WhatsApp Scams, Cybersecurity Awareness and Digital Consumer Vulnerability among Mobile Banking Users in Nepal

Anjali Sapkota[1], Bidur Paudel[2]

[1]Central Department of Journalism and Mass Communication, Tribhuvan University, Nepal

https://orcid.org/0009-0003-4485-0728

[2]Department of sociology, Butwal Multiple Campus, Tribhuvan University, Nepal

https://orcid.org/0009-0008-9166-0827

DOI: https://doi.org/10.47772/IJRISS.2026.1013COM0038

Received: 29 May 2026; Accepted: 13 June 2026; Published: 23 July 2026

ABSTRACT

This study examined WhatsApp scam exposure, cybersecurity awareness, and digital consumer vulnerability among mobile banking users in Nepal. A cross-sectional survey was completed by 402 adults who used mobile banking or digital payment services and WhatsApp or a comparable messaging platform. The analysis used descriptive statistics, reliability assessment, exploratory factorability diagnostics, Pearson correlations, chi-square tests, exploratory mediation, and ordinary least squares regression with HC3 robust standard errors. Nearly half of respondents (47.3%) had received suspicious or scam-like WhatsApp messages. The leading message types were suspicious links requesting personal information, fake investment or trading offers, online earning schemes, fake job offers, lottery or prize messages, and fake bank-verification messages. Personal financial loss was reported by 3.5%, while 35.1% knew someone who had lost money. In the adjusted model, cybersecurity awareness was negatively associated with susceptibility, $B = -0.141$, $p = .012$, whereas trust in WhatsApp messages, $B = 0.249$, $p < .001$, and prior exposure frequency were positive predictors. Digital literacy, digital financial literacy/safety, and perceived risk were not significant after adjustment. Exposure was significantly associated with WhatsApp groups containing unknown people. The findings support multilingual, scenario-based awareness, app-based alerts, independent verification routines, and simpler reporting channels for Nepal's banking, wallet, regulatory, educational, and law-enforcement stakeholders.

Keywords: WhatsApp scams, mobile banking, cybersecurity awareness, digital literacy, consumer vulnerability

INTRODUCTION

Digital payments have moved from a supplementary service to a daily financial habit for many Nepali consumers. Mobile banking, digital wallets, QR payments, online fund transfers, and bank-to-wallet transactions now support routine activities such as balance checking, mobile recharges, utility payments, remittances, and small-business settlements. Nepal Rastra Bank reported 30.05 million registered mobile banking customers in Baisakh 2083 and, in the same month, recorded 78.89 million mobile banking transactions worth NPR 612.39 billion, 49.94 million wallet transactions, and 59.26 million QR-based payment transactions (Nepal Rastra Bank, Payment Systems Department, 2026). Nepal Telecommunications Authority also reported 26.5 million mobile-broadband subscriptions as of Ashadh 2082, indicating that mobile connectivity is a central infrastructure for digital finance (Nepal Telecommunications Authority, 2025). These figures do not by themselves prove that all consumers use digital finance safely, but they show the scale at which financial decisions are now mediated through mobile devices.

The same mobile ecosystem that supports convenient payments also gives scammers direct access to consumers. Messaging applications allow offenders to approach users through unknown numbers, temporary

profiles, forwarded posts, social groups, hacked contacts, and impersonated institutions. WhatsApp is especially relevant because users often treat it as a personal communication space rather than a formal financial channel. A fraudulent message may therefore arrive in the same application used for family updates, work coordination, community groups, and small-business communication. When a scam message carries a bank logo, a familiar name, a government-style warning, or a promise of quick income, users may process it socially before evaluating it technically.

Messaging scams are not confined to one country or platform. Meta reported that WhatsApp removed more than 6.8 million accounts linked to criminal scam centers in the first half of 2025 (Meta, 2025). In the United States, the Federal Trade Commission reported USD 470 million in consumer losses from scams that began with text messages in 2024 (Federal Trade Commission, 2025). These international figures should not be treated as Nepal estimates, but they demonstrate a broader pattern: scammers use mobile messaging, social engineering, and cross-platform movement to reduce suspicion and speed up decisions. The international evidence also matters because Nepali consumers may receive messages from foreign numbers, international investment schemes, fake recruitment accounts, and online earning offers that travel across borders.

Nepal-specific institutional evidence makes the topic more urgent. The Financial Intelligence Unit of Nepal identified cyber-enabled fraud as a growing financial crime concern and highlighted typologies that include gift or parcel fraud, social-media impersonation, fake online business or trading platforms, OTP-sharing fraud, lottery fraud, and unauthorized access to bank or wallet accounts (Financial Intelligence Unit Nepal, 2024). The Nepal Police Cyber Bureau provides an online financial fraud complaint route and asks complainants to submit relevant URLs and screenshots (Nepal Police Cyber Bureau, n.d.). These signals show that WhatsApp-based scams are not only a personal inconvenience; they intersect with consumer protection, payment-system trust, digital financial literacy, and law-enforcement reporting.

Despite the policy importance of this issue, empirical evidence on WhatsApp scam vulnerability among Nepali mobile banking users remains limited. Much cybersecurity behavior research examines organizational compliance, email phishing, or general internet safety. The Nepali consumer setting is different because it combines rapid mobile finance adoption, multilingual communication, family and community networks, high reliance on group messaging, remittance-related expectations, job-seeking pressures, and trust in informal recommendations. A message that would appear suspicious in an office email may feel credible when forwarded by a friend, placed in a community group, or framed as a bank or government notice.

Understanding this issue is also important for maintaining trust in digital finance. A single scam incident can produce losses for an individual consumer, but repeated incidents can reduce confidence in mobile banking, wallets, and QR payments more broadly. Users who hear stories of friends losing money may become anxious about using legitimate digital services, while users who believe scams are unavoidable may accept unsafe shortcuts. Fraud prevention therefore has two goals: it should prevent immediate financial harm and preserve confidence in safe digital payment channels. Evidence on the message types, sender sources, and trust mechanisms that matter in Nepal can help institutions design warnings that feel relevant to users rather than distant from their daily experience.

This study addresses that gap by examining three connected questions: what types of suspicious WhatsApp messages Nepali mobile banking users report, how awareness, literacy, perceived risk, trust, and prior exposure relate to susceptibility, and why users believe some people trust or respond to scam messages. The study intentionally uses research questions rather than formal prediction statements because the available evidence is best suited to identifying patterns, associations, and practical intervention points. The manuscript also avoids causal language because the data were collected at one point in time. Its contribution is local, empirical, and applied: it connects consumer survey data with banking, wallet, regulatory, educational, and law-enforcement implications for Nepal.

LITERATURE REVIEW

Cybersecurity awareness is commonly understood as the user's ability to recognize digital threats and act in ways that reduce risk. In organizational research, awareness and security attitudes have been linked to

intentions to follow information security policies (Bulgurcu et al., 2010; Parsons et al., 2014). Consumer research extends this idea by showing that safer behavior depends not only on access to technology but also on the ability to interpret risk cues, control impulsive responses, and translate knowledge into daily routines (Crossler et al., 2013; Dodel & Mesch, 2019; Hadlington, 2017). For mobile banking users, awareness is practical rather than abstract: users must know that OTPs, PINs, passwords, account numbers, and identity information should not be shared through messaging links or informal chats.

