ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Level of Awareness and Susceptibility to Phishing Attacks Among Students of Quezon City University: A Stratified Survey Study

Iverson John S. Ventura, Harold R. Lucero, Lance Luis P. Ballesteros, Justin T. Reyes, Roland Allan Gabriele L. Villareal[4], Ramer Lazan

College of Computer Studies, Quezon City University

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150500131

Received: 13 May 2026; Accepted: 18 May 2026; Published: 08 June 2026

ABSTRACT

Phishing attacks continue to pose serious cybersecurity risks in educational institutions as students increasingly rely on digital platforms for academic and personal activities. This study aimed to determine the level of phishing awareness and phishing susceptibility among students of Quezon City University, particularly comparing IT and non-IT students. Using a descriptive-comparative quantitative research design, data were collected from 397 students through a stratified survey conducted using online and printed questionnaires. Statistical tools such as frequency and percentage, weighted mean, independent samples t-test, and Pearson Product-Moment Correlation Coefficient were used to analyze the data. The findings revealed that students generally demonstrated a high level of phishing awareness but showed a moderate level of phishing susceptibility. Results also indicated a significant difference in phishing awareness between IT and non-IT students, with IT students exhibiting higher awareness levels. However, no significant difference was found in phishing susceptibility between the two groups. Furthermore, a significant moderate negative relationship was identified between phishing awareness and phishing susceptibility, indicating that higher awareness is associated with lower vulnerability to phishing attacks. The study concludes that although students possess adequate knowledge regarding phishing threats, awareness alone does not completely prevent risky online behavior. The findings may contribute to the development of targeted cybersecurity awareness programs and safer digital practices among university students.

Keywords: Cybersecurity Awareness, Phishing Attacks, Phishing Susceptibility, Stratified Survey, University Students, Quantitative Research

INTRODUCTION

In the digital age, phishing attempts are among the most common and serious forms of cybercrime. These attacks involve fraudulent communication designed to deceive individuals into revealing sensitive information such as passwords, banking details, and personal data. According to Bhavsar et al. (2018) , phishing is a form of social engineering that exploits human behavior rather than technical vulnerabilities. As digital communication continues to expand, phishing incidents have also increased in both frequency and sophistication, with attackers employing more deceptive and targeted strategies (Mouncey & Ciobotaru, 2025). Abufardeh & Falah (2023) further emphasize that phishing remains one of the most persistent global cybersecurity threats due to its simplicity and widespread impact.

Phishing attacks continue to evolve, becoming more personalized and harder to detect (Alkhalil et al., 2021). These threats expose individuals and organizations to risks such as data breaches, financial losses, and unauthorized access to personal accounts (Kuraku et al., 2023). Despite ongoing awareness efforts, many users still lack sufficient cybersecurity knowledge and practical skills to effectively identify phishing attempts (Tanti, 2024). Students are particularly vulnerable due to their frequent use of digital platforms for academic and personal activities, as well as varying levels of cybersecurity awareness.

In the Philippine higher education context, cybersecurity education is often not formally integrated into academic curricula and is typically limited to orientation or informal learning. As a result, students rely heavily on personal judgment when evaluating suspicious online messages. Previous studies show that this contributes to continued

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

vulnerability among students, as limited awareness and weak verification practices increase exposure to phishing attacks (Alqahtani et al., 2025; Okokpujie et al., 2025).However, existing studies are mostly foreign based, limiting their applicability to Philippine public universities (De Ramos & Esponilla II, 2022).

Previous studies suggest that phishing attacks are effective because they rely heavily on social engineering techniques that exploit trust, urgency, and authority rather than technical weaknesses (Desolda et al., 2022; Lin et al., 2019).Research also indicates that awareness does not always translate into safe behavior, as responses are influenced by situational, cognitive, and behavioral factors such as decision-making style, attention, time pressure, and message characteristics (Auton & Sturman, 2025; Diaz et al., 2020; Nasser et al., 2020). This awareness–behavior gap highlights the importance of examining both phishing awareness and susceptibility in understanding cybersecurity behavior among students (Broadhurst et al., 2019; Sturman et al., 2024).

Despite existing literature, there remains limited localized and institution-specific evidence on phishing awareness and susceptibility among students at Quezon City University. While studies confirm general student vulnerability, there is insufficient understanding of how aware students are of phishing indicators, how susceptible they are to phishing attempts, and whether differences exist between IT and non-IT students within the same institution.

Therefore, this study aims to assess phishing awareness and susceptibility among students of Quezon City University using a stratified survey design. Specifically, it seeks to examine differences between IT and non-IT students and determine the relationship between phishing awareness and susceptibility. The findings are expected to provide empirical evidence that may support the development of targeted and context-appropriate cybersecurity awareness programs.

Statement of the Problem

This study aims to determine the level of phishing awareness and susceptibility among students at Quezon City University, with particular emphasis on comparing IT students and non-IT students. Specifically, this study seeks to answer the following questions:

1. What is the profile of the Quezon City University students in terms of:

   1.2 Age;

   1.3 Sex; and

   1.4 Academic program (IT and non-IT)?

2. What is the level of phishing awareness among Quezon City University students?
3. What is the level of phishing susceptibility among Quezon City University students?
4. Is there a significant difference in the level of phishing awareness between IT students and non-IT students at Quezon City University?
5. Is there a significant difference in the level of phishing susceptibility between IT students and non-IT students at Quezon City University?

