GAS Journal of Engineering and Technology (GASJET)

Volume 2, Issue 3, 2025 Journal Homepage: https://gaspublishers.com/gasjet-home/ ISSN: 3048-5800
Email: editor@gaspublishers.com

Student Perceptions of Social Engineering Attacks: A Survey-Based Analysis

Christine Joy Yap[1], Roxan C. Dela Cruz[2], Kristine Soberano[3]

[1]State University of Northern Negros, Sagay, Negros Occidental

Received: 09.06.2025 | **Accepted:** 01.07.2025 | **Published:** 02.07.2025

***Corresponding Author:** Christine Joy Yap

DOI: *10.5281/zenodo.15792783*

Abstract

Review Article

The emergence of social engineering attacks has been a growing concern for cybersecurity because these attacks abuse human behavior instead of exploiting the weaknesses of technology. College students are prime targets because of their extensive use of technology and social media use along with limited formal training in cybersecurity. The purpose of this study is to explore college students' perceptions, awareness, and behaviors of social engineering threats. A descriptive survey design was applied and involved 250 students enrolled in a range of different academic programs and year levels at Trinidad Municipal College. The data was collected using a validated researcher-developed questionnaire and analyzed using SPSS with descriptive and inferential statistics. The survey measured students' current awareness about social engineering techniques; students' previous experiences with suspicious-looking content; and students' self-reported cybersecurity practices. Results indicated that although 90% of respondents routinely used the internet and 97% used social media, only 63.6% had a previous knowledge of social engineering. A large number of respondents, 83.4%, also indicated they received suspect messages - most frequently phishing scams according to previous surveys - but by far the majority chose to ignore them as opposed to taking proactive action. The statistical analysis does not show any significant correlation between demographic data and either awareness or confidence levels, but 91% of students in this study displayed a strong interest in receiving literacy education related to cybersecurity. The results suggest that while students show some level of awareness, they have neither the confidence nor experience to identify and respond to social engineering threats effectively. The recommendation is to promote structured cybersecurity education across all academic courses and programs, especially for students not in IT-related programs. More engaging, peer-led programs and using verified/current online platforms by the institutions would help students develop digital resilience.

Keywords: Cybersecurity Awareness, Phishing Attacks, Social Engineering, Student Perception, Survey-Based Research.

Citation: Yap, C. J., Dela Cruz, R. C., & Soberano, K. (2025). Student perceptions of social engineering attacks: A survey-based analysis. *GAS Journal of Engineering and Technology (GASJET)*, *2*(3), [1-10].

INTRODUCTION

Nowadays, social engineering attacks emerge as the most careful and effective among the so-called security threats that face the world. Whereas normal cyber-attacks exploit technical vulnerabilities, social engineering manipulates human nature by deception, trickery, and trust in order to obtain confidential information or gain unauthorized access to systems.. Social engineering attacks take different forms, including phishing emails, pretexting, baiting, and tailgating, and could prove hard to detect as they typically are individual and subtle. As a result, even individuals with basic cybersecurity knowledge can fall victim to these tactics [1].

Students constitute an extremely vulnerable target in social engineering situations. Their continuous use of digital media, active engagement of social media platforms, and access to online communication tools make them vulnerable to cybercriminals. Additionally, the learning environment itself is usually devoid of comprehensive cybersecurity training, which makes students incapable of recognizing and responding to social engineering attacks. Many students may not fully understand the concept of social engineering or its implications, which increases their susceptibility to these types of attacks [2].

Understanding student views of social engineering is important because of many reasons. To begin with, this helps in gauging their current situations regarding skills and information that they already have. On the other hand, it helps in understanding their attitudes towards cybersecurity and the behaviors that potentially keep them at risk. It can also indicate the directions in which the efforts related to training and raising awareness could be more effective if the intervention would be in educational establishments. From the data collected from students, some useful information can be extracted for improving researchers' and educators' targeted training activities.

This research primarily aims to investigate and analyze the students' perception of social engineering attacks via a survey-based methodology. The study will identify the awareness level, knowledge about the tactics of social engineering, and if students have had any experience with such attacks. Moreover, the study will examine whether students feel that they run the risk of falling prey to social engineering attacks and how confident they feel about identifying suspicious activities and what they would do in response to potential threats.

The survey is designed for the purpose of spreading among a wide range of students with various academic backgrounds so that we can be sure that the received data is wide and relevant. Analyses will be conducted which will help define the tendencies, uncover knowledge gaps, and reveal the relationships between perception and behavior in the collected data. Some of the factors like age, gender, the field of study, and the frequency of use of the Internet will be taken into account as well to comprehend how these factors make an impact on the social engineering perceptions.

