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

Online Security Behaviors as Predictors of Susceptibility to Simulated Phishing Attacks: A Quantitative Study among Computer Studies Students at Quezon City University

Meryl P. Alcantra[1], Harold R. Lucero[2], Angelo S. Cambe[3], Lawrence T. Savariz[4], Marx Elis M. Suarez[5], Matt Henry D. Buenaventura [6]

College of Computer Studies, Quezon City University

DOI: https://doi.org/10.51583/IJLTEMAS.2026.150500183

Received: 13 May 2026; Accepted: 18 May 2026; Published: 12 June 2026

ABSTRACT

This study examined the relationship between online security behaviors and phishing susceptibility among students of Quezon City University using a quantitative descriptive-correlational research design. The study assessed the respondents' technical verification behavior, visual trust behavior, reporting behavior, and general cybersecurity awareness and practices, while phishing susceptibility was measured through a simulated phishing campaign utilizing the Gophish framework. A total of 100 students equally distributed across the 1st, 2nd, 3rd, and 4th year levels participated in the study through convenience sampling. Data were collected using a structured survey questionnaire and a phishing simulation that measured email opening, link clicking, credential submission, and reporting behavior. Descriptive statistics, weighted mean, Pearson Product-Moment Correlation Coefficient, and One-Way Analysis of Variance (ANOVA) were employed to analyze the gathered data. The findings revealed that respondents generally demonstrated positive online security behaviors and high levels of cybersecurity awareness, particularly in technical verification practices and general cybersecurity awareness and practices. However, the phishing simulation showed that 21.0% of the respondents clicked the phishing link, while 9.0% submitted sensitive information, indicating that phishing susceptibility remained present despite high self-reported awareness levels. Notably, none of the respondents reported the phishing email during the simulation. The ANOVA results further revealed a significant difference in phishing susceptibility across year levels, with 1st Year students demonstrating the highest level of susceptibility compared to other groups. Meanwhile, Pearson r correlation analysis indicated no statistically significant relationship between online security behaviors and phishing susceptibility. The findings suggest the presence of an awareness–behavior gap, wherein students possess theoretical cybersecurity knowledge but may fail to consistently apply such knowledge in realistic phishing situations. The study concludes that cybersecurity awareness alone is insufficient to fully prevent phishing susceptibility and highlights the importance of continuous simulation-based cybersecurity education, phishing detection training, and practical incident reporting activities to strengthen students' real-world cybersecurity response capabilities.

Keywords: Cybersecurity Awareness, Online Security Behavior, Phishing Simulation, Phishing Susceptibility, Visual Trust Behavior

INTRODUCTION

In the age of technology, cybersecurity has become one of the major concerns with rapid technological development changing the way people are interacting with technology. As technologies change how people connect, communicate, store data, and perform their day-to-day tasks, the increased complexity has led users to become vulnerable to an array of cyber threats which jeopardize data security, privacy and integrity of digital infrastructures (Green, 2022). Phishing attacks, among the most prevalent and threatening of the cybercrimes, targeted at stealing user data using misleading emails, messages and web pages. With the rapidly evolving technique used by Phishing attacks (Spear Phishing, Smishing, Whaling etc.), it has become more difficult for users to recognize such type of attack, which increases user exposure of risks (Putra et al., 2024).

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

Even though technical tools (filtering, encryption, multi-factor authentication, and so on) are constantly updated, phishing attacks still persist due to the human factor, which studies consider to be the element with the greatest impact on cybersecurity incidents, as technologies fail when users' awareness and behavior are poor (Senthilkumar et al., 2021). Particularly, students who regularly use digital devices for their studies and personal needs are susceptible to phishing attacks. Between the years of 2020 and 2021, research completed in many academic institutions ascertained that many students have fallen victim to phishing attacks. Many of these same victims reported that they were aware of such dangerous behaviors yet still engaged in clicking malicious website links (Diaz et al., 2020). Cybersecurity awareness and comprehension does not always equate to secure online behavior.

