Global Journal of STEM Education & Management Research

Cybersecurity Human Factors in Philippine Universities: Forensic Insights from Social Engineering Incidents

Renald N. Mahusay[1], Rommel M. Adricula[2], Roger D. Estampador Jr.[3]
Wayne Adrianne Obeso[4], Ma. Cristina S. Navarra[5], Jomila Cia A. Vasquez[6]
[1,2,3,4,5,6] State University of Northern Negros, Sagay City, Philippines
Corresponding Email: renaldmahusay23@gmail.com

Received: August 6, 2026
Revised: September 6, 2026
Accepted: September 13, 2026

ABSTRACT

Social engineering poses a considerable challenge to higher education institutions, with human behavior contributing to security threat identification, reporting mechanisms, and the safeguarding of evidence. This study investigated the self-reports of participants from several Philippine universities regarding their experience with social engineering attacks, which included cybersecurity, human-factor conditions, and reporting behavior. The trial was conducted from July 21 to July 29, 2026, utilizing a cross-sectional descriptive correlational survey framework using online questionnaires. Data from 130 participants was analyzed using descriptive statistics, reliability testing, Mann–Whitney U test, Chi-square test, Spearman rank correlation, and coding. Results indicated that 31.5% of participants had experienced any suspicious contact with the university while 32.3% had self-reported as having been a victim of crime. In addition, only 13.1% had reported the incident to any personnel of the university's IT or security divisions. The result of the scale assessing knowledge and recognition was noted as highly reliable ($\alpha = 0.923$; $M = 3.71$, $SD = 0.87$). The respondents with formal cybersecurity training scored significantly higher ($M = 4.03$) than those lacking this type of education ($M = 3.59$). Knowledge was strongly connected to the caution of working remotely and personal accountability regarding the safety of the university's assets. The research contributes to the field of cybersecurity governance in higher education by providing an identification of the gaps relating to human factor and reporting which may aid institutions in developing awareness programs, reporting processes and forensic readiness measures. The findings are, however, limited by the fact that the data is cross-sectional, pooled and self-reported.

Keywords: cybersecurity, digital and forensic readiness, Philippine Universities, phishing, social engineering

How to Cite:

Mahusay, R. N., Adricula, R. M., Estampador, R. D., Jr., Obeso, W. A., Navarra, M. C. S., & Vasquez, J. C. A. (2026). Cybersecurity Human Factors in Philippine Universities: Forensic Insights from Social Engineering Incidents. *Global Journal of STEM Education & Management Research*, 2(*3*), 102-117. https://doi.org/10.5281/zenodo.22732072

INTRODUCTION

Universities rely more on interconnected digital platforms to carry out teaching, research, enrollment, finance and student services, and other administrative functions. This dependence creates a complicated cybersecurity environment with a multitude of users, different devices, confidential information, and distributed IT infrastructures. Research into cybersecurity in higher education has shown that this complexity remains a significant obstacle to security management at the university level (Ulven & Wangen, 2021). Although technical measures are necessary, they cannot guarantee prevention from attacks that use human judgment, trust, emotions, and decision-making.

Social engineering attacks are based on manipulation of human factors using email, text, voice messages, and any other communication tool that would force a person to give away information or allow access or perform some actions that will be beneficial for attackers. Unlike purely technical attacks, social engineering is based on psychological influence and context. It has been proven in previous studies that vulnerability is influenced by cognitive traits, message variables, organizational context, and security culture (Desolda et al., 2022; Lain et al., 2022). Therefore, having cybersecurity awareness in its own is not sufficient for individuals to recognize the threat, react properly, and take the right steps in case of an incident.

Once a social engineering attack takes place, the consequences are felt even after the incident has occurred. Such attacks give rise to useful digital evidence, which can include emails, attachments, links, information about devices, logs of authentication, data from browsers, and so on. However, the availability of such evidence depends on how the user behaves after the attack takes place. Reporting the attack a few days after the event and deleting suspicious emails, leaving messages from the attacker without reading them, or lack of clarity regarding further reporting of the incident complicate the investigation process and evidence collection.

This issue is particularly pertinent to higher educational institutions in the Philippines, which deal with a wealth of exclusive records and personal information, which is protected under RA 10173 (Republic Act No. 10173, 2012), and are increasingly relying on digital tools for their essential operations. The National Cybersecurity Plan 2023–2028 describes cybersecurity as a national resilience issue (Department of Information and Communications Technology [DICT], 2024). In this regard, institutional cybersecurity preparedness consists of such elements as policies and technical measures, as well as the ability of users to identify suspicious behavior, know what to do to report it, trust institutions to handle the issue effectively, and contribute to evidence maintenance.

Despite increased research on cybersecurity awareness, phishing vulnerability, training, and security culture, there is still a significant gap in knowledge regarding how human factors, reporting behaviors, and forensic readiness correlate within Philippine Universities. Although previous literature looked at cybersecurity awareness as well as protective behavior against the threat of cybercrimes, limited research simultaneously analyzed awareness, reporting behavior, and forensic readiness in the Philippine HEIs. Existing studies in the Philippines mainly concentrate on cybersecurity awareness, online safety conduct, and student informants (Rotas & Cahapay, 2021; Alves-Foss & Llego, 2024) while greater literature looks at phishing vulnerability, the efficiency of training, and contextual impacts on cybersecurity conduct (Prümmer et al. 2024, 2025). As such, there is not much evidence regarding how users' knowledge and behavioral reactions, reporting choices, and understanding of the institution's ability to handle evidence come together after the occurrence of social engineering cases.

The need for forensic readiness and human factors to be studied jointly is clear because users have an impact on the earliest stages of incident detection, reporting, and evidence preservation. These are instances of users who may understand cybersecurity terminology but will still fail to recognize an attack, be slow to report an incident, or unintentionally destroy evidence crucial for investigations. Likewise, institutions may have advanced technical equipment yet still lack essential pieces of information if users fail to report incidents as quickly as possible or to preserve the necessary information.

This study analyzes the self-reported exposure to social engineering and victimization, cybersecurity awareness and knowledge, human behavioral variables, reporting behavior, cybersecurity training, as well as perceived institutional forensic readiness in a sample from selected universities in the Philippines. The study seeks to bridge the gap that exists between the human-centric cybersecurity studies and the evidence-based preparedness for incidents.

OBJECTIVES OF THE STUDY

This effort was to look at the human factors and forensic readiness concerning self-reported incidents of social engineering in selected universities in the Philippines. The study aimed to:

1. Describe the suspicious communications and the reported victimization of social engineering
2. Examine how cybersecurity knowledge, behavioral tendencies, and workplace pressures influence threat recognition, reporting practices, and evidence preservation.

3. Explore respondents' views regarding university investigation and evidence collection, procedures, response teams, reporting, and culture
4. Compare knowledge that cyber security respondents have been trained to understand
5. Investigate the links of knowledge and behavior useful in the recognition and actions to be taken.

Since the study is based on cross-sectional, pooled, and self-reported data, it aims to identify readiness needs and statistical patterns. It does not recreate the incidents that occurred or identify the attackers.

LITERATURE REVIEW

To support the studies overall framework, this literature review focuses on three core domains: human behavior in social engineering contexts, security culture and training effectiveness, and post-incident digital forensic readiness.

Human Factors in Social-Engineering Incidents

Human factors emphasize a clear gap between threat awareness, actual knowledge, and real-world behavior. Understanding a security risk in theory rarely guarantees that someone will recognize it in practice or react safely under pressure. Syntheses of phishing studies demonstrate that individual cognitive habits, specific message design cues, workplace conditions, and overall organizational culture collectively determine vulnerability (Desolda et al., 2022). This disconnect was evident in a study of Philippine university students, where general threat knowledge failed to translate into safer online habits (Rotas & Cahapay, 2021).

