International Journal of Trend in Research and Development, Volume 13(5), ISSN: 2394-9333
www.ijtrd.com

Social Engineering Exposure and Protective Practices Among Selected Demographic Groups in Nepal: An Exploratory Mixed-Methods Study

[1]Kiran Barakoti, [2]Krishna Kumar Rai, [3]Prof. Raj Kumar Thakur, [4]Sagar Sitaula, [5]Drona Prasad Acharya, [6]Gopal Ghimire,
[1, 4]Independent Researchers, Nepal
[2]Master of Information Technology (MIT), Purbanchal University School of Science and Technology (PUSAT), Biratnagar, Nepal
[3]Professor, Purbanchal University School of Science and Technology (PUSAT), Biratnagar, Nepal
[5]Independent Researcher, Australia
[6]Master of Computer Application, Purbanchal University School of Science and Technology (PUSAT), Biratnagar, Nepal

[1] ORCID ID: https://orcid.org/0009-0005-1250-5342 [2] ORCID ID: https://orcid.org/0009-0002-7980-7108
[4] ORCID ID: https://orcid.org/0009-0006-1687-6594 [5] ORCID ID: https://orcid.org/0009-0005-6701-7223
[6] ORCID ID: https://orcid.org/0009-0005-5044-8588

Abstract: Social engineering attacks are not limited to technical vulnerabilities, but happen through human judgment, trust and common digital actions. The study analyzes reported exposure, awareness of cybersecurity, protective practices and selected impacts for students, working adults, small business owners, and elderly respondents in Nepal. A mixed methodology was used, which included a structured survey of 100 respondents and analysis of documented cyber-fraud and social-engineering cases. The survey data was analyzed using descriptive statistics, cross-tabulation, chi-square test of independence and logistic regression, and the case material was analyzed thematically. Phishing emails were the most common type of attack reported, followed by impersonation scams and fraudulent calls. There were also differences among the four groups in terms of awareness and reported exposures. The study finds that there is a significant disconnect between what participants knew about cybersecurity and the protective behaviors they actually practice: less were using multi-factor authentication or changing their passwords regularly than were aware of or suspicious of. The results suggest that Nepal's cybersecurity programs need to focus more on hands-on verification practices, contextual training, organizational security measures, and safer digital payment habits.

Keywords: *Social Engineering; Phishing; Cybersecurity Awareness; Human Factors; Protective Behavior;*

I. INTRODUCTION

The security issue has been transformed along with the services people use, and digital transformation. A secure system can be compromised if a legitimate user is tricked into providing information, authorizing a transaction, opening a malicious message or trusting a fake identity. Social engineering is thus not just a technical issue, but also a human and organizational security issue. In environments where communication tools and online interaction provide opportunities for manipulation, advanced social engineering is growing, according to Krombholz et al. [1]. In a similar vein, Heartfield and Loukas [2] outline a wide class of attacks that rely on psychological and contextual means to achieve a security-relevant action.

Phishing is the most obvious of these issues, and there are other forms such as impersonation, pretexting, baiting, business email compromise, and fraudulent calls. Social phishing research has shown that attackers can enhance the credibility of a message by using information about a target's social relationships [3]. Previous behavioral research also revealed that users don't always make phishing decisions by conducting a security evaluation; familiarity, expectations, habits and the perceived legitimacy of a request can influence the decision [4, 5]. The susceptibility to phishing is found to be affected by cognitive processing, message characteristics, personal differences, and context, not just technical knowledge [6]-[10] and is still being studied in more recent research.

This is the difference between awareness and behavior that is significant for the present study. Even if a respondent is aware of what phishing is, he or she might fall for a convincing message, especially if the request is urgent, familiar, or authoritative. Context, expectations, habits, and perceived legitimacy have been found to affect phishing decisions in previous research [4, 5]. The problem is not so much if people know about cyber threats, but whether they are able to convert that information into a safe choice when presented with a legitimate request.

These are some of the issues that have specific relevance in Nepal. Digital payment services and mobile financial channels have grown at a rapid pace in the country. As of mid-July 2024, Nepal Rastra Bank has recorded 23.46 million mobile-wallet users and significant increases in QR-based payments and other digital tools [22]. This expansion brings a lot of convenience, but also makes it more common for users to be faced with a decision between real and fake communications. According to the Nepal Police Annual Factsheet for FY 2080/81, there were 19,730 reports of cybercrime applications, including social platforms, emails, messaging, and digital-payment applications [23]. The Electronic Transactions Act offers the foundation legal rules for electronic transactions and unauthorized use of electronic records, and the nation's payments system is bolstered by specific cyber-resilience and financial-literacy programs [24] [25].

Although digital services are growing in number, there is limited evidence in Nepal that exists on the difference in exposure to social engineering and in social engineering protective practices across demographic groups. Previous research has focused on university student users, mobile-banking users, and general cybersecurity awareness [26]-[28] but less research has focused on comparing multiple user groups in the same survey setting. This study bridges that gap by conducting an exploratory survey of 100 participants, and a contextual analysis of documented cases.

The study aims to answer 5 questions. What are the most common social engineering attack types reported by the participants? Secondly, what are the differences in reported

exposure for the four demographic groups? Third, what are the differences in awareness and protective practices? Fourth, what are the financial and psychological impacts of the participants? Lastly, what are practical implications of the observed patterns? The paper adds by combining these questions together in a Nepalese context and by analysing the findings of the survey by interpreting them from the human-factor literature instead of social engineering as merely a technical detection problem.