The final objective of the study is to present the findings, which will supplement the existing knowledge base of cybersecurity education. Through the identification of the concerns and weaknesses of students, this study will supply recommendations for educational institutions, enhanced by which the policymakers and cybersecurity experts will develop and work out the issues.

In this way, the information gained can be used for carrying out interventions that not only expand the knowledge on the topic but also empower students to be able to protect themselves from the social engineering threats present in the digitalized world.

OBJECTIVES OF THE STUDY

The primary aim of this study is to explore and analyze students' perceptions of social engineering attacks with the intent of understanding students' awareness, experiences, and behavioral responses to the given cybersecurity threat. The research seeks to ascertain the extent to which students recognize different social engineering methods-the likes of phishing, baiting, and pretexting-and how confident they are in identifying and avoiding such attacks. More importantly, the study intends to highlight the knowledge gap among students, study relevant factors that might predispose them to attacks, such as age, educational background, and digital behavior, and evaluate their preparedness in responding to such threats. The different survey data collected among a diverse student sampling should provide the needed insight for educational strategies and awareness programs that can equip academics with improved cyber preparedness.

MATERIALS AND METHODS

Research Design

This research employed a descriptive survey research design to evaluate the awareness, perceptions, and behavioral reactions of Trinidad Municipal College students towards social engineering attacks. The descriptive design was chosen for its efficiency in gathering quantifiable and descriptive data using a structured questionnaire to identify patterns, trends, and relationships within the target population.

Sampling Technique

A purposive sampling method was utilized to choose the respondents from the Trinidad Municipal College student population. This non-probability sampling technique was adopted to guarantee participation by individuals with different academic profiles, digital literacy levels, and experience with online platforms. The sample size target was around 250 students covering various courses, year levels, and genders. Students were also qualified to be included if they were enrolled students of the institution and actively using digital technologies like email and social media.

Instrument Development and Validation

The main data collection instrument was a researcher-made questionnaire developed based on a review of existing literature and previously used instruments in similar studies. The questionnaire was divided into sections covering demographic data, awareness of social engineering tactics, personal experiences, and behavioral responses to suspected threats.

Since the questionnaire was not standardized, it underwent a content validation process by three experts in cybersecurity and educational research. Their feedback was used to revise unclear items and ensure that the content accurately reflected the study’s objectives. A pilot test was conducted with 20 students to assess reliability. Based on the results, Cronbach's alpha was calculated, and the instrument showed an acceptable reliability coefficient ($\alpha = 0.84$), indicating consistency in the responses.

Data Collection Procedure

Prior to data gathering, formal approval was obtained from the relevant academic offices of Trinidad Municipal College. Students were given an informed consent form outlining the purpose of the study, their rights as participants, and the voluntary and confidential nature of their participation. The finalized questionnaire was distributed online via Google Forms, depending on the respondents' access and convenience. Data collection occurred over a two-week period in May 2025.

Data Analysis

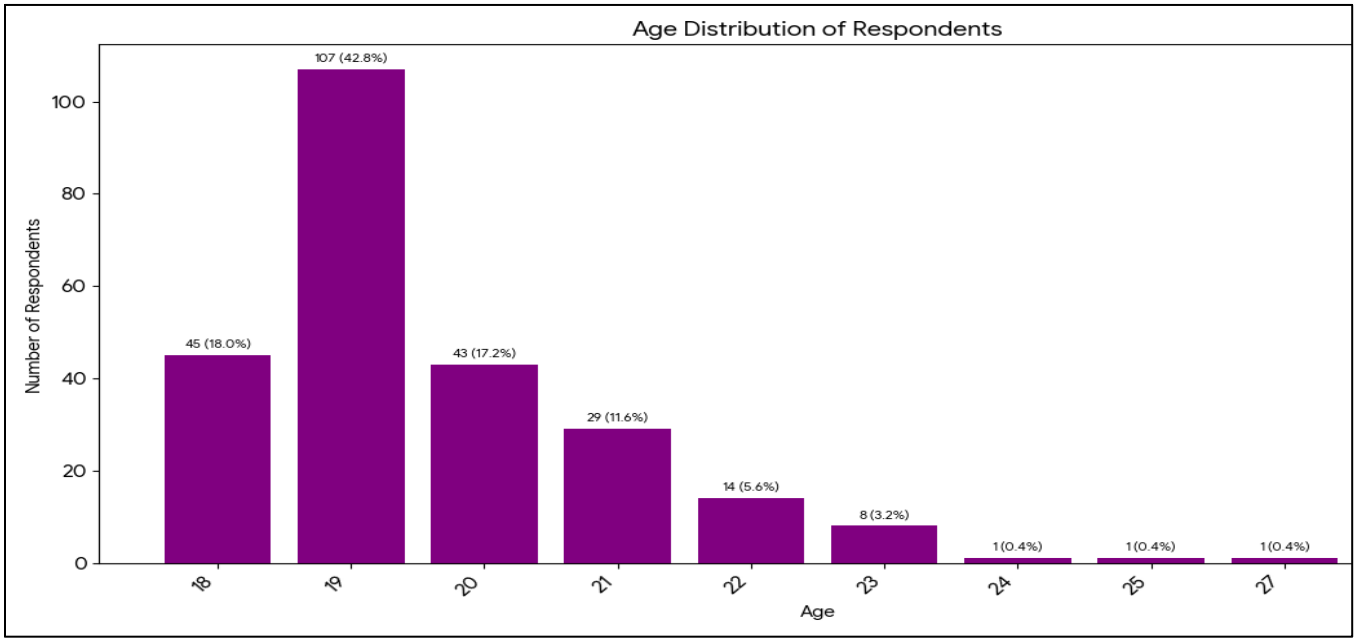
After collection, data were cleaned, coded, and entered into Statistical Package for the Social Sciences (SPSS) for analysis. Descriptive statistics such as frequencies, percentages, and means were used to summarize the demographic information and general awareness levels. Inferential statistics, such as chi- square tests and independent t-tests, were used to examine relationships between demographic variables and awareness or behavior scores. Graphs and tables were used to present data clearly and meaningfully.