Digital literacy and digital financial literacy are related but not identical. Digital literacy refers to the ability to use devices, applications, and online information effectively. Digital financial literacy adds the ability to understand digital financial products, recognize payment risks, protect accounts, and respond to unauthorized transactions or fraud attempts. OECD guidance emphasizes that digital payments create benefits but also expose consumers to security risks, data theft, fraud, and overspending, especially when digital financial literacy is low (OECD, 2025, 2026). In a mobile banking context, a user may be comfortable opening apps and scanning QR codes but still fail to detect a shortened link, fake verification form, spoofed bank page, or manipulated WhatsApp profile.

Perceived risk is another important concept in cyber-safety research. Protection motivation theory proposes that protective action depends on perceived severity, perceived vulnerability, response efficacy, and self-efficacy (Maddux & Rogers, 1983; Rogers, 1975). Technology threat avoidance theory similarly argues that users avoid information technology threats when they judge the threat to be serious and believe that available safeguards will work (Liang & Xue, 2009). These theories suggest that risk perception may reduce vulnerability, but only when users also know what to do. A person may believe that online scams are dangerous yet still click a link if the message appears urgent, if the sender appears familiar, or if the user does not know a trusted verification channel.

Phishing and scam research also highlights the role of suspicion, attention, and automatic processing. The suspicion, cognition, and automaticity model proposes that people become vulnerable when habitual behavior and low-effort processing override careful evaluation (Vishwanath et al., 2018). Systematic reviews show that attackers exploit urgency, fear, reward, authority, familiarity, scarcity, and visual realism to reduce skepticism (Desolda et al., 2022). WhatsApp scams often combine these elements. A fraudulent bank-verification message may use authority and urgency. A fake job or online earning scheme may use reward and scarcity. A family-emergency request may use familiarity and emotion. An investment group may use social proof and repeated success stories.

Trust is therefore a central mechanism in messaging scams. Unlike a random website advertisement, a WhatsApp message can borrow credibility from social relationships, group membership, institutional symbols, language choice, and repeated exposure. A message forwarded by a friend or posted in a group may appear less risky because the user assumes that someone else has already judged it. Similarly, a message with a bank logo or government name may shift the user's attention from verifying the sender to responding quickly. In Nepal, these trust cues may be amplified by multilingual communication, uneven digital literacy, reliance on social networks for information, and the everyday use of WhatsApp for both personal and semi-formal communication.

Prior exposure can operate in two directions. Frequent exposure to scam messages may increase opportunities for risky action because the user encounters more links, requests, and persuasive scripts. It may also indicate that the user belongs to high-risk digital environments, such as groups with unknown members, job-search groups, investment groups, or forwarded-message networks. At the same time, repeated exposure could make some users more skeptical if they learn to identify scam cues. For this reason, exposure should be interpreted carefully. A positive association between exposure and susceptibility does not prove that exposure causes vulnerability, but it may identify settings where prevention is most needed.

Scam susceptibility is also shaped by message design. Social-engineering messages typically ask the user to do something quickly: click, share, pay, download, register, confirm, or forward. The request is often small at first, which makes it appear manageable, but it opens a path to credential theft, unauthorized transactions, or repeated payments. In mobile banking, even a brief lapse can be costly because OTPs and app-based

confirmations are time sensitive. This means prevention messages must be equally concrete. A warning that says “be careful online” is weaker than a warning that says “your bank will never ask for your OTP or PIN on WhatsApp.”

The Nepali mobile banking context gives these concepts a specific meaning. Digital financial services are growing quickly, and users are asked to manage passwords, OTPs, QR payments, wallet transfers, app notifications, and customer-service communication. Many consumers also rely on family members, friends, local agents, or informal advice when navigating digital finance. Scammers can exploit this mixture by pretending to be a bank employee, a wallet company, a recruiter, a customs officer, a government office, a relative in trouble, or a friend whose account has been hacked. Fraud prevention must therefore address both individual skill and the social environments in which messages circulate.

This study uses these perspectives to frame susceptibility as a practical outcome shaped by awareness, literacy, perceived risk, trust, and exposure. It does not assume that awareness or literacy automatically prevents harm. Instead, it examines whether these factors remain associated with lower susceptibility after considering trust and exposure frequency. The framework is intentionally applied: it seeks to identify not only statistically significant predictors but also the message types, sources, vulnerability reasons, and prevention supports that banks, wallet companies, regulators, educators, communities, and law-enforcement agencies can act upon.

Research Objectives and Questions

The study pursued three objectives. First, it identified common types and sources of suspicious WhatsApp messages encountered by mobile banking and digital payment users in Nepal. Second, it examined the associations among cybersecurity awareness, digital literacy, digital financial literacy/safety, perceived risk, trust in WhatsApp messages, prior scam-message exposure, and susceptibility to WhatsApp scams. Third, it described the reasons respondents believed users trust, respond to, or become vulnerable to suspicious WhatsApp messages and the prevention supports they considered most useful.

The study was guided by the following research questions. RQ1: What types and sources of suspicious WhatsApp messages are commonly encountered by mobile banking users in Nepal? RQ2: How are cybersecurity awareness, digital literacy, digital financial literacy/safety, perceived risk, trust, and prior exposure associated with susceptibility to WhatsApp scams? RQ3: What reasons do respondents identify for user vulnerability, and what prevention supports do they prefer for Nepali mobile banking users?

The research questions were selected to match the cross-sectional survey design. The study therefore reports associations rather than causal effects. This approach is appropriate because the dataset captures respondents’ experiences, attitudes, and self-reported behaviors at a single point in time. The goal is not to establish temporal ordering but to provide evidence that can guide locally relevant fraud-prevention messages, reporting procedures, and future experimental or longitudinal research.

METHODS

This study used a quantitative cross-sectional survey design. The design was appropriate because the research focused on the distribution of WhatsApp scam exposure and the associations among awareness, literacy, perceived risk, trust, prior exposure and susceptibility at one point in time. Reporting was prepared with attention to relevant STROBE guidance for observational studies (von Elm et al., 2007). The study does not claim that one variable caused another; findings are interpreted as patterns of association that can inform prevention and future research.

The target population comprised adults in Nepal who used mobile banking or digital payment services and also used WhatsApp or a comparable mobile messaging platform. Inclusion criteria were age 18 years or older, use of mobile banking or digital payment services, use of WhatsApp or a similar messaging application, and voluntary consent to participate. A purposive sampling strategy was used because the study required respondents with direct experience of both mobile-based financial transactions and messaging-platform communication. The final analytical sample contained 402 valid responses.

Data were collected using a structured questionnaire administered through Google Forms. Respondents were informed about the study purpose, voluntary participation, anonymity and their right to withdraw. The questionnaire did not ask respondents to disclose account numbers, passwords, PINs, OTPs, or other sensitive financial credentials.

The sampling strategy was intentionally non-probability and purposive rather than probability-based. The unit of analysis was the individual mobile banking or digital payment user. Participants were eligible when they were adults, used mobile banking or digital payment services, used WhatsApp or a comparable messaging platform and voluntarily consented. Because a complete sampling frame of Nepali mobile banking users was not available, the findings should be interpreted as evidence from eligible users in the sample rather than as national prevalence estimates. Participant characteristics were reported to make the sample composition transparent, including gender, age group, education, occupation, province, residence type, monthly transaction category, mobile banking frequency, WhatsApp use frequency and membership in WhatsApp groups containing unknown people.