Related Studies

Phishing awareness refers to an individual's knowledge and ability to recognize phishing threats and apply appropriate preventive measures against cyberattacks. It involves understanding common phishing tactics and identifying warning indicators such as spoofed sender identities, suspicious or shortened URLs, urgent or threatening language, unexpected attachments, and requests for sensitive or confidential information (Kuraku et al., 2023; Sahidjuan et al., 2024). In contrast, phishing susceptibility refers to the likelihood that an individual will engage with phishing attempts by clicking malicious links, responding to fraudulent messages, or disclosing personal credentials and sensitive information (Diaz et al., 2020; Okokpujie et al., 2025). Existing literature emphasizes that awareness and susceptibility are distinct yet related constructs, as possessing general knowledge about phishing threats does not always guarantee safe online behavior. This relationship highlights the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

awareness–behavior gap, wherein individuals may recognize phishing indicators but still fail to apply protective actions consistently in real-world situations. Consequently, phishing awareness and phishing susceptibility are treated as separate but interconnected variables in the present study to determine how awareness influences susceptibility among students of Quezon City University.

The study is anchored on Social Engineering Theory and Protection Motivation Theory, which explain how psychological manipulation and behavioral responses influence phishing vulnerability. Social Engineering Theory explains that phishing attacks rely on manipulation techniques such as authority, urgency, trust, and deception to influence users' decisions and encourage risky behavior (Alqahtani et al., 2025; Sahidjuan et al., 2024). This perspective supports the assessment of phishing awareness through students' ability to identify suspicious sender identities, deceptive URLs, urgent language, and requests for confidential information. Complementing this framework, Protection Motivation Theory posits that awareness alone may not be sufficient to motivate protective behavior because responses to cyber threats are influenced by perceived severity, vulnerability, self-efficacy, and confidence in one's ability to respond effectively (Adeshola & Oluwajana, 2025; Han et al., 2025; William Vortia, 2025). Together, these theories explain why students may remain vulnerable to phishing attacks despite having knowledge of phishing indicators, thereby providing the theoretical foundation for examining the relationship between phishing awareness and susceptibility.

Several studies indicate that university students generally possess moderate awareness of phishing threats but often lack practical detection skills necessary to identify sophisticated phishing attempts. Research consistently shows that students struggle to recognize deceptive elements such as spoofed sender addresses, suspicious URLs, misleading content, and manipulative language embedded in phishing messages (Okokpujie et al., 2025; Ruzaili et al., 2026). Awareness levels are influenced by prior cybersecurity education, exposure to awareness campaigns, and formal training, with students who receive structured cybersecurity instruction demonstrating better understanding of phishing risks and indicators (Adeshola & Oluwajana, 2025; Al Zaidy, 2025). However, Kuraku et al. (2023) emphasized that many students fail to consistently apply verification techniques such as validating URLs and confirming sender legitimacy before responding to messages. Similarly, Ismail et al. (2023) found that even students enrolled in information technology-related programs experienced difficulty identifying advanced phishing attempts despite their familiarity with phishing concepts. Researchers further note that phishing detection depends not only on awareness but also on cognitive and situational factors such as attention, mental workload, distraction, and time pressure, which significantly affect users' detection performance during urgent or stressful situations (Nasser et al., 2020; Sturman et al., 2024). Experimental tools such as the Phishing Email Suspicion Test further demonstrate that phishing detection abilities vary among users, highlighting the importance of assessing practical awareness rather than relying solely on self-reported knowledge (Hakim et al., 2021).

Phishing susceptibility among university students remains a major cybersecurity concern due to students' extensive use of email, social media, and online academic platforms (Diaz et al., 2020; Lin et al., 2019). High levels of digital interaction increase students' exposure to phishing attempts and may lead to impulsive or careless online decisions. Studies reveal that even students who exhibit awareness of phishing threats remain vulnerable when phishing messages appear urgent, authoritative, or personally relevant (Casagrande et al., 2023; Lin et al., 2019). This reinforces the awareness–behavior gap, wherein knowledge about phishing threats does not necessarily translate into safe cybersecurity practices. Additionally, susceptibility is influenced by several situational, psychological, and demographic factors. Research indicates that academic background, age, year level, and prior cybersecurity training affect students' responses to phishing attempts (Lee et al., 2023; Okokpujie et al., 2025). Decision-making styles also play a significant role, as heuristic and impulsive processing increase vulnerability while analytical evaluation reduces susceptibility (Gan et al., 2024; Gwenhure, 2025). In line with Protection Motivation Theory, perceived threat severity, perceived vulnerability, and confidence in one's ability to respond effectively also shape users' protective behaviors against phishing attacks (Adeshola & Oluwajana, 2025; Han et al., 2025).

The literature likewise highlights the importance of cybersecurity education and intervention programs in reducing phishing susceptibility. Experimental studies demonstrate that structured cybersecurity training programs, phishing simulations, and gamified learning strategies improve students' phishing detection abilities and encourage safer online behavior (Azzeh et al., 2022; Jampen et al., 2020; Le-Nye et al., 2024; Yin et al.,

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

2025). However, researchers caution that the effectiveness of training interventions may decline over time without continuous reinforcement and contextualized awareness initiatives (Mouncey & Ciobotaru, 2025; Vivien A. Agustin et al., 2024). These findings suggest that phishing susceptibility results from the interaction of awareness, behavioral tendencies, cognitive processes, and contextual influences rather than awareness alone.

