories explain (Rogers, 1975; Liang & Xue, 2009), and on their attitudes and the advice of those around them (Ajzen, 1991), as well as basic digital skill (van Deursen & van Dijk, 2011). This study is accordingly guided by protection-motivation and technology threat-avoidance theory, complemented by the theory of planned behaviour, and it uses these theories to identify the specific knowledge, awareness, behaviour, skill, attitude and access factors expected to shape whether a mobile money user in Tanzania can resist fraud; the theoretical basis for each is set out fully in Section 2.1.

© 2026 Author(s). This article is licensed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0).

Mobile money in Tanzania links four kinds of player: the user, whose wallet is tied to a phone number; agents, the kiosks where cash is deposited and withdrawn; the mobile network operator (MNO), which runs the wallet system; and banks, which settle transfers (GSMA, 2024). Fraud enters this chain at its weakest points, usually people, and most often the user, through SIM-swap, scam calls and messages that extract a PIN or OTP, dishonest agents who run fake reversals, and phishing (Pallangyo, 2022). These acts are offences under the Cybercrimes Act, 2015 (United Republic of Tanzania, 2015), but pursuing the fraudster rarely recovers the user's money, which is why prevention at the point of use, rather than prosecution after the fact, is the more realistic route to protecting users.

This study therefore sets out to assess what makes mobile money users in Tanzania able to resist fraud, to measure this directly among real users, to identify which factors matter most, and to translate the findings into a practical framework for building user resilience. Its research aim is to determine which digital-financial-literacy, risk-appraisal and social-support factors most strongly predict mobile money users' fraud resilience in Tanzania, and to use that evidence to propose concrete, evidence-based steps that providers, regulators, agents, educators and users themselves can take to close the gaps the evidence reveals.

1.1 Problem Statement

The problem is consequential because the scale is large. As mobile money use has grown, even a small proportion of successful fraud produces heavy losses and erodes the trust on which financial inclusion depends (GSMA, 2024). The heaviest losses fall on poorer, less-educated and rural users, who can least afford them and are often least prepared to detect a scam. Providers and regulators deploy technical and legal safeguards, but these are insufficient alone, because the final decision, to share a code, approve a transfer or hand cash to an agent, rests with the user. Yet most studies focus on what banks, providers or law enforcement can do, not on the user as a line of defence, and few measure what makes an ordinary user able to resist fraud or translate the findings into a practical plan for the East African setting (Pallangyo, 2022). This study addresses that gap.

1.2 Objectives

The study pursued four objectives: (i) to identify the knowledge, awareness, behaviour, skill, attitude and access factors that help mobile money users resist fraud; (ii) to measure these factors among real users; (iii) to determine which of them matter most for fraud resilience; and (iv) to translate the findings into a practical framework for building user resilience.

1.3 Research Hypotheses

Guided by protection-motivation, threat-avoidance and planned-behaviour theory (Rogers, 1975; Liang & Xue, 2009; Ajzen, 1991), the study tested ten directional hypotheses, each predicting a positive effect on users' fraud resilience, at alpha = 0.05, the conventional social-science threshold:

H1: Digital financial literacy positively influences fraud resilience.
H2: Fraud awareness positively influences fraud resilience.
H3: Security behaviour positively influences fraud resilience.
H4: Digital skills positively influence fraud resilience.
H5: Risk perception positively influences fraud resilience.
H6: Self-efficacy positively influences fraud resilience.
H7: Caution and skepticism positively influence fraud resilience.
H8: Social influence positively influences fraud resilience.
H9: Information access positively influences fraud resilience.
H10: Safety attitude positively influences fraud resilience.

II. LITERATURE REVIEW

2.1 Theoretical Framework

2.1.1 Protection Motivation and Technology Threat-Avoidance Theories

This study is guided principally by theories of protective behaviour, because knowing about a risk is not the same as acting on it. Protection motivation theory holds that people take protective action when they believe a threat is real and serious and that they can do something about it (Rogers, 1975); this underpins the study's risk-perception and self-efficacy constructs. Technology threat-avoidance theory extends the same logic to information-technology threats, describing how users appraise a threat and their coping ability before acting (Liang & Xue, 2009). These theories are well established but were developed largely in high-income settings; their application to low-literacy, agent-mediated mobile money in East Africa is what this study examines.

© 2026 Author(s). This article is licensed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0).

2.1.2 Theory of Planned Behaviour

The theory of planned behaviour adds that attitudes, subjective norms (the views of others), and perceived behavioural control shape what people actually do (Ajzen, 1991). This motivates the study's measures of safety attitude, social influence, and caution. Together these theories frame fraud resilience as the product of threat appraisal, coping capacity and social context, which the study operationalises through its constructs.