The questionnaire was developed from the study objectives, conceptual framework, prior cybersecurity and consumer-vulnerability literature and locally relevant forms of WhatsApp-enabled financial fraud. The initial item pool was organized around demographic characteristics, digital financial service use, scam exposure, message types and sources, cybersecurity awareness, digital literacy, digital financial literacy/safety, perceived risk, trust in WhatsApp messages, susceptibility, response behavior, perceived reasons for vulnerability and preferred prevention supports. English-Nepali wording and scenario-based statements were used to increase clarity for Nepali respondents. Five-point Likert-type items were used for construct measurement and the instrument intentionally avoided asking for sensitive credentials such as account numbers, passwords, PINs, OTPs, or card details.

Measurement validation was treated as a staged construct-evidence process. Content coverage was assessed by mapping questionnaire sections and items to the three research questions and conceptual constructs. After data import, Likert items were checked for valid 1-5 coding before composite scores were calculated. Internal consistency was evaluated using Cronbach's alpha, corrected item-total correlations and alpha-if-item-deleted diagnostics. Exploratory factorability was assessed using the Kaiser-Meyer-Olkin statistic and Bartlett's test of sphericity before exploratory factor analysis. Because several non-susceptibility scales showed low internal consistency and mixed factor patterns, these measures were interpreted as applied composite indicators rather than as fully validated latent variables.

The questionnaire covered demographic characteristics, mobile banking usage patterns, WhatsApp use, membership in WhatsApp groups with unknown people, exposure to suspicious messages, message types and sources, cybersecurity awareness, digital literacy, digital financial literacy/safety, perceived risk, trust in WhatsApp messages, susceptibility to WhatsApp scams, initial response behavior, reasons for vulnerability and preferred prevention supports. Likert-type construct items used a five-point response scale, where higher values represented more of the named construct. No reverse-coded items were identified in the cleaned analytical dataset.

Construct scores were interpreted as practical indicators rather than fully validated latent variables. This distinction matters because the survey was designed for an emerging Nepali consumer-fraud context where standardized WhatsApp-scam scales are not yet well established. The susceptibility measure captured self-reported risky engagement and near-belief tendencies, while the awareness, literacy, financial-safety, risk and trust measures captured related protective or vulnerability orientations. The analysis therefore emphasized transparent reporting of reliability, factorability and robustness rather than overstating measurement precision.

Data screening showed 402 imported rows and 60 imported variables. No missing cells were detected, no invalid Likert values remained after recoding and no exact duplicate rows were found. One duplicated timestamp was retained because the substantive responses differed. Gender, province, residence, monthly transaction and response-frequency label variants were harmonized without changing substantive meaning. One multivariate construct-score outlier at $p < .001$ and one regression residual with an absolute studentized value greater than 3 were retained because the responses were within valid bounded Likert patterns.

The analysis included frequencies, percentages, means, standard deviations, internal consistency reliability, exploratory factorability diagnostics, Pearson correlations, chi-square tests, exploratory bootstrap mediation through trust and ordinary least squares regression with HC3 robust standard errors. Cronbach's alpha was used to assess internal consistency, recognizing that alpha is affected by scale length, inter-item covariance, and dimensionality (Cronbach, 1951). HC3 robust standard errors were used because residual diagnostics indicated heteroskedasticity; this estimator improves inference under nonconstant error variance in finite samples (MacKinnon & White, 1985). Statistical significance was evaluated at $p < .05$.

The initial model that treated prior exposure frequency as a linear ordinal predictor showed evidence of specification nonlinearity. The final regression therefore treated prior exposure frequency as a categorical predictor with "never" as the reference category. In the final model, the Ramsey RESET result was not statistically significant, the Durbin-Watson statistic indicated acceptable independence, and multicollinearity was low. Residual normality and homoscedasticity were violated, so robust inference was retained. Exploratory mediation through trust was reported cautiously because the study was cross-sectional and several predictor scales had low internal consistency.

RESULTS

Table 1 presents the respondent profile. The sample contained slightly more male respondents (53.0%) than female respondents (46.0%), with a small number identifying as other (1.0%). Respondents were mostly young adults: 40.3% were aged 18-24 years and 31.8% were aged 25-34 years. Nearly half held a bachelor's degree (45.5%). The largest occupational groups were students (26.1%), private-sector employees (20.4%), and business owners or entrepreneurs (13.9%). Bagmati Province accounted for 34.6% of the sample, followed by Lumbini Province (15.4%) and Koshi Province (14.4%). Municipal residents formed the largest residence category (40.8%), followed by metropolitan or sub-metropolitan residents (36.6%).

Table 1 Respondent Profile (N = 402)

Variable	**Category**	**N**	**%**
Gender	Female	185	46.0
	Male	213	53.0
	Other	4	1.0
Age group	18-24 years	162	40.3
	25-34 years	128	31.8
	35-44 years	68	16.9
	45-54 years	31	7.7
	55 years and above	13	3.2
Education	Below SEE/SLC	22	5.5
	Intermediate/+2	102	25.4
	Bachelor's degree	183	45.5
	Master's degree or above	61	15.2
	Technical/vocational education	34	8.5

Occupation	Student	105	26.1
	Private sector employee	82	20.4
	Business owner/entrepreneur	56	13.9
	Self-employed/freelancer	36	9.0
	Homemaker	26	6.5
	Government employee	25	6.2
	Teacher/academic professional	24	6.0
	Banking/finance sector employee	21	5.2
	Unemployed	15	3.7
	Farmer	12	3.0
Province	Koshi Province	58	14.4
	Madhesh Province	37	9.2
	Bagmati Province	139	34.6
	Gandaki Province	47	11.7
	Lumbini Province	62	15.4
	Karnali Province	26	6.5
	Sudurpaschim Province	33	8.2
Residence	Metropolitan/sub-metropolitan city	147	36.6
	Municipality	164	40.8
	Rural municipality	91	22.6
Monthly transaction	Below NPR 15,000	67	16.7
	NPR 15,000-30,000	87	21.6
	NPR 30,001-50,000	78	19.4
	NPR 50,001-75,000	39	9.7
	Above NPR 75,000	30	7.5
	Prefer not to say	101	25.1

Note. Percentages are based on 402 valid responses and may not sum exactly to 100 because of rounding.

Digital financial service use was broad. All respondents used a mobile banking app. In addition, 71.1% used QR payments, 64.2% used digital wallets, 60.7% used online fund transfers, and 55.7% used internet banking.

The most common primary uses were balance checks (92.3%), mobile recharge (64.9%), fund transfer (62.7%), utility bill payment (55.7%), bank-to-wallet transfer (44.5%), wallet loading (42.5%), and QR payment (42.3%). These patterns show that respondents were not occasional observers of digital finance; most were active users of mobile financial services.

Table 2 summarizes mobile banking frequency, WhatsApp exposure, and selected response indicators. One third of respondents used mobile banking daily, and 28.6% used it several times a week. WhatsApp use was also frequent, with 57.2% reporting daily use and 24.4% reporting use several times a week. A majority (52.7%) belonged to WhatsApp groups that included unknown people, and 47.3% reported receiving a suspicious or scam-like WhatsApp message. Personal financial loss was reported by 3.5%, but 35.1% knew someone who had lost money, suggesting that harm may be more visible through social networks than through direct self-disclosure.