Ethical Considerations

This study upheld ethical standards throughout its conduct. Participants were informed about their voluntary participation and their right to withdraw from the study at any point in time without incurring any penalties. The entire study maintained anonymity and confidentiality, and no information that might identify the participants was collected. The study protocol was reviewed and approved by the Academic President of College of Administration for the different department, which ensured that ethical guidelines were complied with. All data collected were stored securely and used only for academic purposes.

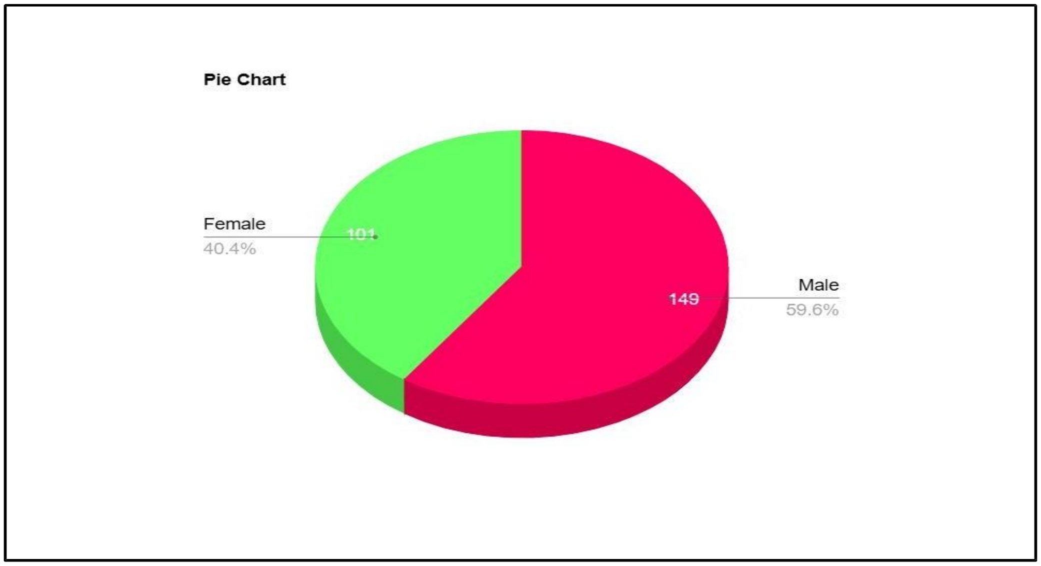
RESULTS AND DISCUSSION

Figure 1. Age group Analysis



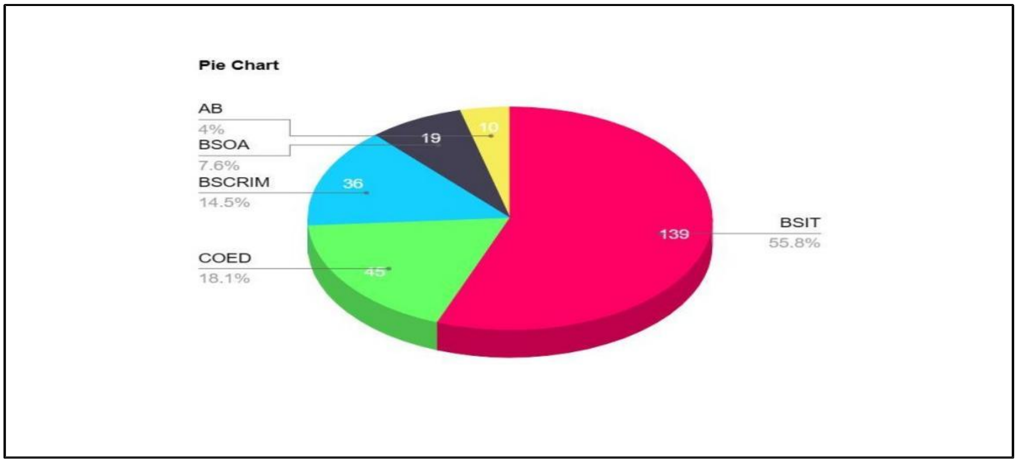
The age distribution revealed that the majority of participants were 19 years old (42.8%), followed by those aged 18 (18.0%) and 20 (17.2%). This suggests that a large portion of the respondents were in their first year of college. This early stage in their academic journey typically corresponds with limited formal instruction in cybersecurity concepts. According to Abdulla et al. [3], younger populations are more digitally active but often lack the cognitive maturity and critical experience to identify and respond to social engineering threats effectively. These findings reinforce the need to integrate cybersecurity education early in the curriculum to equip students with fundamental digital defense mechanisms.