This gap becomes particularly dangerous during an active social engineering attempt. An individual might understand the definition of phishing yet still fall for a spoofed message that seems to originate from a professor, campus official, or IT service provider. Similarly, someone might know the proper security protocol but bypass it due to deadline stress or confusing reporting procedures. When users engage with an attacker, delete suspicious emails, or delay notifying security teams, they amplify the damage of the attack while simultaneously wiping out the digital traces critical for forensic investigation (Desolda et al., 2022; Lain et al., 2022).

Incident Exposure, Training, and Security Culture

Training is widely recognized as an effective method for lowering the risk of social engineering. Successful training is supposed to help individuals learn to spot, check, inform on and secure evidence from any dubious interaction. The latest studies have shown that training is effective in improving detection and resistance skills, provided it meets four conditions: relevance, repetitiveness, engagement and feedback; still, outcomes differ among various techniques used, targeted behavior and delay of measurements (Marshall et al., 2024; Prümmer et al., 2024, 2025).

Training works within a wider security culture. Systematic reviews identify the value of management support, clear rules, communication, and opportunities to apply security knowledge (Khando et al., 2021). Cybersecurity culture is built through regular organizational practices, not a one-time announcement (Uchendu et al., 2021). In universities, these practices include clear reporting contacts, nonpunitive reporting, timely review of incidents, preservation of original evidence, and lessons that improve future decisions.

Forensic Readiness After Social-Engineering Incidents

Prevention must be connected to incident response and investigation. The NIST Cybersecurity Framework (CSF) 2.0 organizes risk management around the Govern, Identify, Protect, Detect, Respond, and Recover functions (Pascoe et al., 2024). Current NIST guidance integrates incident response throughout these functions and treats preparation and continuous improvement as part of cybersecurity risk management (Nelson et al., 2025).

In the Philippines, university cybersecurity operates within the Data Privacy Act of 2012 and the National Cybersecurity Plan 2023–2028 (Republic Act No. 10173, 2012; DICT, 2024). Philippine research shows that student threat knowledge does not necessarily translate into protective behavior (Rotas & Cahapay, 2021), while a recent multi-university study reports varied security and privacy awareness among college students (Alves-Foss & Llego, 2024). These findings provide a national context for interpreting the present pooled survey.

Synthesis and research gap. Recent international literature explains how phishing risk is shaped by cognition, context, and training, whereas Philippine studies report awareness and protective-behavior patterns among students (Desolda et al., 2022; Prümmer et al., 2024; Rotas & Cahapay, 2021; Alves-Foss & Llego, 2024). However, the reviewed literature does not link these human factors to reporting behavior and to a university's perceived capacity to preserve and investigate digital evidence. The present study addresses this bounded gap by analyzing pooled, respondent-level indicators of exposure, knowledge, behavior, reporting, and institutional forensic readiness; it does not substitute self-reports for verified forensic cases.

This study is also informed by relevant behavioral and organizational cybersecurity perspectives, including Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), Human Factors Theory, and cybersecurity culture frameworks. These perspectives emphasize that cybersecurity actions are influenced by perceived risks, attitudes, social expectations, organizational support, and the interaction between users and security systems.

METHODOLOGY

Research Design and Forensic Interpretive Framework

The study employed a cross-sectional, multi-university, descriptive-correlational survey design. Design was descriptive as it captured characteristics of respondents, suspicious contacts, instances of victimization, reporting behavior, knowledge, human factor conditions, perceptions of institutional readiness, it was also correlational as it assessed certain distinctions and relationships regarding cybersecurity training, knowledge, reported victimization, and behavior. The respondent was the main unit of analysis.

Participants and Sampling

There was a total of 130 respondents from selected universities in the Philippines. Participants were students, professors, non-teaching personnel, and administrators from pooled university respondents; students constituted the largest group. Purposive sampling was used to reach individuals affiliated with Philippine universities and utilizing digital services in academic and administrative contexts. The participating universities were pooled and anonymized; therefore, the number of institutions and participant distribution per institution were not included because the study was designed to analyze respondent-level patterns rather than institution-level comparisons. The sample was not probability-based, and findings are limited to the respondents involved in the study.

Research Instrument

Research was conducted using an online survey. The questionnaire contained demographic questions and questions on suspicious contacts, frequency of incidents, victimization, type of crime, context of incidents, recognition of the threat and reporting of the incident; nine statements about cyber knowledge and recognition; seven statements related to human behavior and work pressure; six statements on the forensic readiness of organizations, six statements on institutional support, resources, and culture of reporting and five statements on perceived threats and their consequences; eight statements on possible means for protection. The questionnaire also included four open-ended questions where responses about the reasons why social engineering works, cases observed or experienced, recommendations for the university and other comments were collected.

Likert type 5-point scaling was used - with 5 denoting Strongly Agree, 4 denoting Agree, 3 denoting Neutral, 2 denoting Disagree and 1 denoting Strongly Disagree. Higher values meant greater agreement with the statement. Protective and vulnerability wording was found in the human factor section. Due to low internal consistency of the reverse coded safe-action construct statement it was uncovered in separate statements rather than being considered a single behavior scale. Internal consistency of multi-item domains was measured using Cronbach alpha.

Validation and Reliability

Content validity was established through expert review by three information technology education experts using a Content Validity Index (CVI). The questionnaire obtained an Item-level Content Validity Index (I-CVI) above .80 and a Scale-level Content Validity Index (S-CVI/Ave) above .80, indicating that the items were relevant, clear, and appropriate for measuring cybersecurity awareness and knowledge, behavioral practices, institutional response and forensic readiness, and risk perception among respondents.

Reliability was assessed using Cronbach's alpha for the four multi-item domains in the pooled sample. The cybersecurity awareness and knowledge domain showed excellent internal consistency (α = .911), while behavioral practices demonstrated acceptable internal consistency (α = .787). Institutional response and forensic readiness (α = .959) and risk perception (α = .956) also showed excellent internal consistency. Although the behavioral practices domain had a lower coefficient than the other domains, its alpha value remained internally coherent and suitable for analysis. Together, the CVI-based expert validation and Cronbach's alpha results support the questionnaire's appropriateness and reliability for examining cybersecurity human factors and forensic readiness in Philippine higher education.

Data Collection, Ethics, and Consent

The questionnaire was administered through Google Forms from July 21 to 29, 2026. The survey link was distributed through email and Facebook Messenger group chats to prospective respondents in selected Philippine universities. Institutional permission was obtained for data collection, participation was voluntary, and all 130 retained records indicated consent. The analysis used de-identified pooled responses and did not identify respondents or participating universities.

Ethics approval and consent to participate. The material used for this paper contained only de-identified pooled summaries. It did not include names of respondents or universities. The available files did not include the university permission documents, an ethics-review decision or approval number, participant information and consent text, recruitment procedures, or a data-retention plan. This paper therefore states only the confirmed institutional permission. It does not assume details that were not provided.

Data Analysis and Software Environment

All analyses were performed in Python 3.13.14 using pandas, SciPy, and statsmodels. Frequency and percentages summarize categorical variables, while means and standard deviations summarize Likert-type item and domain scores. Internal consistency was measured using Cronbach's alpha. Several variables were tallied to calculate the number of respondents of each group, with those sums being summarized by percentages that could themselves exceed 100%. The score for knowledge and awareness was created from the nine questions asked by all respondents. Because the distribution of scores in the trained group did not show normality, a nonparametric Mann-Whitney U test was used for comparing the two groups. In addition, Chi-square test of independence was used to survey the association of formal training and three categories of the response to victimization acts present in the study. The coefficients of Spearman were used to investigate the association of knowledge with each variable related to human factor. All analyzed statistical relationships were regarded as statistically significant only if their prior significance was established based on alphas of two-tailed test equal to .05 and Bonferroni's adjustment for relationships between knowledge and behavior of respondents was accounted as equal to .007. The interpretation of statistical significance was considered along with reliability and credibility of the study design, not just as proof for causality.