2.2 Empirical Review

2.2.1 Factors in User Fraud Resilience

Financial literacy, the knowledge and skill to make sound money decisions, is consistently linked to better financial outcomes; Lusardi and Mitchell (2014), synthesising survey evidence across many countries, found that financial literacy is generally low, unevenly distributed by education, gender and income, and a reliable predictor of sound financial behaviour, though their focus is general personal finance rather than fraud resistance specifically. As money becomes digital, this literacy must extend into digital financial literacy, covering how digital services work, what they cost and how to use them safely; Morgan et al. (2019), in a policy analysis for the Asian Development Bank Institute, argued that digital financial literacy is a distinct competence combining financial and digital skill, and identified risk awareness and self-protection knowledge as core components, a conceptual claim the present study tests empirically. Applying protection motivation theory directly to a security context, Arachchilage et al. (2016) found in an experimental study that threat perception, perceived severity, perceived susceptibility and self-efficacy all positively predicted phishing-avoidance behaviour, while the perceived cost of taking protective action predicted it negatively, a pattern this study expects to extend to mobile money fraud. Studies of everyday digital use show that people often manage the mechanics of a service but struggle to judge information, which is precisely the weakness fraud exploits (van Deursen & van Dijk, 2011). Most directly relevant, Aloyce et al. (2026), surveying 231 active mobile money users in Dar es Salaam and Kibaha alongside key-informant interviews, found impersonation-based fraud pervasive, with 72.3% of users targeted, and identified user compliance with fraudulent requests as shaped by awareness gaps and situational pressure rather than by access to technology, directly supporting this study's user-centred, literacy-based framing. Together, these studies agree that knowledge, awareness, safe behaviour and digital skill jointly shape whether a user can resist deception, though only Aloyce et al. (2026) tests this directly among Tanzanian mobile money users, and none measures the full set of literacy, appraisal and social-support factors together, which is the gap this study fills.

2.2.2 Measuring Digital Financial Literacy and Related Constructs

National and cross-country surveys now measure adult financial literacy and its digital dimension; the OECD's (2020) international financial literacy survey established standardised instruments covering knowledge, attitudes and behaviour, showing these are distinct, measurable competencies rather than a single trait, while Morgan et al. (2019) proposed that digital financial literacy additionally requires measuring digital-service-specific knowledge, risk awareness and self-protection ability. Nyamwihula (2024), surveying Airtel Money users in Tanzania on cybersecurity awareness, found a marked lack of formal security training, with most users' knowledge coming informally from provider security tips rather than structured education, and documented clear demand for structured training, a measurement gap this study's training-relevant constructs help address. However, most standardised instruments, including the OECD's, were designed for banking contexts in high-income countries; few are adapted to agent-based mobile money or to the specific behaviours that resist SIM-swap, OTP-sharing and fake-reversal fraud, and Nyamwihula's (2024) study, while Tanzania-specific, is confined to a single provider and does not measure the broader set of literacy, risk-appraisal and social constructs this study operationalises directly.

2.2.3 Determinants of Fraud Vulnerability and Resilience

Evidence indicates that risk is unevenly distributed: digital skills track age and education (van Deursen & van Dijk, 2011), and weak financial knowledge is more common among women, older people and the less-schooled (Lusardi & Mitchell, 2014). In mobile money, rural, older and less-literate users rely more on agents and intermediaries, which can expose them to dishonest agents and to sharing secret codes (Pallangyo, 2022). Aloyce et al. (2026) add a determinant seldom captured elsewhere: 86.2% of Tanzanian users targeted by impersonation fraud were targeted repeatedly, indicating that prior victimisation, and whatever accompanying situational or trust-based vulnerability produces it, is itself a determinant of continued exposure rather than fraud being a one-off, randomly distributed event. Arachchilage et al. (2016) isolate self-efficacy and perceived severity as independent, significant determinants of avoidance behaviour once other factors are controlled, which motivates testing self-efficacy as a distinct predictor here rather than folding it into general awareness. Studies agree that vulnerability is patterned by demographic and situational factors, but they seldom isolate which user-level factors most strongly predict resilience once others are held constant in a single model, which this study tests directly.

© 2026 Author(s). This article is licensed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0).