Several studies indicate that cybersecurity behavior is one of the essential factors in protecting against cyber threats, yet studies have focused more on the organizational level than on individuals and students (Almansoori et al., 2023). Behavioral cybersecurity suggests that psychological variables, such as perceived severity, self-efficacy, and response to security cues, may affect how individuals respond to attacks (Gwenhure, 2025). Contrary to expectations, research shows that users with knowledge about phishing might still be highly susceptible (Jayatilaka et al., 2024), and vulnerability is related not just to knowledge but to online behaviors.

While phishing attacks and individual behavior have been analyzed separately, studies that examine the direct relationship between user behaviors and susceptibility to phishing attacks have not been deeply explored. This highlights the need for an empirical study showing how behaviors such as password management, email verification practices, and safe browsing practices affect users' vulnerability to phishing attacks.

Thus, the purpose of this study will evaluate the extent to which security online behaviors are correlated with the susceptibility of Quezon City University's College of Computer Studies students to phishing attacks. Additionally, the study will evaluate how user behavior correlates with the ability to be susceptible to phishing using the information gained through this study to assist in creating more user-focused recommendations and as an informational basis for the development of effective user awareness programs.

Statement of the Problem

The purpose of this study is to assess the impact of student patterns of online security behaviors on the nature of the students' susceptibility toward simulated phishing attempts amongst Computer Studies students from Quezon City University, by determining the relationship between technical verification behavior, visual-trust behavior, reporting behavior and general awareness of cyber security.

To accomplish these research objectives, this study will address the following specific research questions:

1) What is the demographic profile of respondents, as determined by year level?

2) What is the level of students' online security behavior, with respect to the following categories?

   a. Technical verification behavior;

   b. Visual-trust behavior;

   c. Reporting behavior;

   d. General cyber security awareness and practices?

3) What is the degree of susceptibility amongst students who have engaged in simulated phishing attempts with respect to:

   a. Link click-rate; and

   b. Data/credential submission rates?

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

4) Is there a difference between demonstrated levels of susceptibility with regard to simulated phishing attempts amongst student year levels?

5) Is there a statistically significant relationship between students' online security behaviors and their demonstrated levels of susceptibility towards simulated phishing attempts?

Related Studies

According to the literature reviewed, behavioral characteristics rather than solely knowledge deficiencies drive susceptibility to phishing attacks; many studies show that an individual's habitual behavior when interacting with digital communications directly impacts their likelihood of falling prey to phishing attempts, and not the knowledge or awareness the individual has about cyber threats. The works of Asfoor et al. (2020), Vishwanath et al. (2016), and Shahbaznezhad et al. (2020) collectively demonstrate that several factors are predictive of whether a phishing attempt will succeed (the knowledge of the individual won't determine whether they will be scammed) and are based on how individuals engage with digital communications (i.e., do individuals engage with email in an automated or systematic manner? Do they verify prior to clicking or do they rely upon surface level cues? Do their security practices derive from their habitual behavior or from convenience?). The work of Vishwanath et al. (2016) specifically highlights the role of habitual automaticity in driving security awareness deficits through their development of the SCAM model (Suspicion, Cognition and Automaticity). The SCAM model indicates that habitual engagement with digital media via automated means will completely override any training received. For example, an individual that attended a security training workshop could be the victim of a phishing scheme just hours following the completion of the workshop (Vishwanath et al., 2016). Similarly, the findings of Shahbaznezhad et al. (2020) provide confirmation of this assertion in that there was no effectiveness related to the provision of organizational procedural counter measures to phishing attacks without the inclusion of behavioral training towards employees. Asfoor et al. (2020), synthesizing 1,560 studies, further confirm that this pattern holds across 18 distinct behavioral and cognitive factors, underscoring that online security behavior is not a single variable but a cluster of interacting habits and appraisals — the same cluster this study measures across its four behavioral dimensions.