Descriptive thematic coding was used to analyze open-ended responses. Repeated concepts were put into specific classifications, and multiple themes could be assigned to one answer. Frequency of themes was utilized to enhance quantitative results. Since the documents available did not have independent coding or confirm inter-coder agreement, the obtained qualitative results were treated as subsidiary evidence instead of being treated as qualitative analysis.

RESULTS AND DISCUSSION

This section shares the findings of 130 respondents who agreed to take part in the study. The results are organized based on the study goals: reported suspicious contacts and experiences with social engineering; knowledge about cybersecurity, behaviors, and work pressure factors; readiness for forensic investigations and the culture of reporting; comparisons based on cybersecurity training; and links between knowledge and behavior. According to the design, which involved a pooled, cross-sectional approach based on self-reported data, the analyses highlight patterns at the respondent level without comparing individual universities or detailing specific incidents.

The questionnaire documentation outlined the five-point response scale as follows: 1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree. The response workbook recorded the item responses as numeric values. Accordingly, the analyses report means and standard deviations as agreement scores and do not impose additional categorical cutoffs such as "high" or "very high." Percentages may not total exactly 100.0% because of rounding.

Respondent Profile

All 130 consented records were retained for analysis. The sample was mainly students (68.5%) and respondents aged 18–24 years (71.5%); 71.5% reported no formal cybersecurity training. Figure 1 presents the full demographic and background profile graphically to make the distribution across respondent characteristics easier to read.

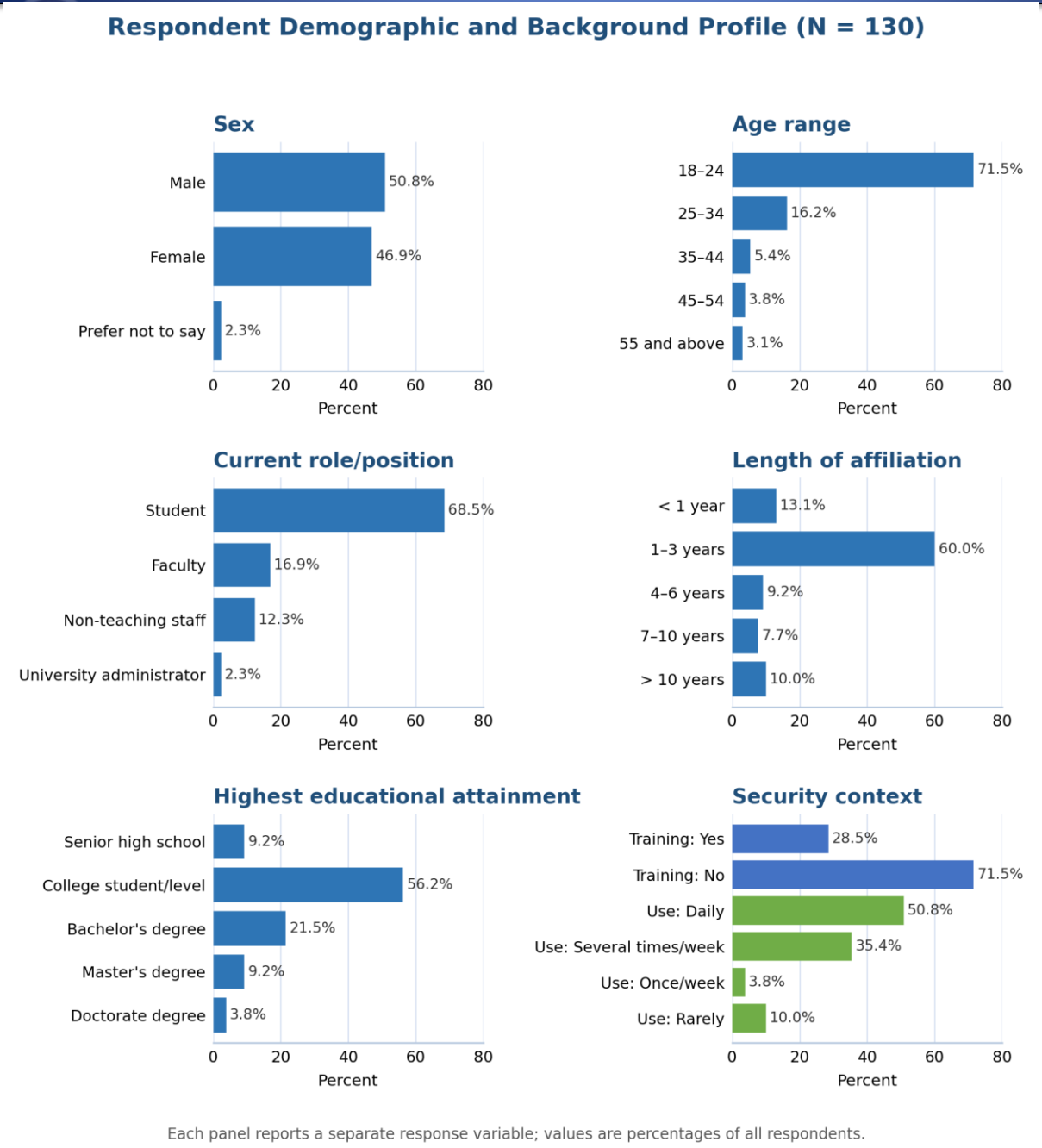

Figure 1. *Demographic and background characteristics of respondents (N = 130).*

Note. Each panel summarizes a separate response variable. Percentages are based on N = 130 and may not total 100.0% because of rounding.

Suspicious Contacts, Victimization, and Incident Reporting

Figure 2 shows that 31.5% of respondents reported receiving a suspicious university-context contact and 32.3% reported self-identified victimization. Formal reporting was much less common, with only 13.1% confirming a report to university IT or security personnel. Detailed exposure, frequency, context, and reporting values are retained in Table 1.

Among respondents who reported victimization, smishing or SMS phishing (61.9%) and email phishing (57.1%) were the most frequently selected attack types. Vishing or voice-call deception, pretexting, and baiting were less frequently selected. Percentages exceed 100% because respondents could select more than one attack type.

The reporting gap is especially important for readiness. Among respondents who explicitly answered no to formal reporting, the most common reason was that the incident seemed unimportant (53.8%); other barriers included not knowing how to report, expecting no action, and fear of embarrassment or blame.