2.2.4 Building User Resilience

Consumer-education and awareness interventions can raise safe behaviour: Arachchilage et al. (2016) found that an educational mobile game intervention grounded in protection motivation theory raised participants' phishing-avoidance behaviour by 28% in a post-test, concrete evidence that theory-based education measurably improves resilience rather than merely raising awareness in principle. Nyamwihula (2024) found Tanzanian mobile money users wanted structured workshops and training programmes beyond the informal tips currently provided, indicating clear demand for exactly this kind of intervention in the Tanzanian context. Design-science research offers a structured way to turn such evidence into practical, evaluable artefacts such as frameworks (Hevner et al., 2004; Peffers et al., 2007), which this study adopts to build its resilience framework. Yet few resilience frameworks are grounded in direct, multi-construct measurement of user-level determinants in an African mobile-money setting: Aloyce et al. (2026) document the problem in Tanzania but do not propose a framework, and Nyamwihula (2024) is confined to one provider, leaving education efforts without a validated, evidence-based framework tuned to the factors that matter most across the wider mobile money ecosystem, which is the contribution this study makes.

2.3 Research Gap

The literature establishes that user knowledge, awareness, behaviour and social context shape protective action, and that vulnerability is unevenly distributed. What is missing is direct, user-level measurement of the digital-financial-literacy factors that predict fraud resilience among mobile money users in East Africa, and a practical, evidence-based framework built on those findings. Prior work centres on providers, banks or law enforcement, or on financial literacy in general, rather than on the user as a line of defence against mobile money fraud. This study addresses that gap.

2.4 Conceptual Framework

The study models ten predictor constructs and one outcome. Digital financial literacy, fraud awareness, security behaviour and digital skills capture what users know and do; risk perception, self-efficacy, caution and skepticism, and safety attitude capture how they appraise risk; social influence and information access capture the support around them; and fraud resilience is the outcome. Each predictor is hypothesised to have a positive effect on fraud resilience (H1-H10). The framework is shown in Figure 1, and each construct is defined operationally in Appendix A.

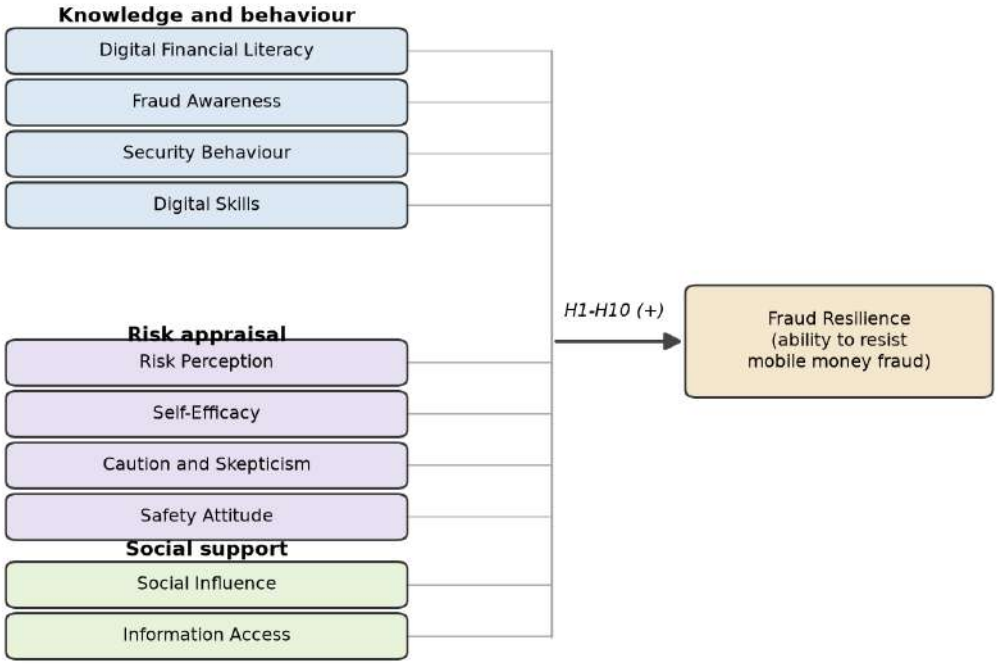


Figure 1. Conceptual framework linking digital-financial-literacy, risk-appraisal and social-support constructs to mobile money fraud resilience.

© 2026 Author(s). This article is licensed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0).

III. METHODOLOGY

3.1 Research Design

The study adopted a cross-sectional, quantitative survey design with a deductive approach, complemented by a design-science strand that produced the practical framework (Creswell & Creswell, 2018; Saunders et al., 2019; Hevner et al., 2004; Peffers et al., 2007). This design suited the objectives because the study measured defined constructs across many users at one point in time and tested hypothesised relationships with fraud resilience, which calls for standardised measurement and statistical analysis. The design was theory-guided by protection-motivation, threat-avoidance and planned-behaviour theory (Rogers, 1975; Liang & Xue, 2009; Ajzen, 1991).