Figure 2. Gender group Analysis



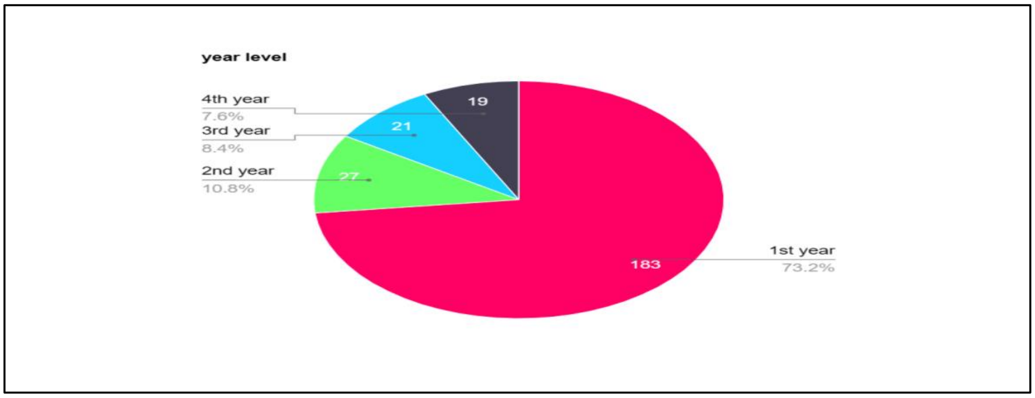
Of the respondents, 59.6% identified as male, while 40.4% identified as female. Statistical analysis (chi-square tests) showed no significant relationship between gender and cybersecurity awareness ($p > 0.05$). This supports the findings of Albladi and Weir [4], who concluded that gender does not significantly influence susceptibility to social engineering attacks. Hence, awareness campaigns and training programs should be designed to address all genders equally without making assumptions about digital literacy based on gender identity.

Figure 3. Courses Group Analysis



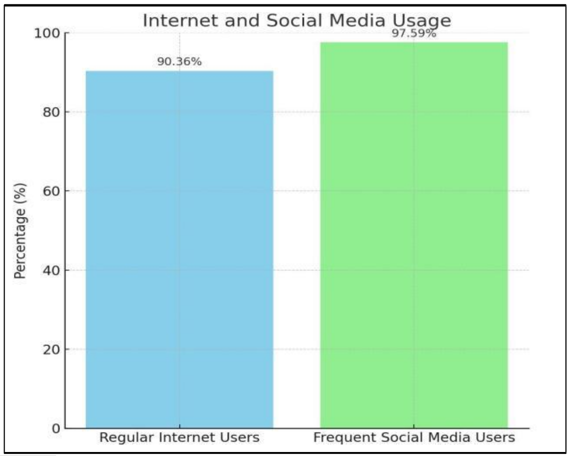
More than half of the respondents (55.8%) were enrolled in the Bachelor of Science in Information Technology (BSIT) program. Despite this, awareness gaps regarding social engineering techniques were still prevalent. This is concerning, as students in technology-related courses are expected to have higher exposure to cybersecurity concepts. Alsulami et al. [5] similarly found that even technically trained students often overlook social engineering threats due to insufficient practical exposure. This highlights the necessity of embedding dedicated cybersecurity units—particularly on social engineering—across all disciplines, including non-IT programs.