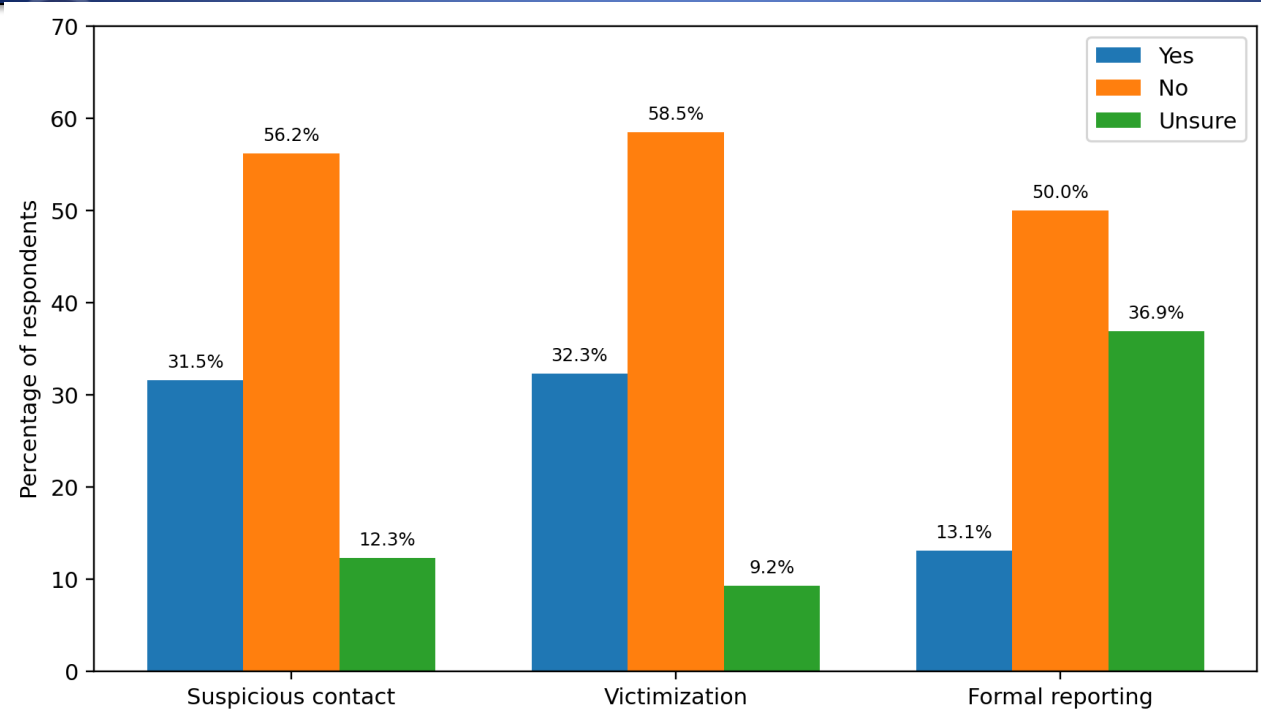

Figure 2. *Distribution of reported suspicious contact, victimization, and formal reporting responses.*

Cybersecurity Knowledge and Recognition

The knowledge and recognition scale was internally consistent (Cronbach's α = .923; M = 3.71, SD = 0.87). General awareness of common cyber threats ranked highest, whereas confidence in recognizing a social-engineering attempt ranked lowest. Knowledge of the proper reporting protocol and understanding of social engineering also fell below the overall scale mean.

Table 1

Cybersecurity Knowledge and Recognition Scores

Item	M	SD	Rank
I am aware of the common types of cyber threats (e.g., phishing, malware, ransomware).	4.24	1.10	1
I understand what social engineering is and how it works.	3.52	1.20	8
I can distinguish between a legitimate email and a phishing email.	3.85	1.07	3
I am familiar with the university's existing cybersecurity policies and guidelines.	3.73	0.99	4
I know the proper protocol for reporting a suspected cyber incident.	3.52	1.09	7
I am aware of the Data Privacy Act of 2012 and its implications for my online behavior.	3.99	1.14	2
I regularly update my passwords and use multi-factor authentication (MFA).	3.65	1.14	5
I understand the term "digital forensics" and its role in investigating cybercrimes.	3.57	1.16	6
I feel confident in my ability to recognize a social engineering attempt.	3.35	1.05	9

Note. Scores ranged from 1 to 5. Higher means indicate higher numerical agreement with each statement. Overall scale M = 3.71, SD = 0.87, α = .923.

Human Behavior and Work-Pressure Factors

The human factor items contained both protective and vulnerability-oriented statements and were therefore examined individually. Respondents reported relatively higher agreement with being more cautious when working remotely than on campus (M = 3.70, SD = 0.94) and feeling personally responsible for protecting university digital assets (M = 3.69, SD = 1.03). Among the vulnerability-oriented statements, academic deadlines taking priority over security precautions received the highest mean (M = 3.44, SD = 1.06), followed by time pressure and heavy workload causing security warnings to be overlooked (M = 3.25, SD = 1.04). Lower means were observed for fear-driven clicking (M = 2.82, SD = 1.33), trusting professional-looking emails from unknown senders (M = 2.62, SD = 1.28), and curiosity-driven opening of suspicious attachments (M = 2.62, SD = 1.36).

Table 2

Human Behavior and Work-Pressure Factors

Statement	Direction	M	SD
I tend to trust emails from unknown senders if they appear professional.	Vulnerability-oriented	2.62	1.28
Time pressure and heavy workloads may cause me to overlook security warnings.	Vulnerability-oriented	3.25	1.04
I am more cautious about cybersecurity when working remotely than on campus.	Protective	3.70	0.94
The fear of losing access to a service may push me to click suspicious links.	Vulnerability-oriented	2.82	1.33
Curiosity about an unexpected email or message has led me to open suspicious attachments.	Vulnerability-oriented	2.62	1.36
I feel personally responsible for safeguarding the university's digital assets.	Protective	3.69	1.03
Concerns about academic deadlines often take priority over security precautions.	Vulnerability-oriented	3.44	1.06

Note. For vulnerability-oriented items, a higher mean represents greater agreement with the stated vulnerability. The mixed-direction seven-item composite had limited internal consistency (α = .623); item-level findings are therefore emphasized.

University Forensic Readiness, Reporting Culture, and Resources

The six-item forensic investigation readiness scale showed high internal consistency (α = .948) and an overall mean of 3.61 (SD = 1.02). The highest-rated item was trust that the university handles reported incidents with confidentiality and professionalism (M = 4.00, SD = 1.11). The lowest-rated item concerned whether the university regularly conducts digital forensic investigations on reported incidents (M = 3.46, SD = 1.09). Perceptions of sufficient evidence collection, an established CIRT, communication of forensic findings, and a clear forensic protocol produced means between 3.51 and 3.66.

The six-item institutional support, resources, and reporting-culture scale also showed high reliability (α = .911), with an overall mean of 3.66 (SD = 0.96). Cybersecurity discussion in classrooms received the highest mean (M = 3.93, SD = 1.14), followed by encouragement to report suspicious activities without fear of reprisal (M = 3.88, SD = 1.14) and management commitment (M = 3.82, SD = 1.12). The lowest mean was recorded for the sufficiency of university cybersecurity budgets (M = 3.12, SD = 1.17).

Table 3

Perceived University Forensic Readiness and Institutional Support

Domain and item	M	SD	Domain
The university conducts regular digital forensic investigations on reported incidents.	3.46	1.09	Forensic readiness
The university collects sufficient evidence (e.g., logs, screenshots) when investigating cyber incidents.	3.66	1.13	Forensic readiness
There is a clear forensic protocol in the institution for handling social engineering cases.	3.51	1.16	Forensic readiness
The university's IT team shares forensic findings with end-users to prevent future incidents.	3.52	1.18	Forensic readiness
I trust that the university handles reported cyber incidents with confidentiality and professionalism.	4.00	1.11	Forensic readiness
The university has an established cyber incident response team (CIRT).	3.54	1.20	Forensic readiness
The university provides adequate cybersecurity training programs for all stakeholders.	3.57	1.12	Institutional support
There are visible awareness campaigns (posters, emails, seminars) on cybersecurity on campus.	3.67	1.22	Institutional support
Management and administrators demonstrate strong commitment to cybersecurity.	3.82	1.12	Institutional support

Domain and item	M	SD	Domain
Cybersecurity is discussed in classrooms as part of the curriculum (where applicable).	3.93	1.14	Institutional support
The budget allocated for cybersecurity in Philippine universities is sufficient.	3.12	1.17	Institutional support
I feel encouraged to report suspicious online activities or messages without fear of reprisal.	3.88	1.14	Institutional support

Note. Forensic readiness scale: M = 3.61, SD = 1.02, α = .948. Institutional support/resources/reporting-culture scale: M = 3.66, SD = 0.96, α = .911.