3.2 Study Area

The study was conducted in Tanzania, covering both urban and rural areas so as to capture the range of mobile money users, from town-based users with easier access to information to rural users who rely more heavily on agents. This urban-rural coverage was important because vulnerability to fraud is expected to differ across these settings.

3.3 Target Population

The target population was adult mobile money users in Tanzania, who number in the tens of millions (GSMA, 2024). Users were the unit of analysis because it is the user who authorises transactions and holds the PIN and OTP, and therefore whose literacy and behaviour determine fraud resilience.

3.4 Sampling and Sample Size

Because the population is very large, the Yamane formula (Yamane, 1967), a common alternative to the Krejcie and Morgan table (Krejcie & Morgan, 1970), indicates that a few hundred respondents suffice at 95% confidence (e = 0.05), since for a large N the required sample approaches 1/e^2, that is about 400. Data collection continued until 650 valid responses were obtained, exceeding this minimum and improving statistical power. Respondents were reached through convenience and snowball sampling to include a range of ages, genders, education levels, and both urban and rural residents; the reliance on non-probability sampling is acknowledged as a limitation.

3.5 Data Collection Instruments and Procedures

Data were collected using a structured questionnaire measuring eleven constructs with 43 five-point Likert items (1 = strongly disagree to 5 = strongly agree): digital financial literacy, fraud awareness, security behaviour, digital skills, risk perception, self-efficacy, caution and skepticism, social influence, information access, safety attitude, and the outcome, fraud resilience. Items were grounded in the reviewed literature and worded in simple, everyday language so any user could respond; the full instrument is in Appendix A. The questionnaire opened with an informed-consent statement and collected no names or phone numbers. Content validity was established by mapping each item to a defined construct; the factor structure was examined by exploratory factor analysis; and internal consistency was assessed with Cronbach's alpha (Cronbach, 1951; Field, 2018) against the 0.70 threshold (Nunnally & Bernstein, 1994), with an overall alpha of 0.896 and construct alphas of 0.828 to 0.916.

3.6 Data Analysis

Data were analysed with descriptive statistics; reliability analysis; exploratory factor analysis using the Kaiser-Meyer-Olkin measure (Kaiser, 1974) and Bartlett's test (Bartlett, 1950); Pearson correlation; and multiple linear regression at alpha = 0.05, with confidence intervals and effect sizes reported (Field, 2018; Hair et al., 2019; Tabachnick & Fidell, 2019). The analysis was fully scripted and is reproducible.

3.7 Ethical Considerations

The study observed informed consent, voluntary participation, anonymity and confidentiality, in compliance with the Personal Data Protection Act, 2022 (United Republic of Tanzania, 2022). Data were collected between February and July 2026 from consenting mobile money users; no names or phone numbers were recorded, and all responses were aggregated before analysis. The study was conducted under the academic framework of the College of Business Education, with consent obtained through the questionnaire's consent statement.

IV. FINDINGS AND DISCUSSION

4.1 Respondent Profile

The sample comprised 650 mobile money users. By gender, 51.8% were male and 48.2% female. By age, 28.6% were 26-35, 25.1% were 36-45, 20.5% were 18-25, 18.2% were 46-60 and 7.7% were above 60. By education, 30.0% held a certificate or diploma, 27.7% had secondary education, 26.8% had a university education or above, and 15.5% had primary education or less. By residence, 55.7% were rural and 44.3% urban. Most were frequent users: 56.0% used

© 2026 Author(s). This article is licensed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0).

mobile money daily and 25.4% weekly, with a mean of 7.29 years of use (SD = 3.16). The age distribution is detailed in Table 1.

Table 1. Respondent Distribution by Age Group (n = 650)

Age Group	n	%
26-35	186	28.6%
36-45	163	25.1%
18-25	133	20.5%
46-60	118	18.2%
Above 60	50	7.7%

4.2 Level and Structure of the Digital-Financial-Literacy Factors

Table 2 reports the mean, standard deviation and range for each of the eleven constructs, on a 1-to-5 scale. Digital skills recorded the highest mean (M = 4.02, SD = 0.70), followed by security behaviour (M = 3.96, SD = 0.57), digital financial literacy (M = 3.92, SD = 0.69), risk perception and caution/skepticism (both M = 3.89), safety attitude (M = 3.81, SD = 0.51), fraud awareness (M = 3.67, SD = 0.60) and self-efficacy (M = 3.58, SD = 0.60). Social influence (M = 3.41, SD = 0.56) and, most markedly, information access (M = 2.93, SD = 0.64) were the lowest-scoring constructs, indicating that users feel comparatively well equipped in their own digital and security skills but receive far less support and information from their social and institutional environment. Fraud resilience, the outcome construct, averaged M = 3.59 (SD = 0.57).