Figure 4. Year level group analysis



First-year students accounted for 73.2% of the sample, which may reflect their higher availability or responsiveness to online surveys. However, their overwhelming presence underlines a strategic opportunity: early academic engagement can be leveraged to foster foundational cybersecurity skills. Institutions can maximize impact by introducing structured digital safety programs during the first year, when students are still forming online habits and attitudes toward risk [6].

Figure 5. Internet and Social Media Usage

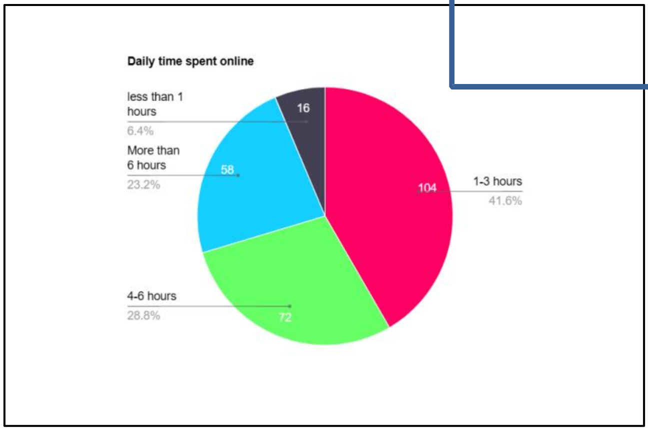


The image part with relationship ID rId21 was not found in the file.

Regular Internet Use:

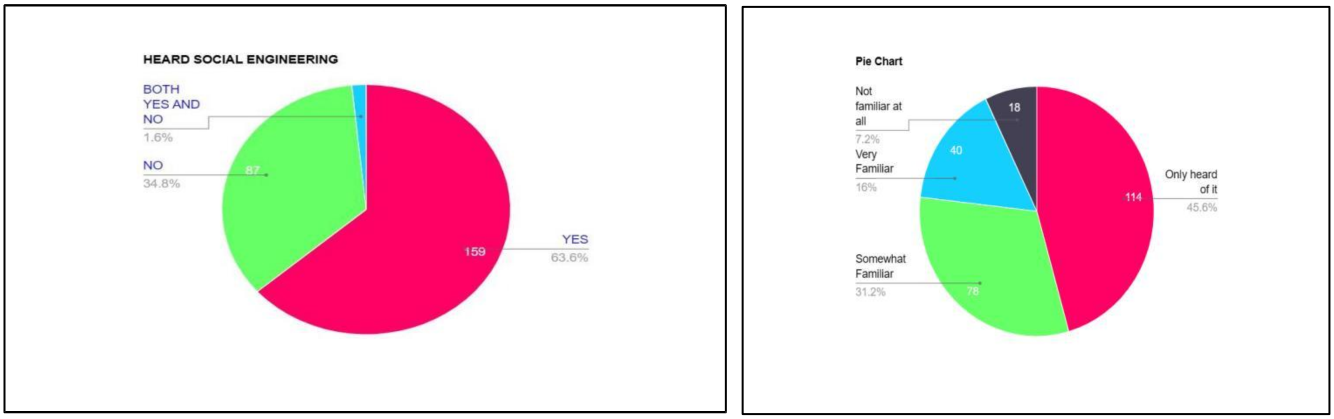
Yes: 225 (90.36%)

No: 25 (9.4%)



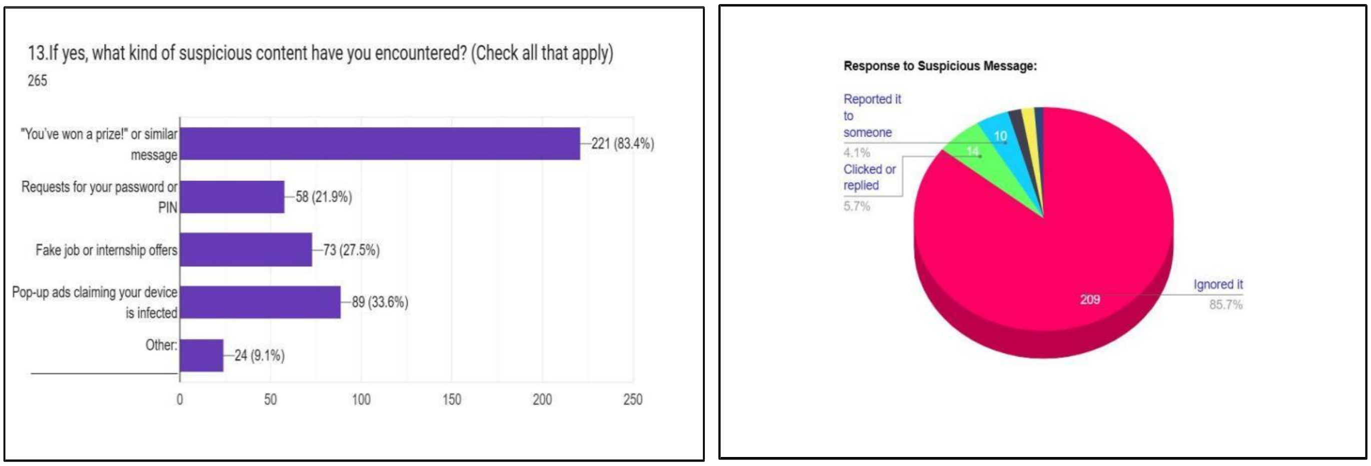
A substantial majority (90.36%) of respondents reported regular use of the internet, while 97.59% were actively engaged with social media platforms. This high level of digital engagement suggests a heightened risk of exposure to cyber threats, especially through phishing, baiting, and impersonation tactics common on social platforms. Daily time spent the portion of respondents are highly active online, with **"1-3 hours" (41.6% or 104 respondents)** and **"4- 6 hours" (28.8% or 72respondents)** being the most common time categories. A moderate number of respondents fall into the **"Morethan 6 hours" category (23.2% or 58 respondents)**, while only a small minority spend **"Less than 1 hour" online (6.4% or 16 respondents)**. This suggests that the majority of the surveyed population spends a significant portion of their day engaged in online activities. Jobbs[6] noted that educational institutions must align cybersecurity instruction with students' online behaviors, ensuring that protective measures are relevant and applicable in real-life digital environments.