Perceived Threat and Priority Safeguards

Respondents gave comparatively high scores to the potential consequences of social engineering. The five-item threat and consequence scale had an overall mean of 4.24 (SD = 0.95; α = .956). Disruption of critical academic operations received the highest mean (M = 4.33, SD = 1.03), followed by compromise of student and faculty personal data (M = 4.32, SD = 0.97) and reputational damage affecting university standing and enrollment (M = 4.28, SD = 1.04).

The eight proposed safeguards also received relatively high scores (overall M = 4.13, SD = 1.11; α = .983). Strong authentication mechanisms ranked first (M = 4.22, SD = 1.11). Strict enforcement of data privacy and security policies and public awareness campaigns were tied next (both M = 4.18). The remaining safeguards had means from 4.04 to 4.15, showing that respondents assigned similar numerical importance to training, simulations, dedicated response capacity, curriculum integration, and accessible reporting channels.

Table 4

Perceived Consequences of Social Engineering and Priority Safeguards

Item	M	SD	Domain
Social engineering poses a serious threat to Philippine higher education institutions.	4.11	1.07	Threat/consequence
A successful social engineering attack could compromise student and faculty personal data.	4.32	0.97	Threat/consequence
A successful attack could disrupt critical academic operations (e.g., online learning, enrollment, research, tuition fee payment).	4.33	1.03	Threat/consequence
The reputational damage from a cyber incident could affect the university's standing and enrollment numbers.	4.28	1.04	Threat/consequence
Philippine universities are increasingly becoming targets of cybercriminals.	4.14	1.03	Threat/consequence
Regular mandatory cybersecurity awareness trainings	4.04	1.17	Safeguard priority
Simulated phishing exercises for students, faculty, staff and administrators.	4.05	1.20	Safeguard priority
Strong authentication mechanisms.	4.22	1.11	Safeguard priority
Establishment of a dedicated forensics/CSIRT team.	4.15	1.18	Safeguard priority
Integration of cybersecurity and digital ethics in the curriculum.	4.14	1.16	Safeguard priority
Clear, accessible reporting channels for suspicious activities.	4.10	1.23	Safeguard priority
Strict enforcement of data privacy and security policies.	4.18	1.15	Safeguard priority
Public awareness campaigns via social media and campus events.	4.18	1.22	Safeguard priority

Note. Threat/consequence scale: M = 4.24, SD = 0.95, α = .956. Safeguard-priority scale: M = 4.13, SD = 1.11, α = .983.

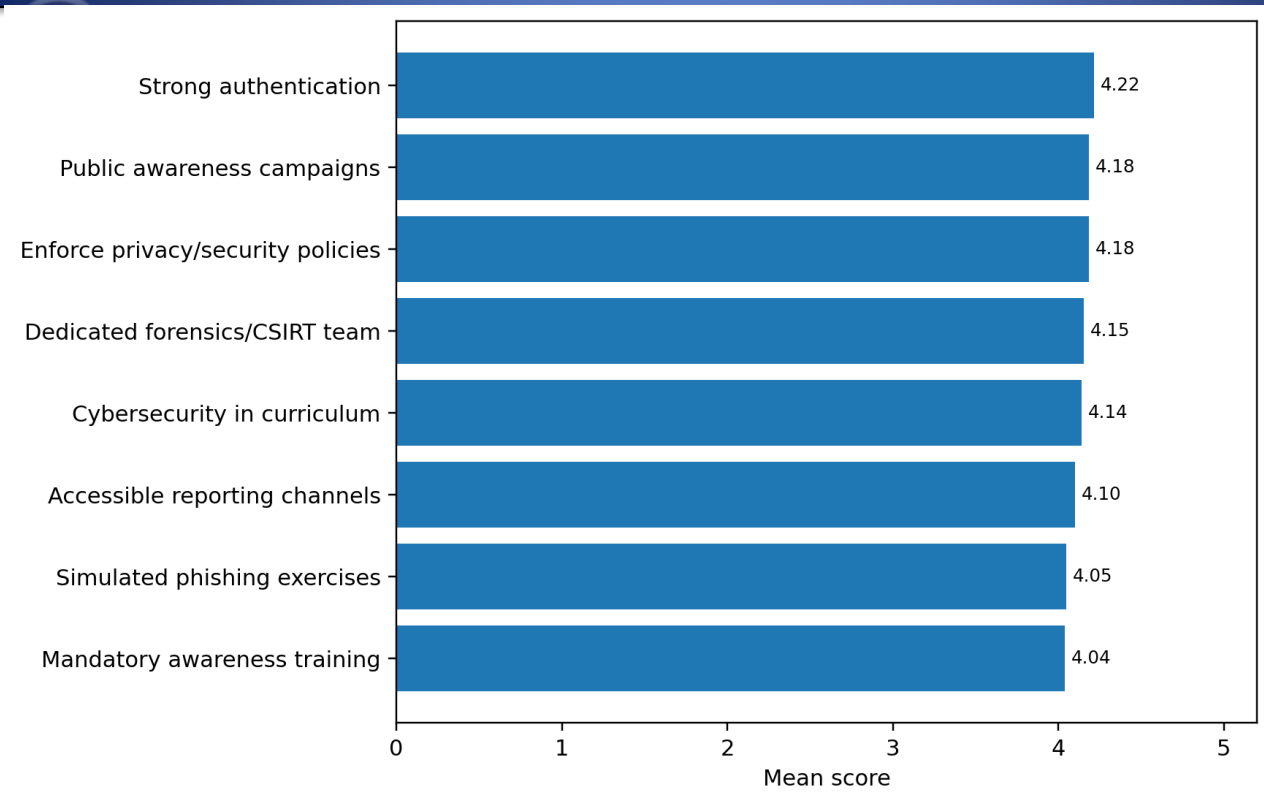

Figure 3. *Ranked mean scores for proposed safeguards against social engineering.*

Cybersecurity Training and Knowledge

Respondents with formal cybersecurity training had a higher knowledge and recognition score (M = 4.03, SD = 0.97, Md = 4.22, IQR = 3.89–4.67) than respondents without formal training (M = 3.59, SD = 0.80, Md = 3.67, IQR = 3.11–4.11). Because the trained group's scores were non-normally distributed, a Mann–Whitney U test was used. The difference was statistically significant, U = 2395.00, p < .001, with a rank-biserial correlation of .392. This represents a moderate group difference in favor of respondents who reported formal training.

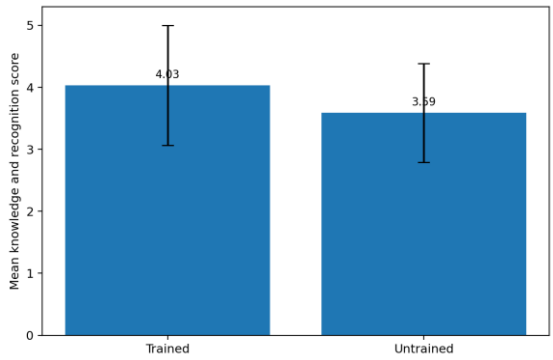

Figure 4. *Mean cybersecurity knowledge and recognition scores by training status. Error bars represent one standard deviation.*

Cybersecurity Training and Reported Victimization

The distribution of self-reported victimization did not differ significantly by training status. Among trained respondents, 14 of 37 (37.8%) reported victimization, 20 (54.1%) reported no victimization, and 3 (8.1%) were unsure. Among untrained respondents, 28 of 93 (30.1%) reported victimization, 56 (60.2%) reported no victimization, and 9 (9.7%) were unsure. The chi-square test was not significant, $\chi^2(2, N = 130) = 0.73$, $p = .693$, Cramér's $V = .075$. Thus, formal training status was not statistically associated with the three-category victimization response in this sample.