Within the Philippine context, cybersecurity research in higher education has largely focused on institutional preparedness, policy implementation, and general awareness rather than student-level phishing behavior. Studies in Philippine public institutions identified challenges such as limited cybersecurity resources, lack of cybersecurity courses, and dependence on basic awareness campaigns as primary defense mechanisms (De Ramos & Esponilla II, 2022). National surveys further indicate that Filipinos demonstrate varying levels of cybersecurity awareness, with substantial gaps in practical cybersecurity knowledge and safe online practices (Omorog & Medina, 2020). Although recent local studies have begun examining college students' cybersecurity awareness, these investigations commonly focus on general awareness and fail to comprehensively assess phishing-specific awareness and susceptibility within a single institutional setting (Romel et al., 2025).

Overall, the reviewed literature establishes that phishing remains a persistent cybersecurity threat in university environments due to students' heavy exposure to digital communication platforms. While students generally demonstrate moderate awareness of phishing indicators, many continue to struggle with recognizing deceptive cues and consistently applying safe online practices in real-world situations (Kuraku et al., 2023; Okokpujie et al., 2025; Ruzaili et al., 2026). A recurring theme across studies is the awareness–behavior gap, wherein students who possess knowledge about phishing threats remain susceptible when confronted with urgent, authoritative, or personally relevant phishing messages (Aljeaid et al., 2020; Casagrande et al., 2023; Lin et al., 2019). Cognitive and psychological factors such as self-efficacy, heuristic decision-making, and perceived risk further influence students' responses to phishing attacks (Gwenhure, 2025; Nasser et al., 2020). Although training and simulation-based interventions have proven effective in improving phishing detection and reducing susceptibility, their long-term effectiveness requires continuous reinforcement (Desolda et al., 2022; Jampen et al., 2020; Mouncey & Ciobotaru, 2025). Despite the growing body of international research, limited studies have examined phishing awareness and susceptibility within a localized Philippine public university context, particularly using a stratified approach that considers differences among academic groups. This gap provides the basis for the present study, which seeks to investigate the relationship between phishing awareness and susceptibility among students of Quezon City University.

DESIGN AND METHODOLOGY

Research Design

This study utilizes a descriptive-comparative quantitative research design. It is descriptive because it seeks to systematically describe the current levels of phishing awareness and susceptibility among the respondents using numerical data. Quantitative research designs focus on the collection and analysis of numerical data through systematic and objective procedures. (Slater & Hasson, 2025). It is also comparative because it aims to determine whether there are similarities or differences between two distinct groups: IT and non-IT students. According to Siedlecki (2020), descriptive studies may be purely descriptive or descriptive-comparative, and they may be used to describe variables, population characteristics, or differences among naturally occurring groups without manipulating variables. This design is highly appropriate for the study as it allows the researchers to objectively assess and statistically analyze students' level of phishing awareness and susceptibility based on their responses and experiences regarding phishing attacks.

Data Gathering

Data for this study were collected from currently enrolled students of Quezon City University. The researchers used both online and face-to-face survey distribution to increase respondent participation and accessibility. The online survey was administered through Google Forms, while printed questionnaires were distributed personally within the university premises.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

This mixed mode of distribution allowed the researchers to reach students from different academic programs and year levels. The survey was conducted to assess students' awareness of and susceptibility to phishing, with emphasis on comparing students enrolled in IT-related programs and non-IT programs.

Population and Sampling Procedure

The population of this study comprises the total student population of Quezon City University, which is 11,459 students across various academic departments. The choice of this large population provides a diverse pool of respondents both from IT and non-IT backgrounds**.**

To determine the minimum required number of respondents, the researchers used Slovin's formula with a margin of error of 0.05. Based on the total population of 11,459 students, the computed minimum sample size was approximately 387 respondents. However, to increase the credibility of the results and account for possible data cleaning or invalid responses, the researchers collected a total of 397 valid responses.

The study employed stratified convenience sampling. Respondents were first classified into two groups: IT students and non-IT students. After this classification, participants were selected based on their availability and willingness to participate in the study. This approach allowed the researchers to compare phishing awareness and susceptibility between students with technical and non-technical academic backgrounds.

Table 1. Population Distribution of the Respondents According to IT Programs

IT Programs	Population Size
Bachelor of Science in Computer Engineering (BSCE)	26
Bachelor of Science in Information and Technology (BSIT)	139
Bachelor of Science in Computer Science (BSCS)	24
Bachelor of Science in Information Systems (BSIS)	27
Total	216

Among the respondents, IT field accounts the majority with a total of 216 total respondents, within this group Bachelor of Science in Information Technology (BSIT) provided the largest number of participations with a total number of 139.