II. RELATED WORK

A. Social engineering and the human factor

Social engineering is all about relationships. The attacker sets a situation whereby the target's normal expectations provide an advantage to the attacker. Krombholz et al. [1] recognize the emerging sophistication of social engineering in online communication contexts and Heartfield and Loukas [2] offer a structured perspective on social engineering attacks, focusing on phases and attack templates that can be reused. The views are helpful for a survey-based study since they shift the argument from the notion that victims are simply lacking in technical knowledge. Technical skills do not necessarily mean that a person will respond to a message that it appears as if it came from a trusted colleague, bank, employer, or government office.

Let's take social phishing as an example. Jagatic et al. [3] have shown that it is possible to use social information to make phishing messages more convincing. Relevance to Nepal is simple: People are increasingly being connected by digital services in known institutions and personal networks, thus attackers can take advantage of institutional familiarity and technical deception. Another identity and context-based form of business email compromise is the creation of verisimilitude in the email. According to the FBI, BEC is a fraud involving the exploitation of official accounts or legitimate identities to coax transfers or divulge information [20].

The humane factor shouldn't however be called a weak link. However, Heartfield and Loukas [11] demonstrated the possibility of the user being a security sensor as well by providing him with the right mechanisms and incentives to detect and report semantic social engineering. This distinction is important for the design of interventions. Security programs that focus on users as a source of error tend to focus on blame and compliance. When users are part of the security system, it is possible to implement reporting systems, verification processes, and feedback loops to simplify the making of secure decisions.

B. Phishing susceptibility and demographic differences

Previous research into phishing vulnerability has shown that demographic and situational factors can be significant, but can be different in different cases. Sheng et al. [6] explored the differences in phishing susceptibility and effectiveness of anti-phishing interventions by conducting a large role-play survey. Iuga et al. [8] also explored the factors that impact whether or not an internet user can identify a phishing page from a legitimate page. They argue that susceptibility is multi-factorial and cannot be boiled down to one defining characteristic [16].

Age is very important in this study because there is an elderly sample. Sarno et al. [17] reported that older adults might exhibit distinct decision-making patterns when determining phishing messages, but their experiments did not reveal any simple age-related decline in the overall ability to classify a message. It is important to note this as a caveat on the present study. The higher the percentage of response that elderly persons indicate greater exposure to fraudulent calls or less awareness, the conclusion should not be that the age itself makes people vulnerable. Instead, it is possible that age interacts with digital experience, familiarity with the channel, confidence, and the type of deception employed.

Susceptibility can also be influenced by the work context. Williams, Hinds and Joinson [9] identified that the factors of authority and urgency can impact an employee's susceptibility to targeted phishing, and that context can impact how an employee reacts to a suspicious message. It is applicable to small business owners and professionals—often, they need to make quick decisions in financial and operational communication. When a request requires being placed in a work or payment setting, it looks like a plausible request when it is included in the personal inbox.

C. Awareness, protective behavior, and training

A recurring finding in the literature is that knowledge alone is insufficient. Downs et al. [4] discovered that users can get a good sense of familiar risks without learning transferable strategies for unfamiliar risks. Egelman, Cranor, and Hong [5] showed that the design and timing of phishing notifications can influence user reaction to them. Vishwanath et al. [7] demonstrated that there are automatic components to people's email behavior that can lead to phishing susceptibility, so training must not only include conscious knowledge, but also automatic behavior.

This distinction is in line with organizational information-security research. There are findings that support the attitude-behavior link, such as those that have been reported by Bulgurcu, Cavusoglu and Benbasat [13] and Herath and Rao [14] that information-security awareness influences attitudes and beliefs related to policy compliance, and that perceived threats, benefits, costs and deterrence have been found to influence protective behavior. Siponen, Pahnila, and Mahmood [15] also studied the compliance issue of information-security policy as a behavioral and organizational issue. These studies have contributed to the interpretation that secure behavior is based on an interaction of awareness, perceived risk, organizational expectations, usability and the actual cost of complying with the security recommendations.

The impact on cybersecurity education is significant. Bada et al. [12] state that campaigns can be unsuccessful if they provide information without considering the concepts of motivation, usability, and behavior change. The approach of a continuous learning-program approach, in which content and evaluation metrics are based on roles, is also recommended by NIST SP 800-50 Rev. 1 [21]. In the Nepal context, this means that the awareness raising messages need to be tailored to each group's channel and decision-making process and should not be one size fits all.

D. Digitalization and the Nepalese context

Social engineering is a socio-technical problem and the digital space in Nepal offers ample motivation to analyze this problem. According to the payment oversight reporting documents released by Nepal Rastra Bank, wallets, QR payments, mobile banking and other payment instruments experienced rapid growth in Nepal [22]. The report also highlights the growing significance of cybersecurity and digital financial literacy alongside the increasing availability of payment options. The Nepal Police cybercrime factsheet offers an alternate operational view of the volume and variety of cybercrime complaints as well as the different types of digital channels that are used to report cybercrime cases [23].

There are some limited existing studies on the awareness level of cybersecurity in Nepal. A recent study of university students showed that there are major deficiencies in the knowledge and practice of cybersecurity, confirming that empirical studies of other groups of individuals are required [26]. This study thus does not claim to be a national prevalence study but an exploratory comparison. The research gap is by no means that there is no cybersecurity research in Nepal but it is the least combination of demographic exposure, awareness and protective behaviors with socio-economic impacts in one empirical model.

III. RESEARCH METHODOLOGY

A. Research design

The study used a mixed-methods design. The quantitative component was intended to describe patterns of awareness, reported exposure, and protective behavior across four demographic groups. The qualitative component was used differently: rather than treating external incidents as additional survey observations, it provided context for understanding how deception, credential compromise, impersonation, and payment manipulation can occur in real-world settings.

The unit of analysis for the survey was the individual respondent. The study did not attempt to estimate the national incidence of social engineering, and the results should not be generalized to all Nepalese citizens without further probability-based research. The contextual cases were not treated as observations from the same statistical population; they served as external evidence for interpreting the mechanisms and consequences associated with social engineering and related cyber-fraud.