Table 2 Mobile Banking Use, WhatsApp Exposure, and Selected Response Indicators

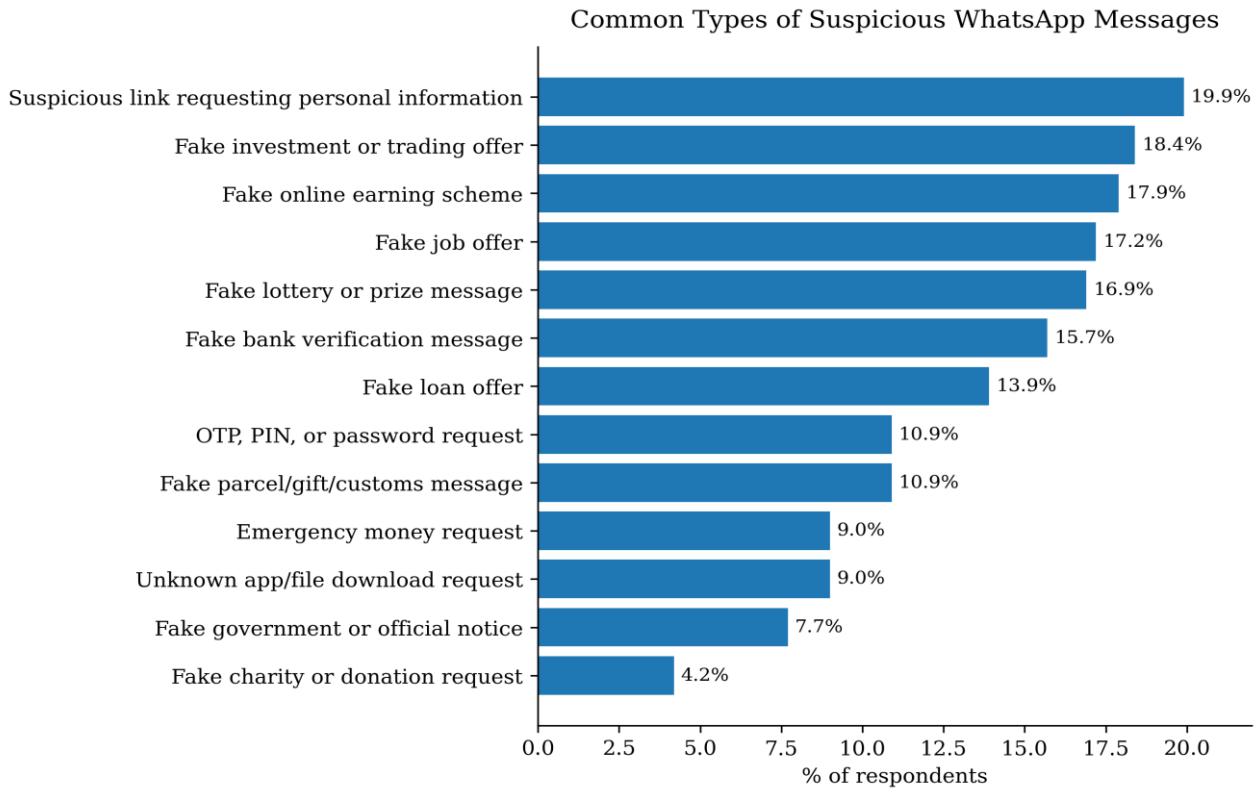
Indicator	**Category**	**N**	**%**
Mobile banking frequency	Daily	133	33.1
	Several times a week	115	28.6
	Once a week	54	13.4
	A few times a month	58	14.4
	Rarely	42	10.4
WhatsApp frequency	Daily	230	57.2
	Several times a week	98	24.4
	Once a week	35	8.7
	A few times a month	20	5.0
	Rarely	10	2.5
WhatsApp group with unknown people	Yes	212	52.7
	No	168	41.8
	Not sure	22	5.5
Received suspicious/scam-like message	Yes	190	47.3
	No	170	42.3
	Not sure	42	10.4
Frequency of suspicious messages	Often	50	12.4
	Sometimes	88	21.9
	Rarely	81	20.1
	Never	161	40.0
Link-verification request received	Yes	176	43.8

OTP/PIN/password request received	Yes	62	15.4
Institutional impersonation received	Yes	146	36.3
Personal financial loss	Yes	14	3.5
Know someone who lost money	Yes	141	35.1
First response to verification link	Call or visit the bank	134	33.3
	Click link and follow instruction	9	2.2
Response to OTP/PIN/password request	Refuse to share it	133	33.1
	Contact bank or wallet provider	99	24.6
	Share if urgent	6	1.5
	Share if official-looking	4	1.0

Note. Selected rows are shown to retain the most policy-relevant usage, exposure, and response indicators. Multi-response items are interpreted as percentages of respondents, not percentages of responses.

RQ1 asked what types and sources of suspicious WhatsApp messages were commonly encountered. Figure 1 shows that the leading message type was a suspicious link requesting personal information (19.9%). Other common messages included fake investment or trading offers (18.4%), fake online earning schemes (17.9%), fake job offers (17.2%), fake lottery or prize messages (16.9%), and fake bank-verification messages (15.7%). Lower but still important categories included fake loan offers, OTP/PIN/password requests, fake parcel or customs messages, emergency money requests, unknown app or file downloads, fake official notices, and fake charity or donation requests.

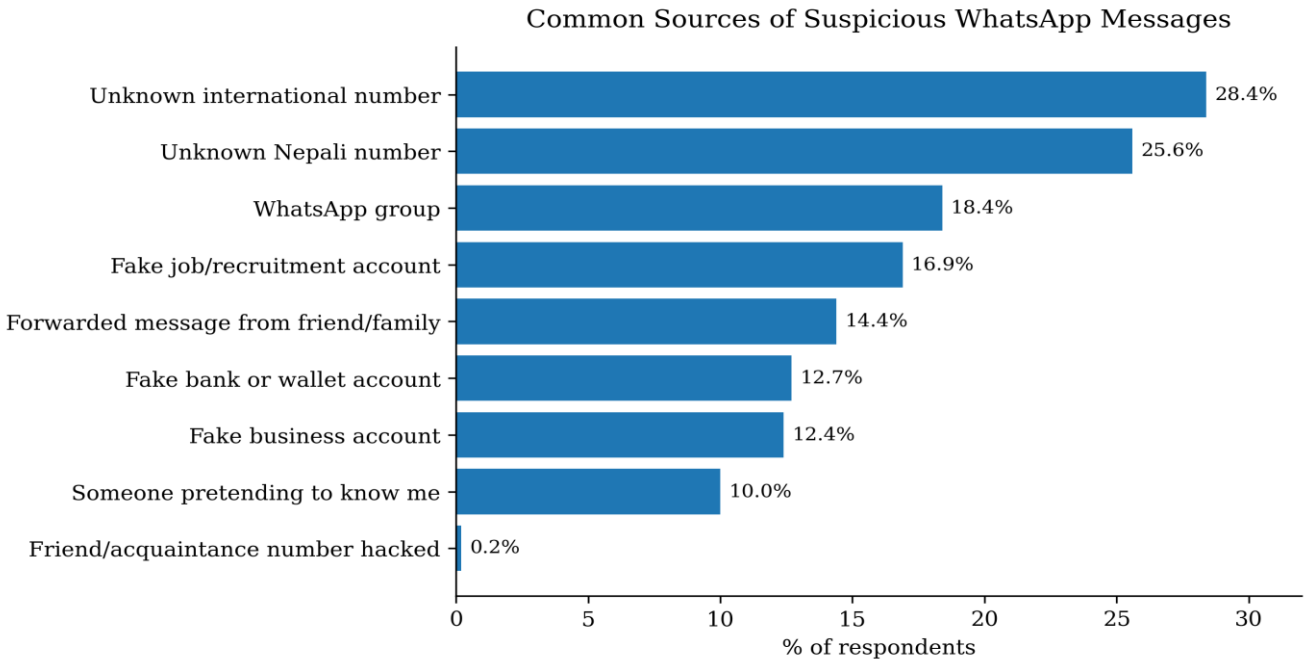
Figure 1 Common Types of Suspicious WhatsApp Messages



Note. Percentages are percentages of respondents; multiple responses were allowed.