Table 2: Population Distribution of the Respondents According to non-IT Programs

non-IT Programs	Population Size
Bachelor of Science in Accountancy (BSA)	28
Bachelor of Science in Entrepreneurship (BS Entrep)	12
Bachelor of Science in Electronics Engineering (BSECE)	42
Bachelor of Early Childhood Education (BECED)	37
Bachelor of Science in Industrial Engineering (BSIE)	52
Bachelor of Science in Management Accounting (BSMA)	10
Total	181

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

The non-IT programs consist of 181 students across 6 different departments, the Bachelor of Science in Industrial Engineering (BSIE) represents the largest group within this classification with 52 respondents. By maintaining a near equal balance with the IT and non-IT classifications, the researchers can effectively compare the points of differentiation regarding phishing awareness and susceptibility between two different clusters.

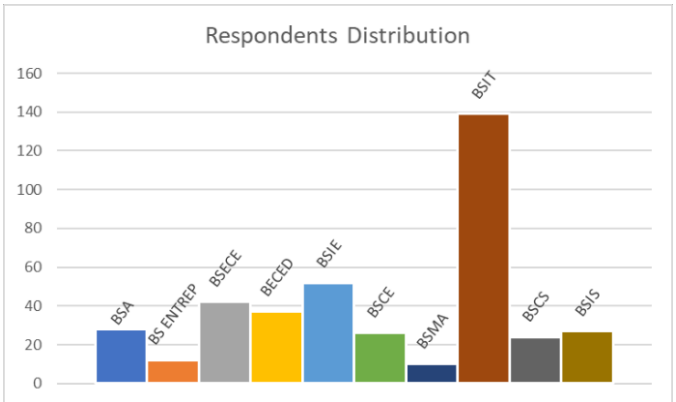

Figure 1. Distribution of Respondents

Figure 1 shows the distribution of respondents by academic program. BS Information Technology (BSIT) recorded the highest number of respondents with 139 participants, followed by BS Industrial Engineering (BSIE) with 52 and BS Electronics Engineering (BSECE) with 42. The remaining respondents came from other programs, indicating that the sample included both technical and non-technical students.

Table 3: Proportionate Sampling of Respondents by Academic Program

Academic Classification	Population	Sample
IT	216	109
Non-IT	181	91
Total	397	200

Table 3 illustrates the proportionate sampling process used to select respondents for the study. From the identified group of 397 students, consisting of 216 IT students (54.4%) and 181 non-IT students (45.6%), the researchers applied a ratio-based approach to derive a target sample of 200 respondents.

Data Gathering Tools

The primary data gathering tool used in this study was a researcher-made structured questionnaire administered through Google Forms and printed survey forms. The questionnaire consisted of three main parts: the respondents' demographic profile, phishing awareness items, and phishing susceptibility items. The demographic profile included age, sex, and academic program.

The phishing awareness and phishing susceptibility sections used 5-point Likert scales to measure the respondents' level of awareness and likelihood of engaging in phishing-related risky online behaviors. The awareness items assessed the respondents' knowledge and ability to identify phishing indicators, while the susceptibility items measured their tendency to respond to potentially fraudulent online messages or links.

The survey was distributed through both online and face-to-face methods. The online survey link was shared through student communication channels, such as class group chats, academic organization pages, and other accessible online platforms. Printed copies of the questionnaire were also personally distributed within the university to increase the number of responses and ensure wider participation. Both formats included a brief introduction explaining the purpose of the study and instructions for answering the questionnaire.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Statistical Treatment of Data.

The data gathered in this study were analysed using appropriate statistical tools based on the specific problems stated in the Statement of the Problem. Frequency and percentage were used to describe the profile of the respondents in terms of age, sex, and academic program. The level of phishing awareness and phishing susceptibility among Quezon City University students was measured using a researcher-made questionnaire. The responses were rated using a 5-point Likert scale and were treated using weighted mean and standard deviation. The weighted mean was used to determine the average level of responses, while the standard deviation was used to measure the variability of responses among participants. Both phishing awareness and phishing susceptibility instruments included positively and negatively worded items, and all negative worded items were reverse-coded to ensure consistency in scoring to ensure that the higher mean scores consistently represent higher levels of awareness or susceptibility.

Table 4. Interpretation scale of Weighted Mean

Statistical Tool/Scale	Interpretation
2.41 - 5.00	Very High
3.41 - 4.20	High
2.61 - 3.40	Moderate
1.81 - 2.60	Low
1.00 - 1.80	Very Low

Table 5. Interpretation scale of Significance Level (p-value)

p-value range	Interpretation
$p \leq 0.01$	Highly Significant Difference
$0.01 < p \leq 0.05$	Significant Difference
$0.05 < p \leq 0.10$	Marginal/Weak Significance
$p > 0.10$	Not Significant

Table 6. Interpretation scale of Magnitude of Difference (t-value)

t-value Range	Interpretation
0.00 – 0.99	Very Small or No Meaningful Difference
1.00 – 1.99	Small Difference
2.00 – 2.99	Moderate Difference
≥ 3.00	Large or Strong Difference

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

RESULT AND DISCUSSION

A. Profile of the Respondents

The data presented in tables with corresponding interpretations to clearly explain the findings. Statistical tools such as frequency and percentage, weighted mean, standard deviation, Independent Samples t-test, and Pearson Product-Moment Correlation Coefficient were used to analyze and interpret the data.

Table 7. Age of Respondents

Ages of the Respondents	Frequency	Percentage
18 – 20 Years Old	219	55.16%
21 – 23 Years Old	168	42.31%
24 Years Old and above	9	2.26%
Total	397	100%

In accordance with table 7, The age distribution of the respondents shows that the majority are within the 18-20 age group (55.16%), followed by those aged 21-23 (42.31%). Only a minimal percentage belongs to the 24 and above category (2.26%), indicating that most respondents are in typical early college age.