B. Participants and sampling

The survey included 100 participants divided into four predefined demographic strata: 40 students, 20 working professionals, 10 small business owners, and 30 elderly individuals. The thesis describes the sampling approach as stratified random sampling, with representation across demographic categories and urban and rural settings. Because the group sizes were deliberately allocated rather than proportional to Nepal's population, the resulting percentages describe the study sample and should not be interpreted as national prevalence estimates.

Table I. Composition of the survey sample.

Demographic group	n	Share of sample
Students	40	40%
Working professionals	20	20%
Small business owners	10	10%
Elderly individuals	30	30%
Total	100	100%

C. Survey instrument and data collection

The questionnaire contained four broad components: demographic information, awareness of social engineering techniques, experience with attacks, and cybersecurity practices. Questions addressed phishing, impersonation, fraudulent communications, password behavior, multi-factor authentication, and link or attachment verification. Both close-ended questions and Likert-scale items were used. The survey was distributed online through Google Forms to participants with digital access and in printed form to reach participants with limited internet access. The original study targeted variation across urban and rural locations and across age and occupational groups.

The use of both online and offline collection was important because a purely online sample could systematically exclude some of the participants the study sought to examine. At the same time, mixed collection modes can introduce mode effects. Responses obtained through a web form and responses obtained on paper may differ because of differences in privacy, interviewer presence, or interpretation of questions. This possibility is treated as a limitation rather than assuming that the two modes are perfectly equivalent.

D. Case-study component

The qualitative component examined three types of contextual evidence. First, the 2016 Bangladesh Bank cyber-heist was considered as a socio-technical financial cyber-fraud case. Contemporary reporting describes 35 fraudulent SWIFT payment messages totaling approximately USD 950 million in attempted transfers, with about USD 81 million ultimately transferred to the Philippines. The attackers compromised the bank's local environment, obtained valid SWIFT operator credentials, and used malware to interfere with local monitoring and records [31], [32]. Importantly, the available evidence does not establish that a phishing email was the initial intrusion vector, so the incident is not presented as a confirmed phishing-led compromise. Second, Kenyan research on the M-Pesa ecosystem was reviewed to understand recurring voice- and SMS-based social engineering, including vishing and smishing. The studies document mobile-money users' exposure to such attacks and describe the role of deception, trust, and limited security awareness [33], [34]. This evidence is treated as a documented attack pattern, not as a single dated M-Pesa incident. Third, Nepalese cyber-fraud patterns were considered using Nepal Police's official cyber-crime factsheet and related guidance [23]. These cases were not used to calculate prevalence and were not treated as observations from the survey. Their purpose was to show how social engineering can operate through different communication and payment environments.

E. Quantitative analysis

Descriptive statistics were used to summarize awareness, reported attack exposure, protective practices, and selected impacts. Cross-tabulations compared the four demographic groups. A chi-square test of independence was used to examine whether reported attack categories differed across groups. The original analysis reported a chi-square statistic of 18.67 with 6 degrees of freedom and a p-value below 0.05. Logistic regression was also reported for selected attack outcomes.

For the chi-square analysis, the null hypothesis was that demographic group and reported attack type were independent, while the alternative hypothesis was that an association existed. The expected frequency for each cell was calculated from the corresponding row and column totals. Because the survey permits respondents to report different attack experiences, the interpretation of the cross-tabulation is limited to the coding scheme used in the original dataset. The paper therefore reports the statistic as an association rather than as evidence of causation.

The reported regression results gave odds ratios of 2.5 for respondents above 50 years in relation to fraudulent-call exposure, 3.2 for small business ownership in relation to impersonation scams, and 1.8 for students in relation to phishing-email exposure. The original analysis reported an overall prediction accuracy of 84 percent. Because the available manuscript does not include the complete model specification, confidence intervals, coding matrix, or calibration measures,

these estimates are treated as reported results rather than as a fully validated predictive model.

Table II. Reported logistic regression results.

Predictor	Reported OR	p-value	Outcome emphasized
Age group above 50	2.5	0.01	Fraudulent calls
Small business ownership	3.2	0.005	Impersonation scams
Student	1.8	0.03	Phishing emails

F. Ethical considerations and limitations of design

Participation was voluntary, respondents were informed about the purpose of the study, and responses were treated as confidential and anonymized. No personally identifying information is reported in this paper. The study is observational and cross-sectional. Consequently, relationships between demographic characteristics, awareness, and reported exposure should be interpreted as associations. The sample size is modest, some strata are small, and self-reported exposure may be affected by recall or social-desirability bias. These limitations are especially relevant when interpreting the regression results for the small-business group, which contains only ten participants.

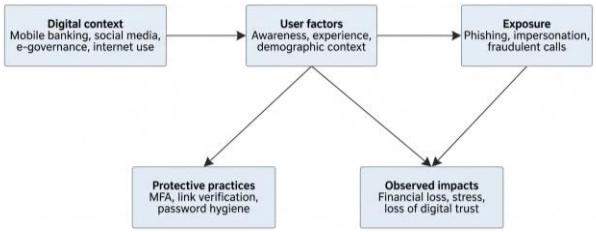

Fig. 1. Conceptual research framework linking digital context, user factors, exposure, protective practices and observed impacts.

IV. RESULTS

A. Awareness of social engineering techniques

The survey results show clear differences in awareness across the four demographic groups. Students recorded the highest awareness for phishing at 75 percent, followed by professionals at 60 percent, small business owners at 50 percent, and elderly respondents at 30 percent. A similar gradient appears for pretexting and impersonation. Awareness of pretexting was 60 percent among students, 50 percent among professionals, 40 percent among small business owners, and 20 percent among elderly participants. For impersonation, the corresponding values were 65, 55, 45, and 25 percent.