Table 5

Formal Cybersecurity Training Status by Self-Reported Victimization

Training status	Victim: Yes	Victim: No	Unsure	Total
Trained	14 (37.8%)	20 (54.1%)	3 (8.1%)	37

Training status	Victim: Yes	Victim: No	Unsure	Total
Untrained	28 (30.1%)	56 (60.2%)	9 (9.7%)	93

Note. Pearson $\chi^2(2, N = 130) = 0.73$, $p = .693$, Cramér's $V = .075$. Row percentages are shown in parentheses.

Associations Between Knowledge and Human-Factor Behaviors

Spearman rank correlations showed that knowledge was strongly associated with greater caution when working remotely and stronger personal responsibility for protecting university digital assets ($\rho = .582$, $p < .001$ for both). Knowledge was also positively associated with recognition that time pressure and heavy workload may cause warnings to be overlooked ($\rho = .306$, $p < .001$). The association with academic deadlines taking priority over security precautions ($\rho = .210$, $p = .016$) did not remain significant after the Bonferroni-adjusted criterion. Table 8 and Figure 5 present the complete pattern.

No statistically significant associations were found between knowledge and trusting professional-looking messages from unknown senders ($\rho = .075$, $p = .398$), fear-driven clicking ($\rho = .079$, $p = .369$), or curiosity-driven opening of suspicious attachments ($\rho = .100$, $p = .259$). An exploratory reverse-coded safe-action composite was also not significantly correlated with knowledge ($\rho = .042$, $p = .635$); because this composite showed limited reliability ($\alpha = .623$), the item-level correlations were retained as the primary results.

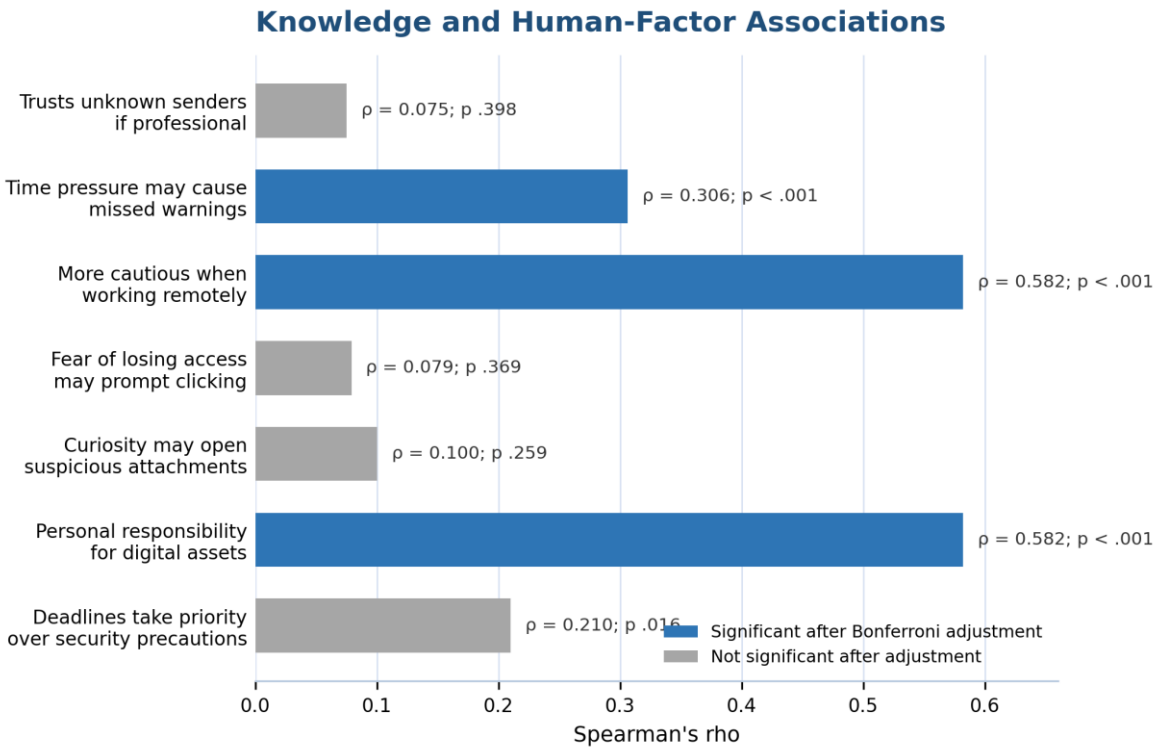

Figure 5. *Spearman correlations between cybersecurity knowledge and human-factor items.*

Note. Blue bars satisfy the Bonferroni-adjusted significance criterion ($p < .007$); gray bars do not.

Open-Ended Responses

Descriptive thematic coding of the open-ended responses supported the quantitative findings. Multiple themes could be assigned to a single response. The most frequently identified reason for successful social engineering was limited awareness, knowledge, training, or digital literacy (84 mentions, 64.6%). Trust in apparently legitimate messages and failure to verify the source was the next most common theme (45 mentions, 34.6%). Other themes included curiosity or tempting offers (13 mentions, 10.0%), urgency and workload-related pressure (12 mentions, 9.2%), and carelessness or inattention (9 mentions, 6.9%).

Incident narratives most often described phishing emails or fake messages that imitated university offices, registrars, information-technology units, scholarship programs, student organizations, or faculty members. Several responses described fake account-verification links, credential-harvesting pages, compromised social-media or email accounts that subsequently messaged classmates, fake scholarship or job offers, and impersonation attempts seeking access to student information. Many respondents also stated that they had not personally witnessed a university-related incident.

Suggested improvements were dominated by awareness campaigns, education, seminars, and training (90 mentions, 69.2%). Respondents also proposed multi-factor or two-factor authentication (19 mentions, 14.6%), stronger technical controls and infrastructure such as email filtering and secure networks (17 mentions, 13.1%), simulated phishing and practical drills (16

mentions, 12.3%), clear reporting channels and response procedures (12 mentions, 9.2%), and dedicated cybersecurity or incident-response personnel (5 mentions, 3.8%).

Table 6

Themes Identified in the Open-Ended Responses

Question area	Theme	Mentions	% of respondents
Reasons for victimization	Limited awareness, knowledge, training, or digital literacy	84	64.6
	Trust in apparently legitimate messages and failure to verify	45	34.6
	Curiosity, rewards, financial lures, or tempting offers	13	10.0
	Urgency, workload, stress, deadlines, or fear	12	9.2
	Carelessness, complacency, or inattention	9	6.9
Suggested improvements	Awareness campaigns, education, seminars, and training	90	69.2
	Multi-factor/two-factor authentication and stronger account protection	19	14.6
	Technical controls, email filtering, secure Wi-Fi, and infrastructure	17	13.1
	Phishing simulations and practical drills	16	12.3
	Clear reporting channels and incident-response procedures	12	9.2
	Dedicated cybersecurity, CERT, CSIRT, or specialist team	5	3.8

Note. Multiple coding was permitted, so percentages do not sum to 100%. Counts represent descriptive theme mentions from the 130 open-ended responses. This subsection should be retained only when the Methods section states that open-ended answers were analyzed through descriptive thematic coding.

Summary of Results by Study Objective

First, approximately one-third of respondents reported suspicious contact or victimization, but only 13.1% confirmed formal reporting. Second, respondents showed stronger numerical agreement with general threat awareness than with confidence in recognizing social engineering and knowledge of reporting procedures. Workload and academic deadlines emerged as the most prominent pressure-related vulnerability statements. Third, respondents expressed comparatively greater trust in confidentiality and classroom integration than in regular forensic investigations and sufficient cybersecurity budgets. Fourth, formally trained respondents had significantly higher knowledge and recognition scores, but training status was not associated with self-reported victimization. Fifth, knowledge was positively associated with remote caution, personal responsibility, and recognition of workload-related risk, but it was not associated with all vulnerability behaviors. These findings describe pooled self-reported patterns and do not establish causation or university-level differences.