Table 8. Gender of Respondents

Gender of the Respondents	Frequency	Percentage
Female	210	52.89%
Male	173	43.57%
Prefer not to say	14	3.52%
Total	397	100%

In accordance with table 8 the gender distribution of the respondents shows that the females constitute the majority of 52.89%.

This was followed by male respondents at 43.57%, while a small portion of the respondents preferred not to disclose their gender at 3.52%. This indicates that the study is slightly dominated by female respondents.

Table 9. Academic Program Classification of the Respondents

Academic Program	Frequency	Percentage
IT	216	54.41%
non-IT	181	45.59%
Total	397	100%

The distribution of respondents according to academic program is presented in Table 9. The results indicate that most respondents are enrolled in IT academic programs, with a frequency of 216, representing 54.41% of the total sample.

On the other hand, 181 respondents are enrolled in non-IT academic programs, accounting for 45.59% of the population. These findings suggest that most of the study participants belong to IT academic programs.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

B. Phishing Awareness among Quezon City University Students

Table 10. The result of findings in accordance to level of Phishing Attack Awareness

Phishing Attack Awareness	Mean (SD)
Q1. I am familiar with the concept of phishing attacks	4.05(1.07)
Q2. I can identify suspicious links or URLs	3.91(1.01)
Q3. I can recognize phishing emails or messages.	4.01(0.98)
Q4. I understand the risks associated with phishing attacks	4.28(1.01)
Q5. I know what actions to take when I encounter a suspected phishing attempt	3.79(1.11)
Q6. I am aware that phishing can occur through multiple platforms (email, SMS, social media).	4.36(0.99)
Q7. I have received training or education about phishing or cybersecurity.	4.35(1.24)
Q8. I am not familiar with the concept of phishing attacks.	3.66(1.41)
Q9. I do not recognize phishing emails or messages.	3.78(1.34)
Overall	3.91

The table 10 findings suggest that Quezon City University students generally have a high level of phishing attack awareness, as reflected in the overall mean of 3.91. This indicates that students are familiar with phishing concepts and understand its risks, which may be attributed to increased exposure to digital platforms and cybersecurity information. The highest-rated indicators show that students are particularly aware that phishing can happen across multiple platforms and that they have received some form of cybersecurity education. This implies that awareness campaigns or informal exposure through social media and academic discussions may be effective in increasing knowledge about phishing threats.

However, the relatively lower scores in identifying suspicious links and knowing appropriate actions suggest that while students are aware of phishing in theory, their practical response skills may still be limited. This gap is important because awareness alone does not fully protect users without proper behavioral response training. Therefore, universities may further strengthen students' cybersecurity preparedness by conducting practical seminars, phishing simulations, and hands-on cybersecurity activities that focus on real life phishing scenarios.

C. Phishing Susceptibility among Quezon City University Students

Table 11. The result of findings in accordance with level of Susceptibility of Phishing Attacks

Susceptibility of Phishing Attacks	Mean(SD)
Q1. I tend to click links from unknown or unverified sources.	1.97(1.15)
Q2. I open email attachments without verifying the sender.	1.94(1.10)
Q3. I trust messages that appear to come from official sources without verifying their authenticity.	2.32(1.22)
Q4. I reuse the same password across multiple accounts.	3.21(1.37)
Q5. I respond quickly to urgent messages without verifying them.	2.27(1.10)
Q6. I carefully check the legitimacy of links before clicking them.	3.88(1.23)
Q7. I verify the sender before opening email attachments.	3.95(1.16)
Q8. I am not familiar with the concept of phishing attacks.	4.03(1.16)
Overall	2.95

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

The result shows that Quezon City University students have a moderate level of susceptibility to phishing attacks, with an overall mean of 2.95. Low mean scores in clicking the links from unknown sources (M = 1.97) and opening email attachments without verifying the sender (M = 1.94) indicate that most respondents practice cautions when encountering suspicious online content. Similarly, lower scores in trusting unverified messages and responding immediately to urgent requests suggest that students are generally aware of common phishing tactics and potential online threats. This finding implies that many students are careful when dealing with suspicious emails, links, and online messages.

However, the relatively higher mean score in reusing the same password across multiple account indicates that some students still engage in risky cybersecurity despite being aware of phishing attacks. This may occur because password reuse is often viewed as more convenient and easier to remember. In contrast, high scores in checking links, verifying senders, and double checking the website URLs suggest that students apply preventive measures before sharing personal information online. The findings suggest that while students demonstrate cautious online behavior in several aspects, some cybersecurity habits still make them vulnerable to phishing attack and other online risks

Table 12. Difference in the Level of Phishing Awareness and Phishing Susceptibility Between IT and Non-IT Students.