Table III. Self-reported awareness of selected social engineering techniques.

Group	Phishing	Pretexting	Impersonation
Students	75%	60%	65%
Professionals	60%	50%	55%
Small business owners	50%	40%	45%
Elderly individuals	30%	20%	25%

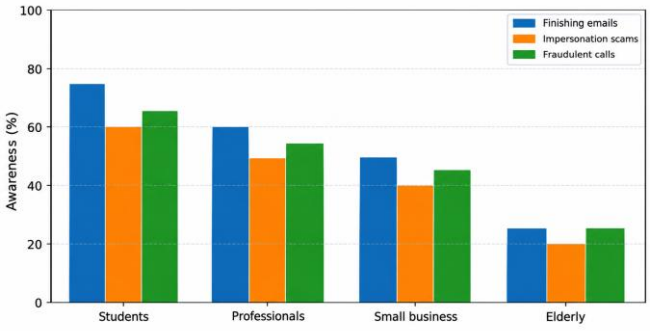

Fig. 2. Awareness of phishing, pretexting and impersonation by demographic group.

The pattern is consistent across the three awareness measures: students and professionals reported greater familiarity, while elderly respondents reported the lowest levels of self-reported familiarity. This should be interpreted carefully. The questionnaire measured recognition or self-reported awareness rather than objectively testing whether participants could identify a malicious message. Research such as Sarno et al. [17] also shows that age-related differences in phishing behavior are more nuanced than a simple assumption that older adults are less capable. In this study, the result is best viewed as an indication of where additional training may be useful, not as evidence of an inherent weakness in an age group.

B. Reported social engineering exposure

Phishing emails were the most frequently reported attack category in the sample, with 60 percent of respondents reporting exposure. Impersonation scams were reported by 40 percent and fraudulent calls by 25 percent. At the demographic level, students reported phishing exposure most frequently at 70 percent, followed by professionals at 60 percent, small business owners at 50 percent, and elderly participants at 25 percent. Impersonation was highest among small business owners at 60 percent, while fraudulent calls were highest among elderly respondents at 30 percent.

Table IV. Reported exposure to selected social engineering attacks by demographic group.

Attack type	Students	Professionals	Small business	Elderly
Phishing emails	70%	60%	50%	25%
Impersonation scams	30%	40%	60%	35%
Fraudulent calls	15%	25%	20%	30%

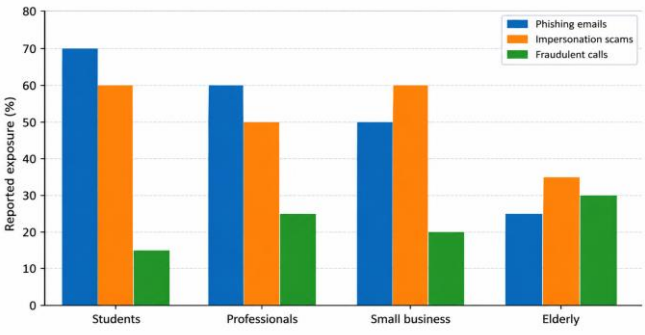

Fig. 3. Reported exposure to phishing emails, impersonation scams and fraudulent calls.

The distribution suggests that the digital context of each group may shape the kinds of attacks they encounter. Students and professionals are frequently exposed to email and online communication, which may help explain the higher reported phishing exposure. Small business owners regularly deal with invoices, suppliers, payments, and urgent requests, making impersonation particularly relevant. Elderly respondents reported a relatively higher proportion of fraudulent calls, which is consistent with research showing that age and communication context can influence responses to phishing-related threats [17]. These are plausible explanations, however; the survey itself cannot establish why particular groups received particular attacks.

C. Association between demographic group and attack type

The chi-square analysis produced $\chi^2 = 18.67$ with 6 degrees of freedom and $p < 0.05$. The null hypothesis of independence was therefore rejected at the stated significance level. The result indicates that the distribution of reported attack types differs across the demographic groups in the sample. In practical terms, the pattern is not consistent with all groups reporting phishing, impersonation, and fraudulent calls at the same rates.

The result adds statistical support to the descriptive differences, but significance should not be confused with effect size or causation. The study does not report Cramer's V, confidence intervals, or a sensitivity analysis for the small-business group. These would be useful in future work to show how strong and stable the observed association is.

D. Regression findings

The reported logistic regression results identify three demographic associations. Respondents above 50 years had an odds ratio of 2.5 for fraudulent-call exposure, small business ownership had an odds ratio of 3.2 for impersonation scams, and students had an odds ratio of 1.8 for phishing-email exposure. The reported p-values were 0.01, 0.005, and 0.03, respectively. The original analysis also reports 84 percent predictive accuracy.

These estimates should be interpreted as relative odds within the sampled data, not as population-level risk ratios. In particular, the small-business estimate should be treated cautiously because only ten respondents belonged to that group. A larger study should report standard errors and 95 percent confidence intervals, specify the reference category, document the exact dependent-variable coding, and use appropriate multi-class or separate binary models when more than one attack type is analyzed.

E. Financial and psychological impacts

Financial loss was reported across all four demographic groups. The original table gives average reported losses of NPR 5,000 for students, NPR 20,000 for professionals, NPR 30,000 for small business owners, and NPR 10,000 for elderly participants. Small business owners therefore had the highest average loss in the table. The thesis also contains a separate pooled estimate that is not consistent with these group values. To avoid creating a misleading summary statistic, this paper reports the group-level table values only.

Table V. Average reported financial loss by demographic group.