Table 2. Descriptive Statistics for the Eleven Constructs (1 to 5 Scale)

Construct	Mean	SD	Min	Max
Digital Financial Literacy	3.92	0.69	2.00	5.00
Fraud Awareness	3.67	0.60	1.75	5.00
Security Behaviour	3.96	0.57	2.00	5.00
Digital Skills	4.02	0.70	1.50	5.00
Risk Perception	3.89	0.53	2.25	5.00
Self Efficacy	3.58	0.60	1.00	5.00
Caution Skepticism	3.89	0.55	2.25	5.00
Social Influence	3.41	0.56	2.00	5.00
Information Access	2.93	0.64	1.00	4.67
Safety Attitude	3.81	0.51	2.00	5.00
Fraud Resilience	3.59	0.57	2.00	5.00

The overall 43-item scale was reliable (Cronbach's alpha = 0.896). Table 3 reports the per-construct alphas: digital skills recorded the highest (alpha = 0.916), followed by digital financial literacy (alpha = 0.906), fraud awareness (alpha = 0.883), self-efficacy (alpha = 0.881), information access (alpha = 0.867), security behaviour and social influence (both alpha = 0.866), fraud resilience (alpha = 0.862), caution and skepticism (alpha = 0.859), risk perception (alpha = 0.847), and safety attitude, the lowest (alpha = 0.828). All eleven constructs met or exceeded the conventional 0.70 threshold (Cronbach, 1951; Nunnally & Bernstein, 1994).

Table 3. Reliability of the Construct Scales

Construct	Items	Cronbach's alpha
Digital Financial Literacy	4	0.906
Fraud Awareness	4	0.883
Security Behaviour	4	0.866
Digital Skills	4	0.916
Risk Perception	4	0.847
Self Efficacy	4	0.881
Caution Skepticism	4	0.859
Social Influence	4	0.866
Information Access	3	0.867
Safety Attitude	4	0.828
Fraud Resilience	4	0.862

The data were well suited to factoring (Kaiser-Meyer-Olkin measure of sampling adequacy = 0.883; Bartlett's test of sphericity, $p < 0.001$; Kaiser, 1974; Bartlett, 1950), and exploratory factor analysis using the Kaiser criterion

© 2026 Author(s). This article is licensed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0).

returned 11 factors explaining 73.5% of the variance, matching the eleven intended constructs and supporting the instrument's construct validity (Hair et al., 2019).

4.3 Determinants of Fraud Resilience

Table 4 reports the Pearson correlation of each of the ten predictor constructs with fraud resilience. All ten correlations were positive and statistically significant ($p < 0.01$). Fraud awareness showed the strongest association ($r = 0.316$), followed by digital skills ($r = 0.254$), self-efficacy ($r = 0.232$), digital financial literacy ($r = 0.213$), security behaviour ($r = 0.205$), social influence ($r = 0.181$), information access ($r = 0.168$), caution and skepticism ($r = 0.085$), risk perception ($r = 0.079$), and safety attitude, the weakest association ($r = 0.055$). Most coefficients indicate small-to-moderate associations by conventional benchmarks.

Table 4. Pearson Correlation of Each Construct with Fraud Resilience

Construct	r
Fraud Awareness	0.316
Digital Skills	0.254
Self Efficacy	0.232
Digital Financial Literacy	0.213
Security Behaviour	0.205
Social Influence	0.181
Information Access	0.168
Caution Skepticism	0.085
Risk Perception	0.079
Safety Attitude	0.055