Variables	IT Mean (SD)	Non-IT Mean (SD)	t	P
Phishing Awareness	3.76(1.19)	3.50(1.07)	2.07	0.035
Phishing Susceptibility	3.03(1.25)	2.91(1.16)	0.89	0.370

Table 12 presents the difference in the level of phishing awareness and phishing susceptibility between IT and Non-IT students using an independent samples t-test. The results show that IT students obtained a higher mean score in phishing awareness (M = 3.76, SD = 1.19) compared to Non-IT students (M = 3.50, SD = 1.07). The computed t-value of 2.07 with a p-value of 0.035 indicates that the difference is statistically significant at the 0.05 level. This suggests that students enrolled in IT-related programs possess significantly greater awareness of phishing threats, phishing indicators, and preventive practices than Non-IT students. The finding may be attributed to IT students' greater exposure to cybersecurity concepts, digital systems, and technical training within their academic programs.

In terms of phishing susceptibility, IT students also recorded a slightly higher mean score (M = 3.03, SD = 1.25) than Non-IT students (M = 2.91, SD = 1.16). However, the computed t-value of 0.89 and p-value of 0.370 indicate that the difference is not statistically significant. This means that despite IT students demonstrating higher phishing awareness, their level of susceptibility to phishing attacks does not significantly differ from that of Non-IT students. The result supports existing literature suggesting that awareness alone may not fully protect individuals from phishing attacks, as susceptibility is also influenced by behavioral, psychological, and situational factors such as urgency, decision-making style, attention, and perceived trustworthiness of messages.

D. Difference in the Level of Phishing Awareness and Phishing Susceptibility Between IT and Non-IT Students

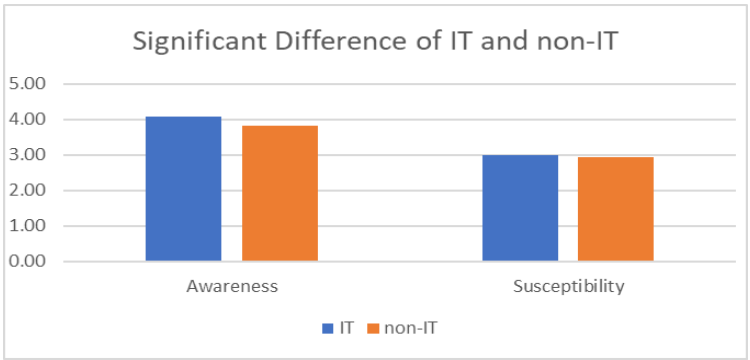

Figure 2. Significant Difference of IT and non-IT Students

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

The results presented in Figure 2 reveal a significant difference in the level of phishing awareness between IT and non-IT students, as indicated by the p-value of 0.0008, which is lower than the 0.05 level of significance. IT students obtained a higher mean awareness score (M = 4.09, SD = 1.17) compared to non-IT students (M = 3.82, SD = 1.07), suggesting that students enrolled in technology-related programs possess greater knowledge and understanding of phishing attacks. This may be attributed to their exposure to computer-related subjects, cybersecurity concepts, and digital technologies within their academic curriculum. Figure 2 further illustrates the noticeable difference in awareness levels between the two groups.

On the other hand, no significant difference was found in phishing susceptibility between IT and non-IT students, as reflected by the p-value of 0.35, which is greater than the 0.05 level of significance. Although IT students showed a slightly higher mean susceptibility score (M = 2.99, SD = 1.26) than non-IT students (M = 2.92, SD = 1.15), the difference was not statistically significant. This suggests that despite differences in awareness levels, both groups demonstrate relatively similar behaviours and vulnerabilities when encountering phishing attempts. The findings imply that awareness alone may not always reduce phishing susceptibility, as actual online behaviour and decision-making may still expose students to cybersecurity risks regardless of academic specialization.

CONCLUSION

This study was conducted to determine the level of phishing awareness and phishing susceptibility among Quezon City University students, particularly between IT and non-IT students. Based on the findings, the researchers found that most students already have knowledge about phishing attacks and are familiar with common signs of online threats. Students are generally careful when using online platforms, although some unsafe online practices are still observed.

The study also found that IT students are more knowledgeable about phishing attacks compared to non-IT students because of their background in technology-related subjects. However, both groups may still become vulnerable to phishing attempts despite differences in awareness. This shows that having knowledge about phishing does not always guarantee safe online behaviour.

In addition, the findings showed that students who are more aware of phishing attacks are less likely to become susceptible to phishing attempts. This highlights the importance of improving cybersecurity awareness and encouraging students to apply safe online practices in their daily digital activities.

Overall, the study helped provide a better understanding of the phishing awareness and susceptibility of Quezon City University students. The findings may be useful in improving cybersecurity awareness programs and promoting responsible online behaviour among students.

ABDEL SAEED I. SAHIDJUAN REFERENCES

1. , Merjina A. Amin, Lina I. Ahaja, Armilyna A. Ahog, Raina T. Ladjahasan, Rima K. Jul, Nerhana J. Radjail, Benczar J. Sayadi, Aljimar J. Sarabi, & Dr. Shernahar K. Tahil. (2024). Understanding the Impact of Phishing Attacks on Organizational Security and Trust. International Journal For Multidisciplinary Research, 6(6). https://doi.org/10.36948/ijfmr.2024.v06i06.34230
2. Abufardeh, S., & Falah, B. (2023). The State of Phishing Attacks and Countermeasures. Sameer Abufardeh & Bouchaib Falah International Journal of Computer Science & Security (IJCSS), (17), 54. https://www.cscjournals.org/manuscript//Journals/IJCSS/Volume17/Issue4/IJCSS-1702.pdf
3. Adeshola, I., & Oluwajana, D. I. (2025). Assessing cybersecurity awareness among university students: implications for educational interventions. Journal of Computers in Education, 12(4), 1283–1305. https://doi.org/10.1007/s40692-024-00346-7
4. Al Zaidy, A. (2025). Measuring Cybersecurity Awareness of Students: a Study of State College Students. Journal of Information Technology, Cybersecurity, and Artificial Intelligence, 2(3), 17–40. https://doi.org/10.70715/jitcai.2025.v2.i3.030
5. Alabab, B., Cubol, J., Pascual, M. A., Ubaldo, E., Sario, D. R., & Velasco, M. (2024). Cybersecurity Awareness of College Students in a Private Higher Education Institution. CGCI International Journal