Group	Average reported loss (NPR)
Students	5,000
Professionals	20,000
Small business owners	30,000
Elderly individuals	10,000

The effects were not limited to money. The thesis reports stress, anxiety, reduced trust in digital platforms, and avoidance of online banking after incidents. Among elderly respondents, 50 percent were reported to experience stress and 20 percent reported avoiding online banking after an attack. These should be understood as self-reported psychological or behavioral effects, not clinical measurements, because the study did not use a standardized psychological instrument.

F. Awareness and protective behavior

One of the clearest findings is the difference between knowing about security and consistently practicing it. The study reports that 40 percent of respondents believed they could recognize phishing attempts, 40 percent routinely verified links or attachments, 25 percent used multi-factor authentication, and 30 percent regularly changed passwords. The thesis also reports an urban-rural difference, with urban respondents showing somewhat greater adoption of MFA and verification practices. These figures point to a practical issue: awareness does not automatically translate into routine protective behavior.

Table VI. Reported adoption of selected cybersecurity practices.

Protective practice	Reported adoption
Regular password changes	30%
Multi-factor authentication	25%
Verification of email links/attachments	40%

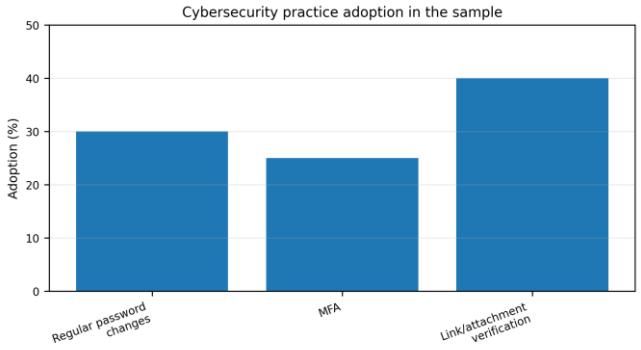

Fig. 4. Reported adoption of selected cybersecurity practices.

The result is important because it changes the interpretation of the awareness problem. If only knowledge were missing, increasing awareness should be sufficient. The observed pattern suggests that knowledge and behavior are not equivalent. This aligns with Downs et al. [4], who found that users may recognize familiar phishing risks without developing robust strategies for unfamiliar messages, and with Bada et al. [12], who emphasize that effective awareness requires the ability and motivation to apply advice. NIST's learning-program guidance [21] likewise recommends measurable and continuous learning rather than isolated awareness messaging.

V. DISCUSSION

A. Reading the demographic pattern

The results as a whole indicate that there were differences in reported exposure between the four groups. The most common type of phishing was in the form of e-mail. The highest incidence of phishing exposure was among students, the highest impersonation exposure was among small business owners, and

the highest incidence of fraudulent-call exposure was among elderly respondents. While this could reflect differences in digital contexts, these differences should not be interpreted as evidence of susceptibility due to demographic identity alone.

There is support in the literature for a contextual interpretation. Williams et al. [9] discovered that both authority and urgency cues affect phishing susceptibility in the workplace. This gives a good insight into how a business owner can be targeted in a financial or supplier scenario. The study by Sarno et al. [17] shows that this isn't as straightforward as just saying that older adults are less able to detect phishing. Iuga et al. [8] also demonstrate that the susceptibility to phishing relies on several personal and message characteristics. Therefore, the primary value of the present study is to describe the various exposures and not to rank the various demographic groups in terms of safety or hazard.

B. The awareness-behavior gap

The most salient finding of the study is the distinction between awareness and protective behavior. Forty percent of respondents indicated that they are able to identify phishing emails, while 25 percent said they employ MFA and 30 percent said they change their passwords frequently. But it is not to say that awareness is of no value. Instead, it indicates that knowledge doesn't represent the entirety of the decision process. Past studies have demonstrated that perceived benefits and costs, social norms, self-efficacy, and the circumstances when a user is asked for a security action all influence security behavior [13, 14].

This suggests a need for Nepal to move towards practical awareness program design. While knowing what phishing means is helpful, there are a few core "rules" that will help users avoid falling victim to phishing attacks: pause before responding, confirm who the sender is using another means, scrutinize links before clicking, never enter passwords or one-time codes, and use MFA if available. The same practices can be reinforced by organizations with transaction verification procedures and role-specific training.

C. Digital payments and institutional trust

Trust is a critical security concern in the growing payment system in Nepal. In reference to the growth of mobile wallets, QR payments, mobile banking and instruments, Nepal Rastra Bank has seen it increase rapidly [22]. Satisfaction escalates the amounts of authentic transactions that mimic the scam pattern; message, ask for confirmation, financial action. As more people engage in a valid digital transaction, it could be easier for an attacker to mimic an established transaction pattern.

The institutional dimension is also a key factor. The Electronic Transactions Act provides the legal framework for conducting secure electronic transactions and regulating unauthorized access to them [24] and payment-system regulation has been evolving to include components that focus on cyber-resilience and financial-literacy [22], [25]. But technical measures and legislation will not be able to do away with deception. The FBI's BEC guidance calls on the use of trusted identities and spear phishing to trick legitimate users into making financial transfers [20]. This finding of heightened exposure to impersonation by small business owners, then, aligns with the need for increased independent verification of payment instructions, particularly if a request alters a known process.

D. Increase awareness to interventions that change behavior

The results are consistent with a multi-level intervention strategy. Individual training should be based on recognition and verification of a practical nature. Policies should ensure that at the organizational level secure choice is easy and routine. Payment providers and communication platforms can integrate warnings, transaction monitoring, robust authentication, and reporting options. Agencies can help promote digital-financial literacy, coordinate reporting, and promote public education at the policy level. These measures focus on various aspect of the same issue in addition to awareness.