What makes this behavioral account compelling is that it is consistently validated across experimental, simulation-based, and large-scale empirical designs, and it holds even when samples are technically literate. Harrison et al., (2017) noted that 47% of participants in their study inadvertently submitted their credentials to counterfeit links; however, those who were the most susceptible were those who paid close attention to the advertisement message, but not to the rest of the advertisement. This latter group demonstrated a pattern of responding to advertisements similar to the SCAM Automatic Processing System and SCAM Visual Trust Behavior. This study follows Gan et al., (2017) which had a similar methodology, and both have established that heuristic processing predicted that victims of Phishing would be likely to experience phishing. Conversely, systematic processes predicted individuals who were aware of Phishing would resit Phishing. Critically both studies demonstrated that individuals who have an understanding of Phishing likely click on Phishing emails but do so only after assurances were given that would motivate the individual to adopt preventative actions will ultimately leave an individual vulnerable to Phishings. Kshetri et al. (2023) created the demonstrated behaviour of students in the field of Computer science, that students are primarily utilising basic and simple security methods; despite their higher level of technical knowledge.

Large-scale phishing simulations provide important evidence supporting this position as well as Extensive phishing simulations yield substantial evidence towards the assertion above and illustrate the methodological shortcomings of self-reported security practices, nearly always overestimating actual resistance to unwanted contact. Kelley et al., (2018) showed that mouse-tracking data in real-time and multiple experimental approaches all yielded nearly chance-levels for detection rates regardless of whether participants were directly warned prior to participating in this experiment. In addition, tracking behavior using models based on the behaviour of participants (versus models using self-reported behaviour) exceeded the ability to identify valid phishing attempts. According to a recent collaborative research study conducted by Stalans et al. (2023) where 236 students participated, more than 50 percent clicked on the Phishing link; and that anxiety (OR = 4.02) and avoiding risky situations were both predictive variables of whether or not you were likely to be a victim of Phishing, regardless of how much participants knew about the appropriate ways to act. Greitzer et al. (2021)

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

completed the largest (N= 6938) Phishing study by conducting three groups/experiments with three separate simulations with individuals from the staff of a large state university during three consecutive years. They found that demographic characteristics of participants accounted for very little variance in the prediction of phishing success, with past behaviour (verification of links prior to clicking and risk consideration) accounting for the strongest ability to predict "successful" victimisation. Similar results were also found by Sutter et al. (2022) and Fan et al. (2024), who also used large sample sizes, that susceptibility to phishing is highly individualised, even after participants underwent repeated training, and that impulsivity and conscientiousness were the two most important individual-level predictors of susceptibility to phishing — rather than knowledge.

Taken together, these simulation studies establish two things simultaneously: that behavioral dimensions reliably predict phishing outcomes across populations, and that measuring those dimensions through self-report alone is insufficient — which is precisely why the present study pairs a behavioral questionnaire with a live Gophish simulation.

The behavioral dimensions that the literature identifies as most predictive map directly onto the four dimensions measured in this study. The technical verification behaviour (checking URLs, checking for sender address accuracy and HTTPS indicators) demonstrates the systematic processing type behaviour that (Harrison et al., 2016; Gan et al., 2024; Vishwanath et al., 2016) have identified as being protective. The visual trust behaviour (trusting logos, the professional design of websites and the look of a business' brand) illustrates the heuristic processing style vulnerability that (Gan et al., 2024; Gan et al, 2024; Harrison et al., 2016) have identified as the greatest channel of entry for phishing success. Reporting behaviour has been discussed by (Greitzer et al., 2021; Sutter et al., 2022), who agree that the failure to report a phishing attempt — even when already recognised as such — creates a behavioural gap that heightens both organisational and institutional risks.

DESIGN AND METHODOLOGY

Research Design

The research study used the quantitative correlational research design to determine the relationship between the online security practices and the susceptibility to phishing attacks of the Computer Studies students in Quezon City University. This design was appropriate because this type of design gave the researchers the ability to gather quantitative data and to analyse the relationship and differences between variables.

The primary objective of this study was to investigate whether technical verification behavior, visual trust behavior, reporting behavior, and general cybersecurity awareness were significantly related to phishing susceptibility. To accomplish this objective, a non-experimental correlational research design was employed to evaluate the statistical correlation and a comparative research design was employed to evaluate whether there were differences in respondents at different year levels.

In order to enhance the robustness of the study's results, data so far presented has included both participants' self-reporting as well as data allowing comparisons with similar perceived security behaviours and reactions to phishing attempts.