Figure 2 shows the most common reported sources of suspicious messages. Unknown international numbers were the leading source (28.4%), followed by unknown Nepali numbers (25.6%), WhatsApp groups (18.4%), fake job or recruitment accounts (16.9%), forwarded messages from friends or family (14.4%), fake bank or wallet accounts (12.7%), fake business accounts (12.4%), and someone pretending to know the respondent (10.0%). These sources indicate that scams reached respondents through both unfamiliar senders and socially credible channels.

Figure 2 Common Sources of Suspicious WhatsApp Messages



Note. Percentages are percentages of respondents; multiple responses were allowed.

Table 3 reports composite scale descriptives, internal consistency, and factorability diagnostics. Perceived risk had the highest mean (M = 3.924), followed by digital financial literacy/safety (M = 3.677), cybersecurity awareness (M = 3.671), and digital literacy (M = 3.626). Trust in WhatsApp messages was moderate (M = 3.165), and susceptibility to WhatsApp scams was below the scale midpoint but variable (M = 2.396, SD = 0.672). Internal consistency was strong for susceptibility (alpha = .839) and approached acceptability for the pooled protective competence sensitivity measure (alpha = .670), but was lower for the other constructs. These reliability results require caution when interpreting nonsignificant predictor findings.

The item set was suitable for exploratory factor analysis, KMO = .818, Bartlett's test of sphericity, chi-square(435) = 2420.44, $p < .001$. However, the exploratory solution showed a clear susceptibility factor and mixed or cross-loading patterns among protective-awareness, risk, and trust items. For that reason, confirmatory fit indices, average variance extracted, and composite reliability were not presented as strong validity evidence. The theoretically specified composites were retained for the applied regression analysis, but measurement refinement is recommended for future Nepali studies.

Table 3 Composite Descriptive Statistics, Internal Consistency, and Factorability Diagnostics

Construct	**K**	**M**	**SD**	**Median**	**Alpha**
Cybersecurity awareness	5	3.671	0.459	3.600	.530
Digital literacy	5	3.626	0.403	3.600	.356
Digital financial literacy/safety	5	3.677	0.412	3.600	.366

Perceived risk	3	3.924	0.479	4.000	.369
Trust in WhatsApp messages	4	3.165	0.543	3.250	.528
Susceptibility to WhatsApp scams	8	2.396	0.672	2.125	.839
Protective competence pooled	15	3.658	0.326	3.667	.670

Note. All constructs used five-point Likert-type scoring. KMO overall MSA = .818; Bartlett's test of sphericity: chi-square(435) = 2420.44, $p < .001$; eigenvalues greater than 1 = 9. Alpha values below conventional thresholds indicate that results should be interpreted cautiously.

Table 4 presents Pearson correlations among the study constructs. Cybersecurity awareness was negatively correlated with trust in WhatsApp messages, $r = -.23$, $p < .001$, and susceptibility, $r = -.16$, $p < .01$. Trust was positively correlated with susceptibility, $r = .28$, $p < .001$. Prior exposure frequency showed a strong positive correlation with susceptibility, $r = .71$, $p < .001$, indicating that respondents who more often encountered suspicious messages also reported more risky engagement or near-belief behaviors. Perceived risk was not significantly correlated with trust or susceptibility.

Table 4 Pearson Correlations Among Study Constructs

Variable	**M**	**SD**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
1 CSA	3.671	0.459	—						
2 DL	3.626	0.403	.44***	—					
3 DFL	3.677	0.412	.34***	.36***	—				
4 PR	3.924	0.479	.25***	.16**	.14**	—			
5 Trust	3.165	0.543	-.23***	-.14**	-.14**	-.05	—		
6 Suscept.	2.396	0.672	-.16**	-.07	-.05	.08	.28***	—	
7 Exposure	1.231	1.249	-.07	-.05	-.01	.08	.12*	.71***	—

Note. CSA = cybersecurity awareness; DL = digital literacy; DFL = digital financial literacy/safety; PR = perceived risk; Suscept. = susceptibility; Exposure = prior exposure frequency. * $p < .05$, ** $p < .01$, *** $p < .001$.

Table 5 reports the final HC3 robust regression model predicting susceptibility to WhatsApp scams. The model was statistically significant, $F(9, 392) = 64.49$, $p < .001$, $R^2 = .597$, adjusted $R^2 = .588$. Diagnostic tests supported the final modeling approach: Breusch-Pagan LM = 25.331, $p = .003$, indicated heteroskedasticity; Shapiro-Wilk W = 0.977 and Jarque-Bera chi-square = 22.349 were significant, indicating nonnormal residuals; Durbin-Watson = 1.993 suggested acceptable independence; maximum VIF = 1.402 showed low multicollinearity; and Ramsey RESET $F = 3.128$, $p = .078$, did not indicate clear specification error in the final categorical-exposure model.

Cybersecurity awareness was a significant negative predictor of susceptibility, B = -0.141, SE = 0.056, 95% CI [-0.250, -0.031], $p = .012$. Trust in WhatsApp messages was a significant positive predictor, B = 0.249, SE = 0.043, 95% CI [0.165, 0.333], $p < .001$. All prior exposure categories were positively associated with susceptibility relative to the never-exposed group. Digital literacy, digital financial literacy/safety, and perceived risk were not significant independent predictors after adjustment. Sensitivity analyses using prior exposure as an ordinal predictor and using the pooled protective competence measure produced the same

substantive conclusion: trust and exposure remained central, cybersecurity awareness remained protective in the ordinal exposure model, and broad literacy or perceived-risk measures were not robust independent predictors.

Table 5 HC3 Robust Regression Predicting Susceptibility to WhatsApp Scams

Predictor	**B**	**SE**	**95% CI**	**Std. effect**	**T**	**P**
Intercept	1.197	0.349	[0.511, 1.883]		3.43	< .001
Cybersecurity awareness	-0.141	0.056	[-0.250, -0.031]	-0.096	-2.53	.012
Digital literacy	0.058	0.064	[-0.068, 0.184]	0.035	0.91	.365
Digital financial literacy/safety	-0.016	0.062	[-0.138, 0.107]	-0.010	-0.25	.803
Perceived risk	0.073	0.051	[-0.028, 0.173]	0.052	1.43	.154
Trust in WhatsApp messages	0.249	0.043	[0.165, 0.333]	0.201	5.85	< .001
Prior exposure: Often vs. never	1.060	0.075	[0.913, 1.208]	1.579	14.15	< .001
Prior exposure: Rarely vs. never	0.344	0.064	[0.218, 0.470]	0.512	5.38	< .001
Prior exposure: Sometimes vs. never	1.022	0.059	[0.906, 1.137]	1.521	17.37	< .001
Prior exposure: Very often vs. never	1.157	0.103	[0.953, 1.360]	1.722	11.19	< .001

Note. N = 402. Reference category for prior exposure frequency is never. SE = HC3 robust standard error. Model summary: $R^2 = .597$, adjusted $R^2 = .588$, $F(9, 392) = 64.49$, $p < .001$. Standardized effects for exposure dummies are y-standardized coefficients.