This multi-layered strategy is in line with the overall literature. Egelman et al. [5] demonstrate that warning design has an impact on user response. Heartfield and Loukas [11] show the user can actively contribute to the detection of attacks. Awareness campaigns that are not linked to behavior change are recommended to be avoided, according to Bada et al. [12]. The current framework for continuous learning and evaluation is available from NIST [21]. These studies collectively imply that there is no yes or no answer when it comes to whether technology or awareness is more effective to improve cybersecurity resilience—it is a combination of both.

E. implications for various population groups

The high level of exposure to phishing that was reported in this sample indicates that educational institutions should focus on email, social media, account-recovery, and credential-security scenarios. Simultaneously, training should include realistic decision exercises, not just definitions! Pressures placed on people in the workplace through communication can lead to urgency and need for authority, which should be significant themes for working individuals. Verification of payments, vendor identification and approval of unusual transactions are more relevant for small business owners. For older users, interventions should focus on easily understood communication methods, clear language, everything being demonstrated clearly, and there should be a way for them to check independently for a financial action before they make it.

These recommendations are not to be interpreted as stereotypes. The intent of demographic segmentation is to align the content of the intervention(s) and observed exposure patterns. A person can be involved in more than one type of risk context; for instance, an older small-business owner could be a victim of both impersonation and fraudulent-call risks. Future studies should thus look at crossovers between age, occupation, place, digital experience and past victimization.

F. Relationship to existing Nepalese evidence

The results of the study align with the latest Nepalese study on cyber security awareness among university students [26] but expand the population studied. The national payment environment documented by Nepal Rastra Bank [22] offers a structural explanation for the need for attention to digital-financial scams and the Nepal Police factsheet [23] shows the level and variety of complaints received for cybercrime. The present survey provides a user level perspective by highlighting the differences in awareness and attack exposure by demographic groups.

The study, however, must not overestimate its contribution as well. It does not claim to be nationally representative, provide an estimate of the overall financial impact of cybercrime in Nepal, nor provide an experimental measure of the susceptibility to phishing. Its role is more limited and practical, offering a comparative snapshot of self-reported exposure and protection

among a few selected groups and correlating those observations with existing human-factor research.

G. Methodological interpretation and directions for validation:

The results also indicate the importance of separating exposure, susceptibility and impact. Exposure: a participant states that he or she was exposed to an attack category. Susceptibility is a person's acceptance of an attacker's request or inability to identify a deception under controlled circumstances. Impact refers to consequences following an incident, including loss of money, stress, loss of trust or avoidance of digital service. In the present survey, exposure is measured more directly than experimentally observed susceptibility, and the impact is self-reported. The fact that a group reports more attacks does not mean that they are easier to fool; it could be that they get more appropriate attacks or that they use a communication medium that makes those attacks more visible.

This separation is substantiated by previous fieldwork. Wright and Marett [19] have identified experiential and dispositional factors as associated with phishing responses, and Williams et al. [9] have demonstrated that message context, authority and urgency are factors that influence workplace phishing. Combining survey measures with controlled scenarios or ethically designed phishing simulations could then be used in future Nepalese studies. This type of work would enable researchers to correlate the expectations participants state with their actual reactions to realistic security challenges.

A second methodological problem is the quality of the measures. In the present questionnaire, there are a number of direct percentage indicators that are useful for an exploratory study, but do not offer a standardized scale for cybersecurity awareness or protective behavior. Future studies need to create or adapt validated multi-item scales of constructs including phishing knowledge, perceived susceptibility, security self-efficacy, trust in digital services, and protective intention. Comparisons across demographic groups would be more defensible with internal-consistency analysis, construct validation and test-retest reliability. The use of validated measures would also allow for testing the statistical association of awareness with behavior when controlling for age, occupation, location, digital experience, and prior victimization.

This applies to the same way in statistical analysis. The result of the chi-square test in the present study is helpful as an initial assessment of association, but may be supplemented by reports of an effect size measure, e.g., Cramer's V, in addition to the exact p-value and confidence interval. If multiple attack types are allowed, each attack type should be modeled, not assuming the attack types are mutually exclusive; the coding rule should be documented. A larger sample size would allow for multinomial logistic regression or separate binary models with clear reference groups and diagnostics in the regression case. Confidence intervals in addition to odds ratios would help to make the uncertainty around the estimates for subgroups apparent, especially for small subgroups like small business owners.

The third one is longitudinal assessment. The findings of the present study show that there is an awareness-behavior gap, however, it cannot be established from a cross-sectional study whether training would close the gap. An effective follow-up design would involve assessing awareness and protective practices at baseline, providing a focused intervention, and re-assessing awareness and protective practices at a later time. Possible outcomes may include activation of MFA, link verification actions, suspicious message reports and recognition of simulated phishing. NIST's learning-program guidance [21] presents a good framework for considering awareness as an ongoing program that has measurable results.

Lastly, the national context needs to be continued to be central to future work. Verizon's latest breach research indicates that human activity plays a significant role in breaches, and underscores the relationship between credential abuse, social actions and technical exploitation [29]. Meanwhile, FBI reporting indicates that business email compromise fraud also continues to be a significant financial loss with deception and trusted identities playing a key role [20] [30]. As highlighted by Nepal Rastra Bank [22] there is significant growth in digital payment in Nepal, and user facing security behavior will continue to play a major role even if security technical controls are enhanced. Recent Nepalese research on students [27] and mobile-banking users [28] also indicates that cybersecurity awareness and vulnerability of digital consumers are active research areas in Nepal. Such a larger, multi-sector study might then create a more comprehensive evidence base based on demographic, behavioral, organizational and technology-use factors.