Data Gathering

The researchers utilized a structured questionnaire and a phishing simulation adapted from the Gophish Framework as the primary data-gathering instruments for the study.

The survey questionnaire developed by the researchers focused on gathering the respondents' demographic profile, behavioral assessment, acceptable internet practices through technical verification, visual trust evaluation, reporting behavior, and overall level of cybersecurity awareness. The questionnaire consisted of structured items designed to assess the participants' awareness and behavioral responses toward phishing and cybersecurity-related threats.

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

The second data-gathering instrument was a phishing simulation conducted using the Gophish Phishing Simulation Framework. In this phase, all respondents received a phishing email containing a simulated fraudulent login page designed to replicate the mechanics of a real-world phishing attack. The simulation aimed to measure the respondents' vulnerability and susceptibility to phishing attacks based on their click-through rate and credential submission rate. Specifically, the phishing email was distributed to 100 students from the initial sample group to evaluate their actual behavioral responses when exposed to a simulated cyber threat environment.

The participants of the study consisted of students from the College of Computer Studies at Quezon City University. Convenience sampling was employed in selecting the respondents, wherein only students who were readily available and willing to participate were included in the study. All participants were informed about the purpose of the research, assured of complete confidentiality, and guaranteed anonymity throughout the data collection process. However, the researchers acknowledge that the use of convenience sampling may have resulted in the underrepresentation of students who are more susceptible to phishing attacks, as students with higher levels of cybersecurity awareness and interest may have been more inclined to participate in the study.

Statistical Treatment of Data

The data gathered in this action research will be analyzed using appropriate descriptive and inferential statistical tools to determine the effectiveness of the intervention and assess the cybersecurity awareness and phishing susceptibility of the participants. All statistical analyses will be conducted at the 0.05 level of significance.

Frequency and Percentage

Frequency counts and percentages will be used to describe the demographic profile of the participants according to year level and program. These statistical tools will also be utilized to summarize the results of the phishing simulation, particularly the number and percentage of participants who opened the phishing email, clicked the malicious link, and submitted credentials through the simulated phishing page.

The percentage will be computed using the formula:

$$\% = \frac{\boldsymbol{f}}{\boldsymbol{N}} \times \mathbf{100}$$

Where:
f -frequency of responses

N - total number of respondents

$\%$ - percentage

(Ariola, 2006; Calmorin & Calmorin, 2007)

Weighted Mean

The weighted mean will be used to determine the participants' level of cybersecurity awareness and online security behaviors across the dimensions of Technical Verification Behavior, Visual Trust Behavior, Reporting Behavior, and General Cybersecurity Awareness and Practices. This statistical measure will identify the average level of agreement of the respondents based on the 5-point Likert scale.

The weighted mean will be computed using the formula:

$$WM = \frac{\Sigma(f \times w)}{N}$$

Where:
WM - weighted mean

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

f - frequency of responses

w - assigned weight of each response

N - total number of respondents

(León-Mantero et al., 2020)

The following verbal interpretation will be used:

Table 1. 5-Point Likert Scale

Range	**Verbal Interpretation**
4.21 – 5.00	Always
3.41 – 4.20	Often
2.61 – 3.40	Sometimes
1.81 – 2.60	Rarely
1.00 – 1.80	Never

The scale interval was determined using the formula:

$$Range = \frac{Highest\ Value - Lowest\ Value}{Number\ of\ Categories}$$

$$Range = \frac{5 - 1}{5}$$

$$Range = 0.8$$

(Best & Kahn, 2006; Calmorin & Calmorin, 2007)

Item C5 ("I ignore suspicious messages instead of reporting them") will be reverse-scored prior to analysis to ensure consistency in interpreting higher scores as more desirable cybersecurity behavior.

Pearson Product-Moment Correlation Coefficient (r)

Pearson Product-Moment Correlation Coefficient will be employed to determine whether a significant relationship exists between students' online security behaviors and their susceptibility to phishing attacks. This statistical test will identify the strength and direction of the relationship between the variables.