The research investigated social engineering issues with respect to human behavior and forensic readiness at the organizational level. The findings indicate that there existed a consistent gap between the study participants' general understanding of the importance of cybersecurity and the threat detection capabilities of the respondents. Such a gap is significant because forensic and incident-response capabilities can only be effective when timely actions are carried out by humans. Even the most technologically advanced organization can miss potentially important leads due to lapses in reporting or ignoring suspicious messages.

Reported Exposure, Victimization, and the Reporting Gap

About one-third of the respondents either acknowledged being contacted fraudulently regarding university-related business or noted they had been victimized in some way. The fact that there is virtually no difference between the two figures (31.5% and 32.3% respectively) would probably suggest that the respondents thought about the two questions in a somewhat different light. It is possible that some individuals might start thinking of themselves as crime victims only after access to their account or other losses, while some other responses might refer to criminal contact without the respondents' feeling victimized.

The victims described how they had primarily been attacked by text messages and emails as the most prevalent strategies used against them. This does reinforce the idea that the respondents would prefer to communicate with the university via mobile phones and emails, but the survey did not address the communication channels of the attacks used. The incidents described

included messages that were like emails from universities and such departments as registrar or IT department, scholarships, and student organizations, etc.

One major issue of concern in terms of readiness is the low extent of formal reporting. It became evident from the investigation that just 13.1% of the respondents said they issued a report to the university information technology/security officers regarding the incident, while exactly half of them answered "No" and one-third were rather unsure of what to say. The main motive of the respondents that chose "No" was that the action was not deemed to be worthy of paying attention to. Other reasons for such reluctance included not knowing how the information should be passed on, thinking that nothing would happen because of this action, and fearing the stigma of being blamed for passing the information on. Such behavior confirms the modern incident response process, which encompasses the stages of preparation, reporting, response, and recovery in the context of risk management (Nelson et al., 2025). From the point of view of forensic analysis, any challenges at any of these stages will delay the fact of receiving the initial message and collecting the important evidence, including activity data and logs.

Knowledge, Recognition, and Work-Pressure Factors

The respondents showed an evident inclination to accept augmented awareness about cyber threats and the Data Protection Act more than they possess proficiency and confidence in recognizing social engineering and reporting sessions. This gap is of considerable importance. The concept of awareness refers to the overall knowledge of the subjects concerning the idea while proficiency, confidence, and knowledge of procedures refer to being able to make decisions in real-life situations concerning deceit. For this reason, it turns out that awareness programs need to stop talking about definitions and policies and instead provide concrete skills concerning the ability to recognize, prove the legitimacy of any act, report an incident, and preserve evidence.

When it comes to workload and academic deadlines, these are the major reasons for vulnerability. Respondents said they were more willing to acknowledge that the pressing nature of workload or deadlines can lead to not noticing warnings instead of trusting messages that look trustworthy, as they either avoided them due to fear or opened attachments due to curiosity. This fact might reflect differences in real behavior as a different implication could be that citing workload as a reason for endangerment is more socially acceptable than admitting that one makes mistakes. Human factors studies suggest that phishing decisions are influenced by context, focus, message clues, and mental effort of a person instead of being solely based on a person's phishing knowledge (Desolda et al., 2022; Lain et al., 2022). As a result, universities should work on creating mechanisms that would work under the strain of deadlines.

Perceived University Forensic Readiness and Security Culture

Despite the generally positive perception of readiness of the institution, there are large differences when it comes to the indices themselves. The highest average of the indices was counted with trust in evidence confidentiality, creating attractivity for reporting purposes. People are more inclined to share their mistakes in case they expect that their privacy will be considered. However, a lot of other activities including regular forensic checks, application of forensic procedures, setting up teams for incident response and having enough funds for cybersecurity appeared to be evaluated lower than was expected.

Among various categories, aspects like guidance on cybersecurity, incentives to report incidents freely, and commitment from the management received a higher score than sufficient budget. It follows from this that the respondents have been able to notice some cultural and educational initiatives already present in the company despite believing that it lacks sufficient financing. This is, in fact, a primary principle of cybersecurity culture since it works through the right combination of leadership, communication, training, instructions, and shared responsibility in the company (Uchendu et al., 2021). Still, the presence of good culture must be coupled with trained personnel as well as logging and data storage capabilities, formalized processes, and containment and evidence management tools.

Training, Knowledge, and Reported Victimization

According to the survey, respondents who had undergone training in cybersecurity matched much higher recognition and performance scores than those who were not trained. The finding clearly underlines what structured education means in cybersecurity. The open-ended comments provided some confirmation of this idea since people mentioned awareness, education, and training as the main tools that could be employed to improve the situation.

It has been observed that there may be a correlation between the presence of training and reports of victimization, but it is incorrect to conclude that training is ineffective. The use of surveys in making such determinations may not advance knowledge with regard to the periods of training, the length of the training, the character of training, or the content of training for that matter. Those who received training might have been placed in a role that required them to be more aware of the system, or they may simply be more familiar with social engineering and its consequences. As shown by research into phishing training, effectiveness of the training is determined by elements such as timing and repetition regarding content practiced in real life situations.

It would be improper to make direct numerical comparisons to recent studies since the samples, constructs, and outcomes differed. Conversely, the pattern presented converges with a Philippine study conducted in 2021 which did not find a significant correlation between knowledge of threats and protective behavior (Rotas & Cahapay, 2021) and with a multi-university Philippine study conducted in 2024 which indicated that there is no correlation between security and privacy awareness and the characteristics of the respondents (Alves-Foss & Llego, 2024). The recent international studies also show that the effects of training depend on the nature of the instruction, measuring of results, and strengthening (Marshall et al., 2024; Prümmer et al., 2024, 2025). This paper is the continuation of the provision of evidence that connects training and human factors with self-reported victimization, reporting, and perceived forensic preparedness.

Knowledge-Behavior Relationships

Knowledge was found to have a strong correlation to the level of caution exercised in remote working habits and the level of personal responsibility in protecting university cyber assets. Knowledge was also connected with awareness of the possibility of ignoring security warnings due to workload. The relationships between the variables suggest that knowledgeable participants are more aware of their protective duties and the environmental risk. The positive correlation between workload and effective behavior suggests that the influence of knowledge on risky actions should not merely be seen as direct causation but as an ability of knowledgeable people to be aware of their workload as a risk and act accordingly, rather than in the manner associated with the concept.

Knowledge does not have a significant relationship with any type of behavior associated with vulnerability. It proves to have no relation to trust in messages that look professional, clicking that is motivated by fear, and opening messages due to curiosity. The exploratory safe-action index does not correlate with knowledge and has questionable reliability in general. Thus, it is possible to conclude that the difference between the knowledge of cyber security principles and acting correctly in stressful situations has been demonstrated in.

Implications for Forensic Readiness

It has been stated that it is essential to use an institutional strategy with different layers that take ranked safeguards into account. During the research, it was revealed that the factors of authentication, making and implementing of a privacy and security policy, the Internet public awareness and the ability to address the investigative aspects of the problem gained the highest average mark. All these factors are interdependent. For example, authentication can minimize the consequences of credential theft but will not prevent the original fraud. Awareness may not be enough to guarantee that the message will be properly sent. One can investigate provided that there are monitoring and logging opportunities.

According to the guidelines presented by NIST, it is critical to include forensic technologies in the incident management instead of separating the process of evidence gathering from incident management process (Nelson et al., 2025). Thus, universities ought to determine the incidents to be reported; employ mechanisms to report incidents with ease; protect all kinds of communications, including messages, screenshots, headers of emails, addresses of the webpages visited, usernames and log ins, and the appropriate system log files; guarantee that logging is carried out properly; and ensure that the lessons learned are shared without disclosing the identity of the sources of the information. The fact that confirmation of reports is minimal and there is not much knowledge about the proper ways to report on incidents points to the necessity of informing the public about these aspects instead of hiding them in the technical documentation.