VI. PRACTICAL IMPLICATIONS

The findings suggest five action priorities: Firstly, any awareness program should be addressing repeatable behaviors, not just terminology. Second, training should be tailored for the scenarios that are typical for various groups. Thirdly, financial institutions and payment providers need to improve verification and reporting processes. Fourth, simple protections like independent verification and dual approving of bizarre payments should be implemented in small organizations. Fifthly, national programs should consider both attendance and behavior change as indicators of training success. Fifthly, national programs should consider to measure behavior change as well as attendance when evaluating the success of a training.

The results also confirm the need for local-language, easily accessible training material. The original study noted a difference between the awareness and protective behaviors of rural and urban participants. Don't assume that rural users are less secure, but rather, this should be considered an access and context issue that can be solved through community education, with mobile-friendly content, and cooperation with banks, schools, local governments, and civil-society groups.

VII. LIMITATIONS

There are several caveats that should be taken into account when interpreting. The sample is not nationally representative with only 100 participants. The four demographic groups were proportionately divided, and not based on the proportions of Nepal's population. The number of small-business participants is only 10, potentially lessening the stability of the small-business sub-group estimates and the stability of the regression result. This survey also uses self-report of awareness and attacks experienced, which can lead to recall error, misconceptions about the type of attacks, and social-desirability (S-D) error.

The study is cross sectional and observational, and the reported relationships should not be interpreted as a cause and effect. The chi-square result suggests an association between the demographic group and the type of attack reported, but it cannot reveal that the victimization is caused by the demographic characteristics. Similarly, regression estimates are associations and do not represent causal pathways. The contextual cases provide background information but are not statistically related to the observations of the survey. The Bangladesh Bank incident

is not the best example of an initial compromise via phishing, in particular. Lastly, there are varying types of financial loss in the different parts of the thesis, so the journal version takes the group-level amounts in the financial-loss table and does not calculate a pooled estimate.

Future studies should include larger sample sizes obtained through probability-based sampling or carefully stratified sampling, include confidence intervals and effect sizes, and experimentally test phishing decision-making utilizing validated scales for awareness and behavior. Long-term studies would be particularly valuable to assess long-term effects of targeted training on MFA adoption, verification behavior and incident reporting.

CONCLUSION

This research focuses on the social engineering exposure, awareness of cyber security, protective measures and selected impacts of four demographic groups in Nepal. The most common category of attacks in the sample was phishing, and the distribution of the various types of attacks varied between the groups. The highest incidence of phishing exposure was reported by students, the highest impersonation exposure was reported by small business owners, and the highest number of respondents who said they had been exposed to fraudulent calls were elderly. The chi square test showed a significant relationship between the two variables of demographic group and reported attack type.

The results also show that knowing about cybersecurity does not necessarily mean that protective actions are performed consistently. Forty percent of respondents said they were confident in identifying phishing, 25 percent said they were using MFA and 30 percent said they were changing their passwords regularly. The findings thus support a shift in the focus of awareness campaigns from information delivery to training focusing on repeatable behaviors.

The challenge for Nepal is growing along with the expansion of digital financial and communication services. Mobile wallet, QR payments, online banking, digital public services are increasingly adopted and the security of the ecosystem relies on a combination of technical measures and the ability of the users to identify and verify suspicious requests. Resilient approach should include user education, organizational procedures, secure authentication, payment verification, reporting procedures, and coordinated institutional action.

The primary contribution of the study is not to simply point to one group of demographics that is somehow vulnerable. Rather, it indicates that the groups in the survey experienced different exposure and were different in their awareness and protective behavior. It can contribute to more relevant interventions for schools, workplaces, financial institutions and public agencies. Larger and more widespread studies are required to ascertain if these patterns are representative of Nepal as a whole and which interventions are successful in changing security behavior in the long-term.

References

[1] K. Krombholz, H. Hobel, M. Huber, and E. Weippl, “Advanced social engineering attacks,” Journal of Information Security and Applications, vol. 22, pp. 113–122, 2015, doi: 10.1016/j.jisa.2014.09.005.

[2] R. Heartfield and G. Loukas, “A taxonomy of attacks and a survey of defence mechanisms for semantic social engineering attacks,” ACM Computing Surveys, vol. 48, no. 3, art. 37, pp. 1–39, 2016, doi: 10.1145/2835375.

[3] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, “Social phishing,” Communications of the ACM, vol. 50, no. 10, pp. 94–100, 2007, doi: 10.1145/1290958.1290968.

[4] J. S. Downs, M. B. Holbrook, and L. F. Cranor, “Behavioral response to phishing risk,” in Proc. 2nd Annual eCrime Researchers Summit, 2007, pp. 37–44, doi: 10.1145/1299015.1299019.

[5] S. Egelman, L. F. Cranor, and J. Hong, “You've been warned: An empirical study of the effectiveness of web browser phishing warnings,” in Proc. SIGCHI Conf. Human Factors in Computing Systems, 2008, pp. 1065–1074, doi: 10.1145/1357054.1357219.

[6] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, “Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions,” in Proc. SIGCHI Conf. Human Factors in Computing Systems, 2010, pp. 373–382, doi: 10.1145/1753326.1753383.

[7] A. Vishwanath, B. Harrison, and Y. J. Ng, “Suspicion, cognition, and automaticity model of phishing susceptibility,” Communication Research, vol. 45, no. 8, pp. 1146–1166, 2018, doi: 10.1177/0093650215627483.

[8] C. Iuga, J. R. C. Nurse, and A. Erola, “Baiting the hook: Factors impacting susceptibility to phishing attacks,” Human-centric Computing and Information Sciences, vol. 6, art. 8, 2016, doi: 10.1186/s13673-016-0065-2.

[9] E. J. Williams, J. Hinds, and A. N. Joinson, “Exploring susceptibility to phishing in the workplace,” International Journal of Human-Computer Studies, vol. 120, pp. 1–13, 2018, doi: 10.1016/j.ijhcs.2018.06.004.