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

of Administration, Management, Education and Technology, 1(1), 51–57. https://doi.org/10.70059/1zw7x826

6. Aliyu, M., Bagarawa, M. U., Mu'azu, A. N., & Umar, M. T. (2023). Understanding phishing awareness among students in tertiary institutions and setting-up defensive mechanisms against the attackers. Caliphate Journal of Science and Technology, 5(1), 22–31. https://doi.org/10.4314/cajost.v5i1.4
7. Aljeaid, D., Alzhrani, A., Alrougi, M., & Almalki, O. (2020). Assessment of End-User Susceptibility to Cybersecurity Threats in Saudi Arabia by Simulating Phishing Attacks. Information, 11(12), 547. https://doi.org/10.3390/info11120547
8. Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. Frontiers in Computer Science, 3. https://doi.org/10.3389/fcomp.2021.563060
9. Alqahtani, S., Nanda, P., & Mohanty, M. (2025). Strengthening Cybersecurity: The Influence of Student Behavior, Perceived Factors, and Mitigating Strategies on Phishing Attack Perception (pp. 313–329). https://doi.org/10.1007/978-981-96-1483-7_27
10. Auton, J. C., & Sturman, D. (2025). Persuasion under pressure: the influence of persuasion principles and time constraints on phishing email susceptibility. Information & Computer Security, 33(5), 845–859. https://doi.org/10.1108/ICS-07-2024-0163
11. Azzeh, M., Mousa Altamimi, A., Albashayreh, M., & AL-Oudat, M. A. (2022). Adopting the cybersecurity concepts into curriculum: the potential effects on students' cybersecurity knowledge. Indonesian Journal of Electrical Engineering and Computer Science, 25(3), 1749. https://doi.org/10.11591/ijeecs.v25.i3.pp1749-1758
12. Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on Phishing Attacks. International Journal of Computer Applications, 182(33), 975–8887. www.ijcaonline.org
13. Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2019). Phishing and Cybercrime Risks in a University Student Community. The International Journal of Cybersecurity Intelligence and Cybercrime, 2(1), 4–23. https://doi.org/10.52306/02010219RZEX445
14. Casagrande, M., Conti, M., Fedeli, M., & Losiouk, E. (2023). Alpha Phi-shing Fraternity: Phishing Assessment in a Higher Education Institution. Journal of Cybersecurity Education Research and Practice, 2022(2). https://doi.org/10.32727/8.2023.1
15. De Ramos, N. M., & Esponilla II, F. D. (2022). Cybersecurity program for Philippine higher education institutions: A multiple-case study. International Journal of Evaluation and Research in Education (IJERE), 11(3), 1198. https://doi.org/10.11591/ijere.v11i3.22863
16. 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), 1–35. https://doi.org/10.1145/3469886
17. Diaz, A., Sherman, A. T., & Joshi, A. (2020). Phishing in an academic community: A study of user susceptibility and behavior. Cryptologia, 44(1), 53–67. https://doi.org/10.1080/01611194.2019.1623343
18. Gan, C. L., Lee, Y. Y., & Liew, T. W. (2024). Fishing for phishy messages: predicting phishing susceptibility through the lens of cyber-routine activities theory and heuristic-systematic model. Humanities and Social Sciences Communications, 11(1), 1552. https://doi.org/10.1057/s41599-024-04083-1
19. Gwenhure, A. K. (2025). University students' security behavior against email phishing attacks: insights from the health belief model. Journal of Cybersecurity, 11(1). https://doi.org/10.1093/cybsec/tyaf034
20. Hakim, Z. M., Ebner, N. C., Oliveira, D. S., Getz, S. J., Levin, B. E., Lin, T., Lloyd, K., Lai, V. T., Grilli, M. D., & Wilson, R. C. (2021). The Phishing Email Suspicion Test (PEST) a lab-based task for evaluating the cognitive mechanisms of phishing detection. Behavior Research Methods, 53(3), 1342–1352. https://doi.org/10.3758/s13428-020-01495-0
21. Han, M., Zhao, H., Ma, X., & Shi, R. (2025). Influencing factors of information security behavior among college students based on protection motivation theory: evidence from China. Frontiers in Public Health, 13. https://doi.org/10.3389/fpubh.2025.1677024