A multiple linear regression was fitted with fraud resilience as the dependent variable and the ten constructs, entered as standardized predictors, as independent variables. The model was statistically significant and explained 15.9% of the variance in fraud resilience (R-squared = 0.159, adjusted R-squared = 0.146; $F(10, 639) = 12.11$, $p < 0.001$). Table 5 reports the full set of standardized coefficients. Four predictors were statistically significant: fraud awareness (beta = 0.212, $t = 5.04$, $p < 0.001$, 95% CI [0.13, 0.29]), social influence (beta = 0.110, $t = 2.90$, $p = 0.004$, 95% CI [0.04, 0.18]), security behaviour (beta = 0.103, $t = 2.60$, $p = 0.009$, 95% CI [0.03, 0.18]), and self-efficacy (beta = 0.085, $t = 2.00$, $p = 0.045$, 95% CI [0.00, 0.17]). The remaining six predictors were not statistically significant in the multivariate model: digital skills (beta = 0.080, $t = 1.61$, $p = 0.108$), caution and skepticism (beta = 0.037, $t = 0.95$, $p = 0.344$), information access (beta = 0.032, $t = 0.79$, $p = 0.431$), digital financial literacy (beta = 0.016, $t = 0.33$, $p = 0.741$), risk perception (beta = 0.012, $t = 0.31$, $p = 0.753$), and safety attitude (beta = -0.023, $t = -0.60$, $p = 0.545$). Hypotheses H2 (fraud awareness), H8 (social influence), H3 (security behaviour) and H6 (self-efficacy) were therefore supported; H1, H4, H5, H7, H9 and H10 were not supported.

Table 5. Multiple Linear Regression Predicting Fraud Resilience (Standardized)

Predictor	Beta	t	p	95% CI	Hypothesis
Fraud Awareness	0.212	5.04	< .001	[0.13, 0.29]	Supported
Social Influence	0.110	2.90	0.004	[0.04, 0.18]	Supported
Security Behaviour	0.103	2.60	0.009	[0.03, 0.18]	Supported
Self Efficacy	0.085	2.00	0.045	[0.00, 0.17]	Supported
Digital Skills	0.080	1.61	0.108	[-0.02, 0.18]	Not supported
Caution Skepticism	0.037	0.95	0.344	[-0.04, 0.12]	Not supported
Information Access	0.032	0.79	0.431	[-0.05, 0.11]	Not supported
Digital Financial Literacy	0.016	0.33	0.741	[-0.08, 0.11]	Not supported
Risk Perception	0.012	0.31	0.753	[-0.06, 0.09]	Not supported
Safety Attitude	-0.023	-0.60	0.545	[-0.10, 0.05]	Not supported

Comparing the correlation and regression results shows a clear narrowing: although all ten constructs correlated positively and significantly with fraud resilience on their own (Table 4), only four retained independent significance once all ten were considered together (Table 5), consistent with the predictors sharing overlapping variance. The four significant predictors concern awareness and everyday protective behaviour and belief in one's own ability to cope, while the two lowest-scoring constructs in Table 2, information access and social influence, sit on opposite sides of this pattern: social influence is a significant driver despite its low mean score, whereas information access is not significant

© 2026 Author(s). This article is licensed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0).

despite being similarly low, indicating that the social-support gap is more consequential for resilience than the information-access gap once other factors are held constant.

4.4 A Practical Framework for Building User Resilience (Objective 4)

Building on these findings and on design science (Hevner et al., 2004; Peffers et al., 2007), the study proposes a practical framework of steps to help users resist mobile money fraud, grouped around knowledge, habits and support. Table 6 lists each component, its function and the concern it addresses. Each component responds to a gap identified in the survey, building safety at the point where attacks actually occur, the user, alongside the technical and legal safeguards that providers and the state already operate. The framework is offered as preliminary and not independently validated beyond the empirical analysis that produced it.

Table 6. User-Resilience Framework Components and the Concerns They Address

Component	Function	Addresses
Digital financial literacy education	Teaches how services, charges and risks work	Literacy
Fraud-awareness campaigns	Explain current scam types in plain language	Awareness
Protective-behaviour prompts	Reinforce PIN/OTP secrecy and verify-before-acting habits	Behaviour
Digital-skills support	Helps users transact safely on apps and USSD	Skills
Just-in-time warnings	Provider nudges at moments of transaction risk	Caution
Community and peer channels	Uses family, agents and community to spread safe practice	Social influence
Accessible reporting and support	Easy ways to report, block and seek help	Access, self-efficacy
Agent conduct and monitoring	Trains and monitors agents to reduce agent-assisted fraud	Behaviour
Inclusive design	Reaches rural, older and less-literate users	Equity

4.5 Discussion

Bringing the findings together, the level, determinant and framework results are discussed here against the theoretical and empirical literature reviewed in Section II. The finding that fraud awareness, social influence, security behaviour and self-efficacy are the significant, independent drivers of resilience is consistent with protection-motivation and threat-avoidance theory, which hold that people act safely when they take a threat seriously and feel able to cope (Rogers, 1975; Liang & Xue, 2009), and it closely parallels Arachchilage et al.'s (2016) experimental finding that threat perception, self-efficacy and perceived severity independently predict phishing-avoidance behaviour: this study extends that laboratory-based finding to real mobile money users in a field survey, and confirms self-efficacy as an independent driver in this setting as well.