[10] P. M. W. Musuva, K. W. Getao, and C. K. Chepken, “A new approach to modelling the effects of cognitive processing and threat detection on phishing susceptibility,” Computers in Human Behavior, vol. 94, pp. 154–175, 2019, doi: 10.1016/j.chb.2018.12.036.

[11] R. Heartfield and G. Loukas, “Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework,” Computers & Security, vol. 76, pp. 101–127, 2018, doi: 10.1016/j.cose.2018.02.020.

[12] M. Bada, M. A. Sasse, and J. R. C. Nurse, “Cyber security awareness campaigns: Why do they fail to change behaviour?” in Proc. International Conference on Cyber Security for Sustainable Society, 2015, pp. 118–131.

[13] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, “Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness,” MIS Quarterly, vol. 34, no. 3, pp. 523–548, 2010, doi: 10.2307/25750690.

[14] T. Herath and H. R. Rao, “Protection motivation and deterrence: A framework for security policy compliance in organisations,” European Journal of Information Systems, vol. 18, no. 2, pp. 106–125, 2009, doi: 10.1057/ejis.2009.6.

[15] M. Siponen, S. Pahnila, and M. A. Mahmood, “Compliance with information security policies: An empirical investigation,” Computer, vol. 43, no. 2, pp. 64–71, 2010, doi: 10.1109/MC.2010.35.

[16] J. S. Downs, M. B. Holbrook, and L. F. Cranor, “Decision strategies and susceptibility to phishing,” in Proc. 2nd Symposium on Usable Privacy and Security, 2006, pp. 79–90, doi: 10.1145/1143120.1143131.

[17] D. M. Sarno, J. E. Lewis, C. J. Bohil, and M. B. Neider, “Which phish is on the hook? Phishing vulnerability for

older versus younger adults," Human Factors, vol. 62, no. 5, pp. 704–717, 2020, doi: 10.1177/0018720819855570.

[18] R. S. Dalal, D. J. Howard, R. J. Bennett, C. Posey, S. J. Zaccaro, and B. J. Brummel, "Organizational science and cybersecurity: abundant opportunities for research at the interface," Journal of Business and Psychology, vol. 37, pp. 1–29, 2022, doi: 10.1007/s10869-021-09732-9.

[19] R. T. Wright and K. Marett, "The influence of experiential and dispositional factors in phishing: An empirical investigation of the deceived," Journal of Management Information Systems, vol. 27, no. 1, pp. 273–303, 2010, doi: 10.2753/MIS0742-1222270111.

[20] Federal Bureau of Investigation, Internet Crime Complaint Center, "Business Email Compromise: The $55 Billion Scam," Public Service Announcement I-091124-PSA, Sept. 11, 2024.

[21] M. Merritt, S. Hansche, B. Ellis, K. Sanchez-Cherry, J. N. Snyder, and D. Walden, "Building a cybersecurity and privacy learning program," NIST Special Publication 800-50 Rev. 1, National Institute of Standards and Technology, 2024, doi: 10.6028/NIST.SP.800-50r1.

[22] Nepal Rastra Bank, Payment Systems Oversight Report 2080/81 (2023/2024), Payment Systems Department, Kathmandu, Nepal, 2025.

[23] Nepal Police, "Annual Factsheet on Suicide & Cyber Crime, July/August 2023 to June/July 2024," Government of Nepal, 2024.

[24] Nepal Law Commission, The Electronic Transactions Act, 2063 (2008), Government of Nepal.

[25] Nepal Rastra Bank, Payment Systems Oversight Report 2079/80 (2022/2023), Payment Systems Department, Kathmandu, Nepal, 2024.

[26] B. Bhandari, "Cybersecurity awareness amongst university students: Legal remedies and policies to mitigate risks," Unity Journal, vol. 6, no. 1, 2025, doi: 10.3126/unityj.v6i1.75557.

[27] B. P. Adhikari, A. Acharya, A. Chhatkuli, A. Ghimire, and L. Poudel, "Assessing the cybersecurity literacy proficiency among bachelor's degree students in Nepal," OCEM Journal of Management, Technology and Social Sciences, vol. 5, no. 1, 2026, doi: 10.3126/ocemjmtss.v5i1.89684.

[28] A. Sapkota and B. Paudel, "WhatsApp scams, cybersecurity awareness and digital consumer vulnerability among mobile banking users in Nepal," International Journal of Research and Innovation in Social Science, vol. 10, no. 13, pp. 520–537, 2026, doi: 10.47772/IJRISS.2026.1013COM0038.

[29] Verizon Business, 2025 Data Breach Investigations Report, Verizon, Apr. 21, 2025.

[30] Federal Bureau of Investigation, Internet Crime Complaint Center, 2024 IC3 Annual Report, 2025.

[31] M. L. Yaeger, M. G. R. Goldstein, and K. G. Monty, "The Bangladesh cyberheist: How compliance programs can help protect against cybercrime," The Hedge Fund Journal, Issue 114, June 2016. Available: https://thehedgefundjournal.com/the-bangladesh-cyberheist/.

[32] SWIFT, "Customer security issues," Customer Communication, May 13, 2016. Available: https://www.swift.com/ja/node/22556.

[33] B. M. Nturibi, "A Mobile Money Social Engineering Framework for Detecting Voice & SMS Phishing Attacks-A Case Study of M-Pesa," M.S. project report, School of Science and Technology, United States International University-Africa, 2018. Available: http://erepo.usiu.ac.ke/11732/4148.

[34] P. J. Chebii, "Securing Mobile Money Payment and Transfer Applications Against Smishing and Vishing Social Engineering Attacks," research project, University of Nairobi, 2021. Available: http://erepository.uonbi.ac.ke/handle/11295/155805.