Exploratory chi-square tests showed that receipt of suspicious or scam-like WhatsApp messages did not differ significantly by gender, chi-square(4) = 7.57, p = .109, age group, chi-square(8) = 11.62, p = .169, education, chi-square(8) = 11.68, p = .166, or mobile banking frequency, chi-square(8) = 13.57, p = .094. Exposure differed significantly by whether respondents belonged to WhatsApp groups with unknown people, chi-square(4) = 36.04, p < .001, Cramer's V = .200. This effect was small to moderate and suggests that group membership is a practical exposure pathway.

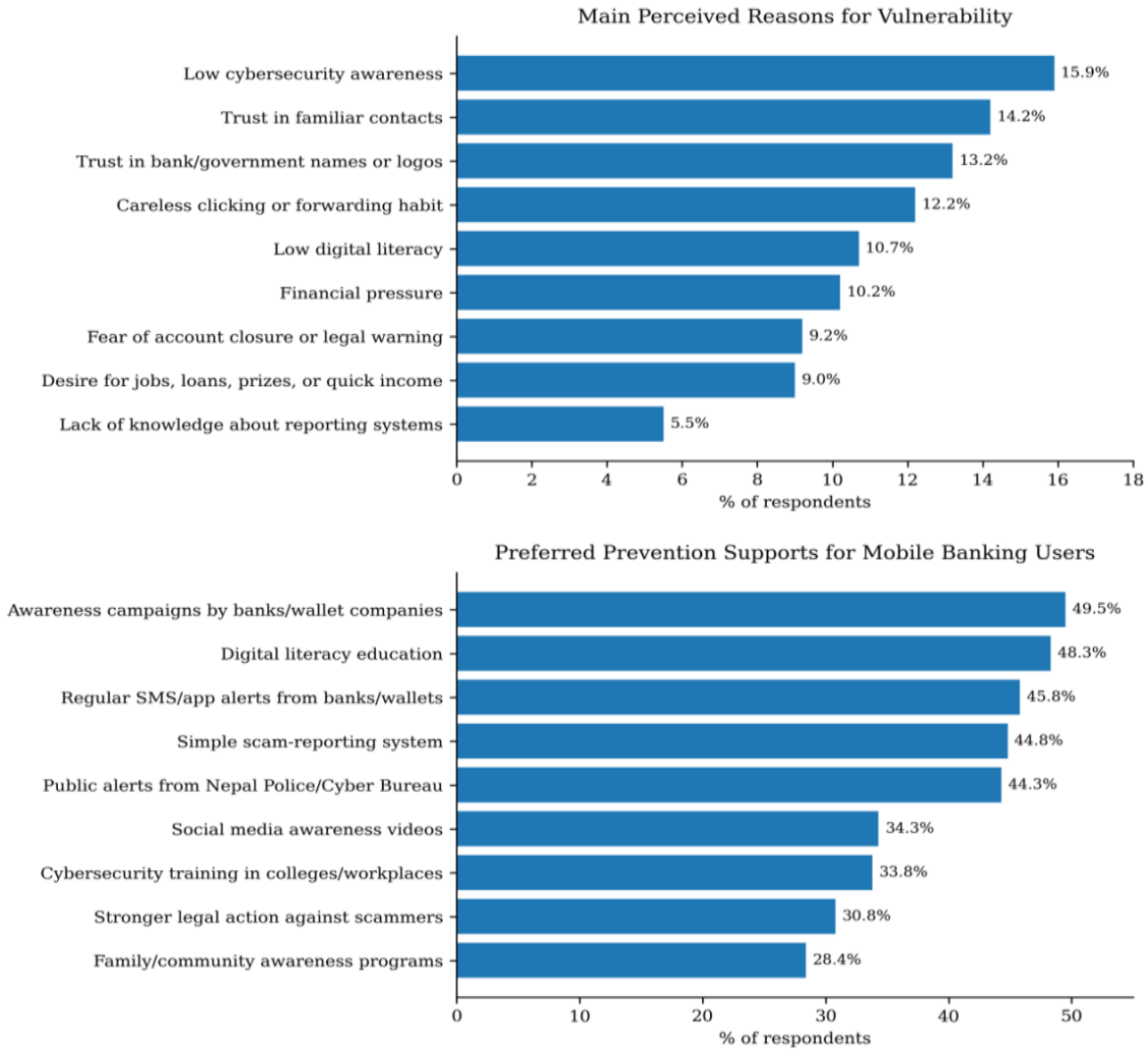
Exploratory bootstrap mediation through trust suggested that cybersecurity awareness had a significant indirect association with susceptibility through trust, indirect effect = -0.052, 95% CI [-0.093, -0.019]. Prior exposure frequency also showed a small significant indirect effect through trust, indirect effect = 0.011, 95% CI [0.001, 0.022]. Indirect effects were not significant for digital literacy, digital financial literacy/safety, or perceived risk. These results should be treated as exploratory because cross-sectional data cannot establish temporal sequence and several antecedent scales had low internal consistency.

RQ3 focused on reasons for vulnerability and preferred prevention supports. Figure 3 shows that respondents most often identified low cybersecurity awareness (15.9%), trust in familiar contacts (14.2%), trust in bank or government names/logos (13.2%), careless clicking or forwarding habits (12.2%), low digital literacy (10.7%), financial pressure (10.2%), fear of account closure or legal warning (9.2%), and desire for jobs, loans, prizes, or quick income (9.0%). Preferred prevention supports emphasized awareness campaigns by banks and wallet companies (49.5%), digital literacy education (48.3%), regular SMS or app alerts (45.8%), simple scam-reporting systems (44.8%), and public alerts from Nepal Police/Cyber Bureau (44.3%).

Keyword-assisted review of open-ended responses, treated as descriptive rather than as full qualitative analysis, pointed to the same practical themes. Respondents mentioned bank, OTP, and account-verification

messages; emergency money requests; suspicious links; job, earning, and investment offers; and WhatsApp account hacking or impersonation. These comments help connect the numeric findings to the everyday language of scam encounters. The pattern suggests that users do not experience scams as a single technical category. Instead, they encounter a rotating set of stories that ask for quick action, borrowed trust, or small first steps that later create financial risk.

Figure 3 Perceived Vulnerability Reasons and Preferred Prevention Supports



Note. Percentages are percentages of respondents; multiple responses were allowed. The figure combines descriptive RQ3 evidence on perceived vulnerability reasons and prevention preferences.

DISCUSSION

This study provides localized empirical evidence on WhatsApp scams and digital consumer vulnerability among mobile banking users in Nepal. The first major finding is that suspicious-message exposure was common. Nearly half of respondents reported receiving a suspicious or scam-like WhatsApp message and substantial minorities had received link-verification requests, institutional impersonation or OTP/PIN/password requests. The most common message types were not technically complex attacks; they were persuasive social-engineering scripts involving personal-information links, investment or trading offers, job and earning schemes, lottery or prize messages and fake bank verification. This pattern closely resembles cyber-enabled fraud typologies highlighted by FIU-Nepal, including parcel or gift fraud, impersonation, fake online business or trading platforms, OTP fraud, lottery fraud and unauthorized access to bank or wallet accounts (Financial Intelligence Unit Nepal, 2024).