The prominence of fraud awareness supports the digital-financial-literacy argument that safe digital-money use is a distinct, learnable competence (Morgan et al., 2019; OECD, 2020), and it extends this literature to the specific case of agent-mediated mobile money fraud in Tanzania, where Aloyce et al. (2026) documented pervasive impersonation-based fraud (72.3% of users targeted) and Nyamwihula (2024) documented weak formal security training among Airtel Money users: the present study's finding that awareness, not general digital financial literacy or risk perception, is what most differentiates more from less resilient users refines both studies by pinpointing awareness specifically, rather than literacy or perceived risk in general, as the lever that matters most.

The most notable and theoretically interesting result is a mismatch: the factors that most protect users, fraud awareness, social influence and everyday protective behaviour, are significant drivers of resilience, yet information access and social influence are, together with fraud awareness itself only moderately rated, among the lowest-scoring constructs in the sample (Table 2). In other words, the capacities that protect users most are, for social influence in particular, among the capacities users possess least, a pattern that contrasts with technology-centred accounts of fraud prevention and points instead to an education-and-social-support gap. Because digital skills and money knowledge are typically strongest among younger, more educated and urban users (Lusardi & Mitchell, 2014; van Deursen & van Dijk, 2011), and because Aloyce et al. (2026) found that most targeted users in Tanzania were targeted repeatedly, this gap is likely to fall hardest on rural, older, less-literate and previously victimised users, for whom agents and trusted community voices are the most credible sources of safety guidance. The encouraging implication, reinforced by Arachchilage et al.'s (2016) finding that a short educational intervention raised avoidance behaviour by 28%, is that resilience can be raised not by more technology but by closing the awareness-and-social-support gap through steady,

© 2026 Author(s). This article is licensed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0).

reachable, theory-based education alongside existing safeguards, exactly the kind of structured training Nyamwihula (2024) found Tanzanian users already wanted.

Taken together, these findings support the study's central contribution: that mobile money fraud resilience in Tanzania is most strongly and consistently driven by fraud awareness, social influence, security behaviour and self-efficacy, while the areas users are least equipped in, information access and social influence, are precisely where intervention is most needed. The proposed framework (Section 4.4) operationalises this conclusion by prioritising awareness, behaviour and social-support-building interventions over generic digital-literacy training alone, in the spirit of design science research (Hevner et al., 2004; Peffers et al., 2007), and directly answers the calls in Aloyce et al. (2026) and Nyamwihula (2024) for a validated, evidence-based response to mobile money fraud in the Tanzanian context.

V. CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

This study examined the digital-financial-literacy factors that help mobile money users in Tanzania resist fraud and translated the findings into a practical framework. Using a quantitative survey of real users and a design-science approach, it found that fraud awareness, social influence, security behaviour and self-efficacy are the significant determinants of fraud resilience, while information access and social influence are the largest gaps. The study's contribution is a validated user-level instrument, evidence on which factors most protect users, and an evidence-based resilience framework. Limitations include the non-probability (convenience and snowball) sampling, the cross-sectional self-report design that captures perceived rather than tested resilience, and the modest explained variance, indicating that other factors also matter.

5.2 Recommendations

The findings translate into stakeholder-specific actions (Table 7). Mobile money providers should run continuous fraud-awareness messaging and just-in-time warnings at the point of transaction; regulators should mandate consumer-protection and financial-education standards; agents should be trained and monitored and used as trusted safety educators; educators and civil society should deliver digital financial literacy, especially to rural, older and less-literate users; and users and communities should keep PINs and OTPs secret, verify before acting, and share warnings. Future research should confirm the measurement model, use probability sampling, and pilot targeted education to test whether it measurably reduces fraud victimisation.

Table 7. Recommendations by Stakeholder

Stakeholder	Recommended action
Mobile money providers (MNOs)	Run continuous fraud-awareness messaging and just-in-time warnings
Bank of Tanzania / regulators	Mandate consumer-protection and financial-education standards
Agents and agent networks	Train and monitor agents; use them as trusted safety educators
Educators and civil society	Deliver digital financial literacy, especially to rural and older users
Users and communities	Adopt PIN/OTP secrecy, verify-before-acting and share warnings

Conflict of Interest

The author declares no conflict of interest. The research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Acknowledgement

The author thanks the survey participants and colleagues at the College of Business Education. The anonymized dataset, codebook, data dictionary, analysis scripts and computed results are available from the corresponding author on reasonable request.

REFERENCES

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211. https://doi.org/10.1016/0749-5978(91)90020-T

© 2026 Author(s). This article is licensed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0).