Figure 6. Awareness and Understanding of Social Engineering



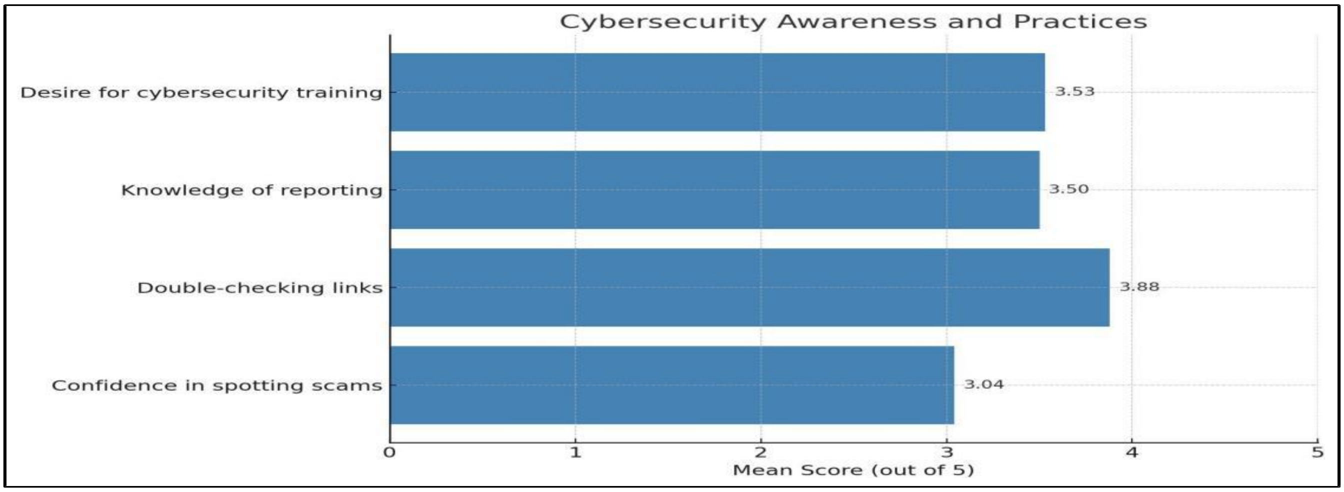
Only 63.6% of students indicated they had heard of the term "social engineering," and just 4.6% considered themselves "very familiar" with it. This stark contrast between usage of digital tools and awareness of associated risks reveals a critical knowledge gap. Rathod et al. [7] emphasized that awareness is the first line of defense against social engineering attacks. Furthermore, Salahdine and Kaabouch [8] argue that awareness without actionable understanding does little to reduce actual vulnerability, pointing to the necessity of hands-on training modules that move beyond basic definitions.

Figure 7. Experience with Suspicious Content



Approximately 83.4% of students acknowledged receiving suspicious messages, the majority of which were identified as phishing attempts. Alarmingly, 85.7% of those who received such content admitted to ignoring it rather than reporting or analyzing it. This passive response validates Hadnagy's assertion that awareness alone does not ensure defensive action [9]. Students may recognize threats but feel ill-equipped to respond, which calls for scenario-based learning methods that simulate real-world cyber incidents.