The second major finding is that trust in WhatsApp messages was one of the strongest independent predictors of susceptibility. This result is consistent with phishing and social-engineering theory, which explains scam vulnerability through reduced suspicion, automatic processing and reliance on credibility cues (Desolda et al., 2022; Vishwanath et al., 2018). In the Nepali setting, credibility cues appear to include bank or government names, official-looking logos, familiar contacts, forwarded messages, group endorsement, urgent account warnings and quick-income promises. The descriptive reasons for vulnerability reinforce this interpretation because respondents selected trust in familiar contacts and trust in bank or government names/logos as common reasons people become vulnerable.

The practical lesson is that awareness campaigns should not only tell users that scams exist. Many users already perceive online risks as high, yet perceived risk did not independently predict lower susceptibility after adjustment. Prevention must teach a specific habit: pause, verify independently and distrust urgent requests that arrive through messaging links, even when they look official or come from a known contact. A consumer who receives a bank-verification link should open the official bank app or call a verified number rather than clicking the message. A user who receives an emergency money request from a familiar name should verify by voice call or in-person contact. A job or earning group should be treated skeptically when it asks for registration fees, deposits, app downloads, account details or OTPs.

Cybersecurity awareness remained protective in the regression model, although its effect was smaller than the effect of trust and prior exposure. This finding fits prior research showing that awareness and security attitudes can support safer behavior (Bulgurcu et al., 2010; Parsons et al., 2014). At the same time, the nonsignificant adjusted effects of digital literacy and digital financial literacy/safety should be interpreted cautiously. The reliability of these scales was low, which may have weakened observed relationships. More importantly, broad literacy may not capture scam-specific competence. A respondent may know how to use QR payments, wallets, and fund transfers but still be unsure whether a WhatsApp link, shortened URL, fake form or impersonated customer-service profile is safe.

This interpretation is important for policy. Digital inclusion campaigns often celebrate the ability to use applications, but scam resistance requires a different kind of competence. It requires skepticism toward unexpected financial messages, knowledge of official verification routes, confidence to ignore pressure and a willingness to ask for help before acting. A user who is digitally active but socially trusting may still be vulnerable. Future instruments should therefore measure concrete behaviors such as checking URL domains, refusing remote-access apps, confirming sender identity, saving evidence and reporting promptly. These behaviors may explain more variance than general self-ratings of digital skill.

The nonsignificant role of perceived risk is also informative. The sample reported comparatively high perceived risk, but risk perception alone did not reduce susceptibility. Protection motivation theory and technology threat avoidance theory help explain why. People act protectively when they believe a threat is serious and believe they can perform an effective response (Liang & Xue, 2009; Maddux & Rogers, 1983; Rogers, 1975). If users fear account closure, legal warning, job loss, or missed financial opportunity, risk perception may even coexist with quick compliance. Awareness programs should therefore combine risk information with simple response scripts: do not share OTPs; do not click verification links; do not install unknown apps; do not pay fees to get a job or prize; contact the bank or wallet provider through a verified channel; and report with screenshots and URLs.

Prior exposure frequency was strongly associated with susceptibility. This finding should not be read as proof that exposure causes vulnerability, because the survey is cross-sectional and the susceptibility scale captures self-reported behaviors and near-belief indicators. However, the association is practically important. Users who frequently receive scam messages have more opportunities to make a mistake and they may also be located in high-exposure digital environments. The significant chi-square association between exposure and WhatsApp groups containing unknown people supports this interpretation. Group-based environments can create social proof, reduce scrutiny and allow scam messages to spread rapidly through forwarding.

The low self-reported personal loss rate, 3.5%, should be treated carefully. Fraud victimization is often underreported because of embarrassment, fear of blame, low confidence in recovery or reluctance to discuss

money. FIU-Nepal notes the importance of timely reporting and also recognizes that victims may hesitate, particularly when losses are small or sensitive (Financial Intelligence Unit Nepal, 2024). The much higher share of respondents who knew someone who had lost money, 35.1%, suggests that financial harm may be more visible at the social-network level than in direct self-disclosure. This difference also shows why community-level prevention matters. People may learn about scams through stories of relatives, friends, neighbors and coworkers.

Overall, the findings support a shift from generic digital literacy toward scam-specific, context-sensitive fraud prevention. The most important behavioral target is not simply "use mobile banking carefully." It is to reduce trust in WhatsApp messages that request action related to money, identity, passwords, OTPs, investments, jobs, loans, prizes, parcels or account verification. The user should not have to become a technical expert. The user needs a small number of durable rules that work across message types: verify outside the chat, never share secrets, avoid unknown groups, avoid payment for promised income and report quickly with evidence.

Practical Implications for Nepal

For banks and digital wallet providers, the findings support scenario-based security messages embedded directly inside mobile banking and wallet applications. App alerts should focus on the exact scam cues reported in this study: links asking for personal information, fake investment and trading offers, online earning schemes, fake job offers, fake bank verification, OTP/PIN/password requests, fake parcel or customs claims, emergency money requests and unknown app downloads. Short warnings should be repeated at moments of risk, such as during first-time transfers, wallet loading, QR payments, device changes, password resets and suspicious login attempts.

Banks and wallet companies should also make verification easier than clicking a message link. Users need a visible in-app button or verified contact route for "I received a suspicious message." The safest instruction is not only "do not click"; it is "open the official app, call this verified number, or report here." Customer-service teams should be trained to respond quickly because users under pressure may return to the scammer if the official response is slow or confusing. Alerts should be written in Nepali and relevant regional languages and they should use common local examples rather than abstract cybersecurity terms.

For regulators and consumer-protection agencies, the findings suggest that digital financial literacy should be integrated with fraud-prevention policy. OECD guidance emphasizes that safe use of digital payments requires consumers to understand fraud, unauthorized transactions and security risks (OECD, 2025, 2026). In Nepal, such guidance can be localized through Nepal Rastra Bank campaigns, wallet-provider coordination, branch-level posters, radio messages, college modules, social media videos and targeted outreach for first-time mobile banking users, migrant-worker families, job seekers, students, older adults and small entrepreneurs.

For law-enforcement and reporting systems, simplified reporting is essential. Respondents preferred simple reporting systems and public alerts from Nepal Police/Cyber Bureau. The Cyber Bureau already requests evidence such as URLs and screenshots for online financial fraud complaints (Nepal Police Cyber Bureau, n.d.). Banks, wallet providers, and regulators can increase use of this pathway by adding report buttons, preserving transaction records, encouraging screenshots before deleting messages, and providing step-by-step guidance after suspected fraud. Reporting instructions should also clarify what users should do immediately: contact the bank or wallet provider, block the sender, do not delete evidence, and change passwords from a clean device when needed.

Institutions should also coordinate public alerts. A scam that begins as a WhatsApp job offer may later involve wallet loading, bank transfers, QR codes, SIM changes or social-media impersonation. Separate warnings from separate agencies can leave consumers confused. A coordinated alert system, using consistent language and shared examples, would make the message stronger: official institutions do not ask for OTPs through WhatsApp, payments should not be made to receive prizes or jobs and suspected fraud should be reported quickly with evidence. Such consistency can reduce uncertainty during the short window in which a user decides whether to comply.

For educational institutions, workplaces, and communities, prevention should be taught through realistic micro-scenarios. A classroom or workplace session can show a fake bank-verification message, a job-offer message, a loan offer, an investment group, an emergency money request, and a parcel/customs message. Participants can practice identifying the cue, choosing a safe response and explaining the decision to family members. This type of practice is more likely to produce durable behavior than a lecture that only defines phishing. Community programs should also normalize verification. Calling a relative to confirm an emergency money request should be seen as responsible, not rude.