Aloyce, G., Budoya, C., & Tesha, G. S. (2026). Impersonation-based fraud in mobile money transactions: Prevalence, patterns, and predictors of user compliance in Tanzania. *East African Journal of Information Technology, 9*(2), 178-188. https://journals.eanso.org/index.php/eajit/article/view/5694

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior, 60*, 185-197. https://doi.org/10.1016/j.chb.2016.02.065

Bartlett, M. S. (1950). Tests of significance in factor analysis. *British Journal of Statistical Psychology, 3*(2), 77-85. https://doi.org/10.1111/j.2044-8317.1950.tb00285.x

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches (5th ed.).* SAGE Publications.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297-334. https://doi.org/10.1007/BF02310555

Field, A. (2018). *Discovering statistics using IBM SPSS statistics (5th ed.).* SAGE Publications.

GSM Association. (2024). *The state of the industry report on mobile money 2024.* GSMA. https://www.gsma.com/sotir/

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis (8th ed.).* Cengage Learning.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75-105. https://doi.org/10.2307/25148625

Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika, 39(*1), 31-36. https://doi.org/10.1007/BF02291575

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30*(3), 607-610. https://doi.org/10.1177/001316447003000308

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

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

Morgan, P. J., Huang, B., & Trinh, L. Q. (2019). The need to promote digital financial literacy for the digital age *(ADBI Working Paper No. 1010).* Asian Development Bank Institute. https://www.adb.org/publications/need-promote-digital-financial-literacy-digital-age

Nyamwihula, D. W. (2024). Examining the awareness of mobile money users on security risks in Tanzania to enhance cybersecurity literacy: A case study of Airtel Money. *European Journal of Theoretical and Applied Sciences, 2*(6), 536-543. https://ejtas.com/index.php/journal/article/view/1312

Nunnally, J. C., & Bernstein, I. H. (1994). *Psychometric theory (3rd ed.).* McGraw-Hill.

Organisation for Economic Co-operation and Development. (2020). *OECD/INFE 2020 international survey of adult financial literacy.* OECD. https://www.oecd.org/financial/education/oecd-infe-2020-international-survey-of-adult-financial-literacy.htm

Pallangyo, H. J. (2022). Cyber security challenges, its emerging trends on latest ICT and cyber crime in mobile money transaction services. *Tanzania Journal of Engineering and Technology, 41*(2), 189-204. https://doi.org/10.52339/tjet.v41i2.792

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-78. https://doi.org/10.2753/MIS0742-1222240302

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

Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students (8th ed.). Pearson.

Tabachnick, B. G., & Fidell, L. S. (2019). *Using multivariate statistics (7th ed.).* Pearson.

United Republic of Tanzania. (2015). *The Cybercrimes Act, 2015 (Act No. 14 of 2015).* Government Printer. https://tanzlii.org/akn/tz/act/2015/14

United Republic of Tanzania. (2022). *The Personal Data Protection Act, 2022 (Act No. 11 of 2022).* Government Printer. https://tanzlii.org/akn/tz/act/gn/2023/395b-1

van Deursen, A. J. A. M., & van Dijk, J. A. G. M. (2011). Internet skills and the digital divide. *New Media & Society, 13*(6), 893-911. https://doi.org/10.1177/1461444810386774

Yamane, T. (1967). *Statistics: An introductory analysis (2nd ed.).* Harper & Row.

© 2026 Author(s). This article is licensed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0).

Appendix A: Survey Instrument (Constructs and Representative Items)

All items use a five-point Likert scale (1 = strongly disagree to 5 = strongly agree). Each construct was measured with three to four items; a representative item is shown.

Table 8. Constructs and Representative Items

Construct	Representative item
Digital financial literacy	I understand how mobile money services, charges and transactions work
Fraud awareness	I am aware of common fraud tricks such as fake reversals, SIM-swap and OTP scams
Security behaviour	I keep my PIN and OTP secret and never share them with anyone
Digital skills	I can use mobile money apps or USSD menus correctly and safely
Risk perception	I believe there is a real risk of being defrauded when using mobile money
Self-efficacy	I am confident I can protect myself if someone tries to defraud me
Caution and skepticism	I verify before acting on unexpected calls or messages about my money
Social influence	My family, friends or community help me learn how to avoid fraud
Information access	I have access to information and campaigns on avoiding mobile money fraud
Safety attitude	I value and try to follow safe practices when using mobile money
Fraud resilience	I can recognize and avoid mobile money fraud attempts

© 2026 Author(s). This article is licensed under the Creative Commons Attribution–NonCommercial 4.0 International License (CC BY-NC 4.0).