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

22. Ismail, N. N. S., Fammy Rikzan, F. I., Katuk, N., Hashim, N. L., & Mohd Zulkefli, N. A. (2023). ENHANCING INFORMATION SECURITY AWARENESS ON PHISHING AMONG IT STUDENTS: A PILOT TEST CASE STUDY AT POLITEKNIK TUANKU SYED SIRAJUDDIN. Journal of Digital System Development, 1, 12–23. https://doi.org/10.32890/jdsd2023.1.2
23. Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. Human-Centric Computing and Information Sciences, 10(1), 33. https://doi.org/10.1186/s13673-020-00237-7
24. Kuraku, S., Kalla, D., Smith, N., & Samaah, F. (2023). Exploring How User Behavior Shapes Cybersecurity Awareness in the Face of Phishing Attacks. International Journal of Computer Trends and Technology, 71, 74–79. https://doi.org/10.14445/22312803/IJCTT-V71I11P111
25. Lee, Y. Y., Gan, C. L., & Liew, T. W. (2023). Susceptibility to instant messaging phishing attacks: does systematic information processing differ between genders? Crime Prevention and Community Safety, 25(2), 179–203. https://doi.org/10.1057/s41300-023-00176-2
26. Le-Nye, E. N. M., Yaacoub, C., & Possik, J. (2024). Evaluating Phishing Awareness Strategies: A Comparative Study of Education-based approaches and Game-based learning. Procedia Computer Science, 251, 666–671. https://doi.org/10.1016/j.procs.2024.11.166
27. Lin, T., Capecci, D. E., Ellis, D. M., Rocha, H. A., Dommaraju, S., Oliveira, D. S., & Ebner, N. C. (2019). Susceptibility to Spear-Phishing Emails. ACM Transactions on Computer-Human Interaction, 26(5), 1–28. https://doi.org/10.1145/3336141
28. Mouncey, E., & Ciobotaru, S. (2025). Phishing scams on social media: An evaluation of cyber awareness education on impact and effectiveness. Journal of Economic Criminology, 7, 100125. https://doi.org/10.1016/j.jeconc.2025.100125
29. Nasser, G., Morrison, B. W., Bayl-Smith, P., Taib, R., Gayed, M., & Wiggins, M. W. (2020). The Role of Cue Utilization and Cognitive Load in the Recognition of Phishing Emails. Frontiers in Big Data, 3. https://doi.org/10.3389/fdata.2020.546860
30. Okokpujie, K., Ariyo, M. A., Moninuola, F. S., Akanle, M. B., & Okokpujie, I. P. (2025). Evaluating Students' Vulnerability and Awareness to Phishing Attacks in Educational Institutions. International Journal of Safety and Security Engineering, 15(3), 621–630. https://doi.org/10.18280/ijsse.150320
31. Omorog, C. D., & Medina, R. P. (2020). Internet Security Awareness of Filipinos: A Survey Paper. https://doi.org/10.25147/ijcsr.2017.001.1.18
32. Romel, M., Florendo, B. B., Jacob, M., Ranit, B., Jnel, M. E., Filamor, M., Marinella, M., & Armeza, J. I. (2025). Examining Cybersecurity Awareness Among College Students Across Various Year Levels in the Province of Laguna. www.ijfmr.com
33. Ruzaili, H., Katuk, N., Zaini, K., & Abdullah, W. (2026). PHISHING AWARENESS AND PREVENTIVE MEASURES AMONG UNIVERSITY STUDENTS: KNOWLEDGE, BEHAVIORS, AND VICTIMISATION PERSPECTIVES. Millenium: Journal of Education, Technologies, and Health, 2026(29). https://doi.org/10.29352/mill0229.43489
34. Siedlecki, S. L. (2020). Understanding Descriptive Research Designs and Methods. Clinical Nurse Specialist, 34(1), 8–12. https://doi.org/10.1097/NUR.0000000000000493
35. Slater, P., & Hasson, F. (2025). Quantitative Research Designs, Hierarchy of Evidence and Validity. Journal of Psychiatric and Mental Health Nursing, 32(3), 656–660. https://doi.org/10.1111/jpm.13135
36. Sturman, D., Bell, E. A., Auton, J. C., Breakey, G. R., & Wiggins, M. W. (2024). The roles of phishing knowledge, cue utilization, and decision styles in phishing email detection. Applied Ergonomics, 119, 104309. https://doi.org/10.1016/j.apergo.2024.104309
37. Tanti, R. (2024). Study of Phishing Attack and their Prevention Techniques. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 08(10), 1–8. https://doi.org/10.55041/IJSREM38042
38. Vivien A. Agustin, Joseph Darwin C. Co, Raymund M. Dioses, Criselle J. Centeno, Angeli Joy M. Farol, & Patricia Jenel P. Marcelo. (2024). Unveiling shadows: A gamified approach to raise awareness and combat phishing tactics. World Journal of Advanced Research and Reviews, 24(2), 2077–2084. https://doi.org/10.30574/wjarr.2024.24.2.3453

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

39. William Vortia. (2025). Modelling cybersecurity awareness, perceived threats and secure online behavioral intentions among Ghanaian university students: A PLS-SEM Approach. Magna Scientia Advanced Research and Reviews, 14(2), 096–111. https://doi.org/10.30574/msarr.2025.14.2.0094
40. Yin, D., Mullarkey, M., de Vreede, G.-J., & Limayem, M. (2025). Learning by Phishing via Post-Simulation Feedback: From Embedded to Non-Embedded Training. MIS Quarterly, 1–17. https://doi.org/10.25300/MISQ/2025/19354