Limitations

There were several restrictions on the results of this research. One restriction was from purposeful sampling and not knowing how many people responded to see the generalizability of the results. It was not possible to account for the number and types of institutions where participants were recruited from and to calculate participants' representation. There was a lack of variety among participants making it hard to analyze results by demographics due to the dominant number of those aged from 18 to 24 years of age and those who haven't worked for longer time periods.

The fact that every single piece of relevant data including exposure, victimization, education, reporting as well as the readiness of institutions among others - was reported by the respondents means that the definition of the concepts and ideas used in the questionnaire coupled with recall and social desirability problems conflict with the very nature of the cross-sectional design. Fourthly, one cannot say that this survey had been intended to obtain all the details of the events, including any digital records, their timeframes, the impacted systems, the number of damages incurred, actions taken and consequences confirmed. Fifthly, as far as training is concerned, it is only presented as binary variable in this study without specification of its time, duration and any other important information. Finally, the quality of the data gathered raises concerns since mixed-item behavior measures are of low reliability and thus do not allow making a credible analysis of the results.

Ultimately, the questionnaire underwent expert validation, pilot trialing, and indicated a range of internal consistency levels from acceptable to excellent. The research is based on data obtained from self-report surveys, which means that the results might

include recall, response, and social desirability bias. Therefore, the conclusions represent the perceptions and experiences of the respondents and not verified cases related to social engineering.

CONCLUSION

The study investigated the aspects of social engineering knowledge and exposure, cybersecurity knowledge, and human behavioral mechanisms including reporting practices and the way subjects perceive forensic readiness. It turned out that roughly one-third of respondents reported suspicious contacts or self-declared victimization cases although formal reporting to university IT and security personnel has been rare. The respondents were found to express a relatively positive attitude toward general cybersecurity awareness, while no good results were shown in their confidence in identifying social engineering and knowing way to report the events.

Those respondents who had been through formal cybersecurity training scored significantly higher in terms of knowledge and identification of the problem as opposed to those without it; nevertheless, the training factor was not related to self-reported victimization. Knowledge was positively correlated with higher caution in remote work, personal responsibility for safeguarding university assets, and identification of security risks related to workload, but it was not significantly correlated to many vulnerability-related behaviors.

Views on college readiness were mostly positive, especially concerning privacy and professionalism in dealing with reported issues. However, less positive responses were recorded on questions regarding the regularity of cyber investigation practices and appropriateness of cybersecurity budget. Overall, the results indicate that universities in the Philippines should dedicate more effort to building appropriate degrees of knowledge of threats, reporting processes, preservation of evidence, and reaction skills.

As this study involved pooled cross-sectional self-reported data, the results reflect the level of perception and experience of respondents rather than confirmed cybersecurity incidents or institutional comparisons. It is advisable for future studies to use probability sampling and make institutional-level studies to gain more knowledge on the human factor of cybersecurity and readiness for investigations in Philippine higher education institutions.

RECOMMENDATIONS

1. A centralized mechanism for reporting cybersecurity incidents should be set up. All the university stakeholders should be informed about it properly. Such a mechanism may include an online form, email, or a hotline, while providing clear instructions on how to deal with suspicious messages, compromised accounts, and how to preserve evidence.
2. Formal incident response procedures in the matter of cyber security should be developed and tested regularly. These procedures should ensure that everything is clear in terms of responsibilities, communication methods, evidence preservation, as well as recovery and escalation processes. There must be tests and simulations so that one can verify and improve the level of preparedness of the institution.
3. It is important to have understanding and practical knowledge of cybersecurity issues through various training sessions and making students, faculty, administrators, and staff, aware of actions to take during cybercrime situations.
4. Enhance preventive and technical security measures, it is essential to employ multi-factor authentication mechanisms, secure account recovery options, mail and message filtering, antivirus and link verification controls, centralized logging, phone monitoring, management of access rights, and timely revocation of unauthorized rights. The abovementioned tools will contribute to ensuring proactive threat prevention and effective investigation of security incidents.
5. It is necessary to organize a Cybersecurity Incident Response Team (CIRT/CSIRT) or an equivalent institution with personnel competent in cybersecurity incidents, appointed authority, functioning coordination tools, and digital forensics capacity. The incident reporting procedures need to ensure confidentiality and assist in timely reporting.
6. Periodic evaluations of institutional cybersecurity and forensic preparedness should be carried out via analysis of a range of performance indicators including time taken to report an incident, length of time before incident response is achieved, results of phishing simulation results, knowledge retention after training, efficiency of evidence gathering, and lessons learnt from earlier incidents. Future research must compare the findings from the surveys that have been carried out to institutional records and cyberinfrastructure benchmarks to strengthen the evidence of preparedness.
7. Future studies must utilize probability sampling and institutional analysis to improve the generalization of findings. Future studies must concentrate on the large-scale samples from many institutions to enable meaningful comparisons of cybersecurity awareness, reporting practices, and forensic preparedness. Institutional-level analysis must provide a deeper understanding of the effect of institution policies and resources on the level of preparedness.

Conflict of Interest

The authors declare that there are no conflicts of interest regarding the publication of this study. The research was conducted independently, and no financial, commercial, or personal relationships influenced the design, data collection, analysis, interpretation, or reporting of the findings.

REFERENCES

Alves-Foss, J., & Llego, B. G. (2024). Internet security and privacy awareness among college students in the Philippines. In 2024 IEEE Cyber Science and Technology Congress (CyberSciTech) (pp. 132–137). IEEE. https://doi.org/10.1109/CyberSciTech64112.2024.00030

Department of Information and Communications Technology. (2024). National Cybersecurity Plan 2023–2028. https://cms-cdn.e.gov.ph/DICT/pdf/NCSP-2023-2028-FINAL-DICT.pdf

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, 1–35. https://doi.org/10.1145/3469886

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees' information security awareness in private and public organisations: A systematic literature review. Computers & Security, 106, 102267. https://doi.org/10.1016/j.cose.2021.102267

Lain, D., Kostiainen, K., & Čapkun, S. (2022). Phishing in organizations: Findings from a large-scale and long-term study. In 2022 IEEE Symposium on Security and Privacy (SP) (pp. 842–859). IEEE. https://doi.org/10.1109/SP46214.2022.9833766

Marshall, N., Sturman, D., & Auton, J. C. (2024). Exploring the evidence for email phishing training: A scoping review. Computers & Security, 139, 103695. https://doi.org/10.1016/j.cose.2023.103695

Nelson, A., Rekhi, S., Scarfone, K., & Souppaya, M. (2025). Incident response recommendations and considerations for cybersecurity risk management: A CSF 2.0 community profile (NIST Special Publication 800-61 Revision 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3

Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Prümmer, J., van Steen, T., & van den Berg, B. (2024). A systematic review of current cybersecurity training methods. Computers & Security, 136, 103585. https://doi.org/10.1016/j.cose.2023.103585

Prümmer, J., van Steen, T., & van den Berg, B. (2025). Assessing the effect of cybersecurity training on end-users: A meta-analysis. Computers & Security, 150, 104206. https://doi.org/10.1016/j.cose.2024.104206

Republic Act No. 10173. (2012, August 15). Data Privacy Act of 2012. https://www.lawphil.net/statutes/repacts/ra2012/ra_10173_2012.html

Rotas, E., & Cahapay, M. (2021). Does threat knowledge influence protective behaviors of students in the context of cyber security in remote learning amid COVID-19 crisis? Journal of Pedagogical Sociology and Psychology, 3(1), 45–53. https://doi.org/10.33902/JPSP.2021167595

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. Future Internet, 13(2), Article 39. https://doi.org/10.3390/fi