For WhatsApp group administrators and community leaders, the significant association between exposure and groups with unknown people points to a clear prevention target. Group administrators can restrict posting, remove suspicious accounts, discourage earning/investment promotion, and pin warnings about OTP secrecy and link verification. Families and community groups can adopt simple rules: no financial links, no investment promises, no job registration fees, no forwarding of bank or government notices unless verified through an official source and no sharing of OTPs or passwords under any condition.

Limitations and Future Research

Several limitations should be acknowledged. First, the study used purposive sampling and should not be generalized to all Nepali mobile banking users. The sample was relatively young and educated and included a large share of respondents from Bagmati Province. Future research should use stratified or probability-based sampling across provinces, rural and urban municipalities, gender groups, age cohorts and education levels. A larger probability sample would allow stronger estimates of exposure and loss prevalence across Nepal.

Second, all measures were self-reported. Self-report data can be affected by recall bias, social desirability bia, and underreporting of sensitive financial loss. Some victims may not want to admit that they clicked a link, shared information, lost money, or trusted a scam. Future studies should, where ethically feasible, combine survey data with anonymized bank or wallet complaint records, Cyber Bureau complaint patterns, app-level warning logs and controlled message-recognition experiments. Such designs would allow researchers to compare stated awareness with observed recognition behavior.

Third, several predictor scales had low internal consistency. The susceptibility scale was strong, but cybersecurity awareness, digital literacy, digital financial literacy/safety, perceived risk and trust require refinement for Nepali mobile banking contexts. Future studies should use cognitive interviewing, translation and back-translation, pilot testing across language groups, confirmatory factor analysis and measurement-invariance testing across provinces and demographic groups. Stronger measurement would make it easier to distinguish general digital competence from scam-specific protective skill.

Fourth, the cross-sectional design prevents causal inference. Longitudinal studies could examine whether awareness interventions reduce trust in scam messages and whether reduced trust lowers later susceptibility. Experimental vignette designs could manipulate sender familiarity, bank logos, government names, urgency, Nepali-language scripts, group endorsement and promised rewards to identify which cues most strongly increase vulnerability. Intervention trials could compare generic warnings with scenario-based prompts, app-based friction, and family/community verification training.

Finally, this study focused on WhatsApp and mobile banking users. Future research should compare WhatsApp with Facebook Messenger, Viber, Telegram, TikTok, SMS, email and phone-call scams because fraudsters move across communication channels as users and platform protections change. Research should also examine how scams target migrant-worker families, older adults, new wallet users, students, job seekers and small businesses. These groups may face different trust cues, financial pressures and reporting barriers.

CONCLUSION

WhatsApp-based scams are a meaningful digital consumer vulnerability for mobile banking users in Nepal. In this survey of 402 users, suspicious-message exposure was common, and the most frequent scams involved suspicious links, fake investment or earning offers, job offers, lottery or prize messages and fake bank

verification. The adjusted regression results showed that cybersecurity awareness reduced susceptibility, whereas trust in WhatsApp messages and prior scam-message exposure frequency increased susceptibility. Digital literacy, digital financial literacy/safety and perceived risk were not significant independent predictors after adjustment, partly reflecting measurement limitations and the possibility that broad competence does not automatically become scam-specific protective behavior.

The study's practical message is clear: prevention should focus on trust, verification and reporting. Banks, wallet providers, Nepal Rastra Bank, Nepal Police Cyber Bureau, educators, communities and platform group administrators should prioritize multilingual, scenario-based messages that teach users to pause before acting, verify outside WhatsApp, refuse all OTP/PIN/password requests, avoid unknown earning and investment groups, preserve screenshots and URLs and report quickly through trusted channels. A safer digital finance ecosystem in Nepal will require not only informed users but also institutions that make safe decisions easier than risky ones.

Because mobile banking is now woven into ordinary financial life, scam prevention should be treated as part of service quality, not as an optional awareness activity. Clear warnings, trusted verification routes and fast reporting support can help users continue using digital finance with confidence while reducing the chance that WhatsApp-based social engineering turns convenience into vulnerability.

REFERENCES

1. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), 523-548. https://doi.org/10.2307/25750690
2. Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika, 16(3), 297-334. https://doi.org/10.1007/BF02310555
3. 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
4. Desolda, G., Ferro, L. S., Marrella, A., Catarci, T., & Costabile, M. F. (2022). Human factors in phishing attacks: A systematic literature review. ACM Computing Surveys, 54(8), Article 173. https://doi.org/10.1145/3469886
5. Dodel, M., & Mesch, G. (2019). An integrated model for assessing cyber-safety behaviors: How cognitive, socioeconomic and digital determinants affect diverse safety practices. Computers & Security, 86, 75-91. https://doi.org/10.1016/j.cose.2019.05.023
6. Federal Trade Commission. (2025, April 14). Top text scams of 2024. https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2025/04/top-text-scams-2024
7. Financial Intelligence Unit Nepal. (2024). Strategic analysis report 2024: Cyber enabled frauds. Nepal Rastra Bank. https://www.nrb.org.np/contents/uploads/2024/11/FIU-Nepal-Strategic-Analysis-Report-2024.pdf.pdf
8. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346. https://doi.org/10.1016/j.heliyon.2017.e00346
9. 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
10. MacKinnon, J. G., & White, H. (1985). Some heteroskedasticity-consistent covariance matrix estimators with improved finite sample properties. Journal of Econometrics, 29(3), 305-325. https://doi.org/10.1016/0304-4076(85)90158-7
11. Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5), 469-479. https://doi.org/10.1016/0022-1031(83)90023-9
12. Meta. (2025, August 5). New WhatsApp tools and tips to beat messaging scams. https://about.fb.com/news/2025/08/new-whatsapp-tools-tips-beat-messaging-scams/

13. Nepal Police Cyber Bureau. (n.d.). साईबर अपराध रिपोर्ट गर्नुहोस् [Report cybercrime]. Retrieved July 9, 2026, from https://cyberbureau.nepalpolice.gov.np/report-cyber-crime/
14. Nepal Rastra Bank, Payment Systems Department. (2026). Monthly payment systems indicators: Baisakh 2083 (Mid-May 2026). https://www.nrb.org.np/psd/payment-systems-indicators-of-2083-baisakh/
15. Nepal Telecommunications Authority. (2025). Telecommunication indicators: Ashadh 2082. https://nta.gov.np/uploads/contents/MIS_%20Ashadh_2082.pdf
16. OECD. (2025). Supporting informed and safe use of digital payments through digital financial literacy. OECD Publishing. https://doi.org/10.1787/21de47d1-en
17. OECD. (2026). Protecting consumers from financial scams and frauds. OECD Publishing. https://doi.org/10.1787/d41817bb-en
18. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computers & Security, 42, 165-176. https://doi.org/10.1016/j.cose.2013.12.003
19. 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
20. Vishwanath, A., Harrison, B., & Ng, Y. J. (2018). Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research, 45(8), 1146-1166. https://doi.org/10.1177/0093650215627483
21. von Elm, E., Altman, D. G., Egger, M., Pocock, S. J., Gotzsche, P. C., Vandenbroucke, J. P., & STROBE Initiative. (2007). The Strengthening the Reporting of Observational Studies in Epidemiology (STROBE) Statement: Guidelines for reporting observational studies. PLOS Medicine, 4(10), e296. https://doi.org/10.1371/journal.pmed.0040296