Figure 8. Confidence and Behavior in Cyber security Practices



The study measured students' self-reported confidence in their cybersecurity behavior using Likert-scale items. The mean score for identifying scam messages was 3.04 (out of 5), indicating moderate confidence. The highest score was in link verification behavior (mean = 3.88), showing that students tend to be cautious with unknown URLs. However, confidence in reporting threats scored only 3.50, suggesting that students are unsure of proper channels or procedures for response. Nwankpa et al. [10] argue that effective cybersecurity education must teach not only how to identify threats, but also how to react appropriately, including reporting and escalating incidents.

Summary of Key Findings

In conclusion, students from diverse backgrounds demonstrate considerable exposure to the digital world, but little preparation for social engineering threats. As the analysis revealed, no significant relationships were found between the demographic variables and cybersecurity confidence or awareness, reaffirming that vulnerability pervades all human groups. 91% reported that they would be very interested in getting cybersecurity education. Overall, these results demonstrate a timely and urgent need for accessible, context-scenarios based cybersecurity training in higher education. If embedded in general courses and if delivered in peer-based format, higher education institutions can enhance digital resilience in these students before they are confronted by real cyber threats.

Perceptions of Preparedness and Importance

While 34.94% admitted to being tricked by scams, 36.55% were unsure—a concerning insight into respondents' awareness of their own vulnerability. Encouragingly, 86.35% believed their school is prepared to handle social engineering threats, and 91.16% emphasized the importance of cybersecurity awareness.

Common Threats and Information Sources

Phishing was the most commonly identified form of social engineering (49.87%), followed by fake tech support calls (28.32%). Common suspicious content included "You've won a prize!" messages (47.52%) and infection- alert pop-ups (19.14%). Social media was the most cited source of cybersecurity information (50.47%), suggesting an informal learning channel with mixed reliability.

Statistical Analysis

Chi-square tests revealed no significant relationships between gender or year level and awareness of social engineering ($p > 0.05$). Similarly, **independent t-tests** showed no significant differences in confidence between male and female respondents ($p = 0.643$), nor between those who had or had not heard of social engineering ($p = 0.931$). These findings indicate that factors such as gender and basic awareness alone may not influence cybersecurity confidence, emphasizing the need for more targeted education strategies.

Implications and Interpretation

The results underline a high baseline exposure to online threats but only moderate awareness and preparedness among students. While most respondents are cautious and aware of the need for cybersecurity training, actual understanding and proactive behaviors remain limited. Educational institutions are thus encouraged to integrate practical, scenario-based cybersecurity programs tailored to students' digital habits and threat perceptions.

CONCLUSION

This study highlights the assessment of understanding and behavioral responses of students concerning social engineering attacks. There is a moderate level of confidence and awareness regarding the identification of threats to cybersecurity, despite the high usage of the internet and social media platforms by the respondents. The majority of students have come across content that they consider suspicious, but a large number of them do not know how to respond to it effectively. Gender, year level, and general awareness have little to no bearing on a student's confidence in employing cybersecurity measures which suggest that contemporary social behaviors are complex and that educational frameworks need to be more refined.

The findings suggest that even if students appreciate the necessity of cybersecurity, there is a major gap when it comes to technology and the implementation of that knowledge. The study highlights the need for engaging, practical, and relevant education about cybersecurity that can be integrated with the online interactions of the students.

RECOMMENDATION

Academic institutions are required to add cybersecurity as an awareness subject in every offered course, targeting it specifically toward non-it programs which may have very little exposure to it. Customized hands-on workshops or training needs to be organized by educational institutions to educate students on effective response measures to social engineering techniques. Since students primarily engage with social media as their main source of information about cybersecurity, institutions need to set up verified social media accounts and platforms to disseminate straightforward, practical, and relevant cybersecurity information. Recruit peer educators from among the students who are easier to relate to, and let them teach using appropriate language and practical illustrations for better comprehension and retention. Ensure that every student is aware of the available cybersecurity policies and the reporting structures in place in order to foster increased responsibility and preparedness.

REFERENCES

[1] Hadnagy, C., & Fincher, M. (2018). *Social engineering: The science of human hacking* (2nd ed.). Wiley.

[2] Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, 8(1), 5.

[3] Abdulla, R. M., Alsewari, A. A., Zain, J. M., & Shakir, M. Z. (2023). Analysis of social engineering awareness among students and lecturers. *IEEE Access*, *11*, 1–12. https://ieeexplore.ieee.org/document/10081241

[4] Albladi, S. M., & Weir, G. R. S. (2018). User characteristics that influence judgment of social engineering attacks in social networks. *Human-centric Computing and Information Sciences*, *8*(1), 5. https://doi.org/10.1186/s13673-018-0130-7

[5] Alsulami, M. H., Alsubaie, A. R., & Alzahrani, H. A. (2021). Measuring awareness of social engineering in the educational sector in the Kingdom of Saudi Arabia. *Information*, *12*(5), 208. https://www.mdpi.com/2078-2489/12/5/208

[6] Hobbs, J. (2023). Cybersecurity awareness in higher education. In *Proceedings of IACIS 2023*. https://iacis.org/iis/2023/1_iis_2023_159-169.pdf

[7] Rathod, T., Meshram, B. B., & Shaikh, R. (2025). A comprehensive survey on social engineering attacks, countermeasures, case study, and research challenges. *Information Processing & Management*, *62*, 103928. https://doi.org/10.1016/j.ipm.2024.103928

[8] Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4), 89. https://www.mdpi.com/1999-5903/11/4/89

[9] Hadnagy, C., & Fincher, M. (2018). *Social engineering: The science of human hacking* (2nd ed.). *Wiley*.

[10] Nwankpa, J. K., Ehie, I. C., & Forbes, J. (2023). A social engineering research partnership in higher education to improve SETA programs. In *AMCIS 2023 Proceedings*. https://aisel.aisnet.org/amcis2023/sig_sec/sig_sec/18/

Appendix A

Survey Questionnaire: Student Perceptions of Social Engineering Attacks

Instructions:
This questionnaire is part of an academic research study on students' awareness and perception of social engineering attacks. Your participation is voluntary, and your answers will be kept strictly confidential. Please read the instructions carefully and answer all applicable questions honestly.

Section I – Demographic Profile

1. Age: _________
2. Gender:
   [ ] Male [ ] Female [ ] Prefer not to say
3. Academic Program: ____________________________________
4. Year Level:
   [ ] 1st [ ] 2nd [ ] 3rd [ ] 4th [ ] Other: _________
5. Do you regularly use the internet? [ ] Yes [ ] No
6. On average, how many hours do you spend online per day?
   [ ] Less than 1 hour [ ] 1–3 hours [ ] 4–6 hours [ ] More than 6 hours
7. Do you frequently use social media platforms (e.g., Facebook, TikTok, Messenger)? [ ] Yes [ ] No

Section II – Awareness of Social Engineering

Note: *Social engineering* refers to techniques used by cybercriminals to trick people into revealing sensitive information or performing actions that compromise security. Common forms include phishing emails, fake support calls, suspicious links, and impersonation.

8. Before this survey, had you ever heard of the term *social engineering*? [ ] Yes [ ] No
9. Which of the following do you think are examples of social engineering? *(Check all that apply)*
   [ ] Phishing emails or messages
   [ ] Free flash drives with unknown origin
   [ ] Calls pretending to be tech support
   [ ] Tailgating (following someone into a secured area without permission)
   [ ] None of the above
10. From where did you first learn about cyber threats or online scams? *(Select one)*
    [ ] School [ ] Social Media [ ] News [ ] Friends [ ] I have no prior knowledge
11. How would you rate your current understanding of social engineering?
    [ ] Very familiar [ ] Somewhat familiar [ ] Slightly familiar [ ] Not familiar at all

Section III – Personal Experience

12. Have you ever received a suspicious message, email, or offer online?
    [ ] Yes [ ] No [ ] Not sure
13. If yes, what kind of suspicious content have you encountered? *(Check all that apply)*
    [ ] "You've won a prize!" or similar message
    [ ] Requests for your password or PIN
    [ ] Fake job or internship offers
    [ ] Pop-up ads claiming your device is infected
    [ ] Other: ______________________________
14. How did you respond to the suspicious message?
    [ ] Ignored it
    [ ] Clicked or replied
    [ ] Reported it to someone

[ ] Searched online for help
[ ] Not applicable

Section IV – Behavior and Confidence

Indicate how much you agree with the following statements:
(1 – Strongly Disagree, 2 – Disagree, 3 – Neutral, 4 – Agree, 5 – Strongly Agree)

No.	Statement	1	2	3	4	5
15	I feel confident in spotting phishing or scam messages.	□	□	□	□	□
16	I double-check links or emails before clicking or replying.	□	□	□	□	□
17	I know how to report suspicious online activities.	□	□	□	□	□
18	I believe students are commonly targeted by social engineering attacks.	□	□	□	□	□
19	I would like to attend seminars or training on cybersecurity awareness.	□	□	□	□	□

Section V – Perception and Preparedness

20. Do you think you could be tricked by a well-crafted scam online?

    [ ] Yes [ ] No [ ] Not sure
21. Do you believe your course or school has prepared you to avoid online threats like social engineering?
    [ ] Yes [ ] No [ ] Not sure
22. In your opinion, how important is cybersecurity awareness for students?
    [ ] Very important [ ] Important [ ] Neutral [ ] Not important

Thank you for participating in this survey!