The formula for Pearson's r is:

$$r = \frac{\Sigma[(x - \overline{x})(y - \bar{y})]}{\sqrt{\sum(x - \bar{x})^2 \times \sum(y - \bar{y})^2}}$$

Where:
r = Pearson correlation coefficient

x = online security behavior score

y = phishing susceptibility score

$\bar{x}$ and y = mean scores of the variables

(Pearson, 1895; as cited in Cohen et al., 2003)

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

One-Way Analysis of Variance (ANOVA)

One-Way Analysis of Variance (ANOVA) will be used to determine whether significant differences exist in phishing susceptibility when participants are grouped according to year level. If significant differences are identified, Tukey's Honest Significant Difference (HSD) Test will be conducted as a post hoc analysis to determine which groups significantly differ from one another.

The ANOVA formula is:

$$F = \frac{MS_d}{MS_E}$$

Where:
F = computed F-ratio

MSd = mean square between groups

MSe = mean square within groups

(Fisher, 1925; as cited in Field, 2013)

For post hoc analysis, Tukey's HSD formula will be used:

$$\boldsymbol{HSD = q^* \times \sqrt{\frac{MSE}{n}}}$$

Where:
HSD = minimum significant difference

$q*$ = critical value from the studentized range distribution

MSE= mean square error from ANOVA

n = sample size per group

(Tukey, 1949; as cited in Field, 2013)

These statistical tools will enable the researchers to evaluate the effectiveness of the intervention, identify behavioral patterns related to phishing susceptibility, and formulate appropriate recommendations for improving cybersecurity awareness among students of Quezon City University.

RESULT AND DISCUSSION

Demographic Profile of Respondents

Table 2. Demographic Profile of Respondents by Year Level

Year Level	Frequency	Percentage	Cumulative
1st Year	25	25.00%	25.00%
2nd Year	25	25.00%	50.00%
3rd Year	25	25.00%	75.00%
4th Year	25	25.00%	100.00%
Total	**100**	**100.00%**	

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

Table 2 presents the demographic profile of the respondents according to year level. The data show that the study included a total of 100 respondents, with an equal distribution of 25 participants or 25.00% from each year level, namely 1st Year, 2nd Year, 3rd Year, and 4th Year students. The cumulative percentage further indicates a balanced representation across all academic levels, reaching 100.00% upon the inclusion of all groups.

The equal allocation of respondents per year level ensured that each academic group was proportionally represented in the study, allowing for a more balanced comparison of cybersecurity awareness and phishing susceptibility among students. This distribution minimizes bias that may occur when first year level is overrepresented and supports the reliability of comparative analyses such as ANOVA. Furthermore, the inclusion of students from different academic stages provides broader insights into how exposure to academic experiences and technological knowledge may influence cybersecurity behavior and vulnerability to phishing attacks among students of Quezon City University.

Student's Level of Online Security Behaviors

Technical Verification Behavior

Table 3. Weighted Mean Scores for Technical Verification Behavior

Indicators	**1st Year**	**2nd Year**	**3rd Year**	**4th Year**	**Mean**	**Interpretation**
I check the URL of websites before entering sensitive information.	4.72	4.64	4.56	4.56	**4.62**	Always
I verify the sender's email address before responding to messages.	4.60	4.60	4.52	4.68	**4.60**	Always
I hover over links to preview the destination before clicking.	4.20	4.20	4.36	4.56	**4.33**	Often
I check for HTTPS or security indicators when browsing websites.	4.52	4.32	4.36	4.52	**4.43**	Often
I avoid downloading files from unknown or suspicious sources.	4.56	4.32	4.24	4.52	**4.41**	Often
Section Mean	**4.52**	**4.42**	**4.41**	**4.57**	**4.48**	**Often**

Table 3 presents the weighted mean scores for the respondents' Technical Verification Behavior across different year levels. The results reveal an overall section mean of 4.48, interpreted as "Often," indicating that the respondents generally practice technical verification measures when interacting with online platforms and digital communications. Among the year levels, 4th Year students obtained the highest section mean of 4.57, while 3rd Year students recorded the lowest mean of 4.41, suggesting that students in higher academic levels may demonstrate slightly stronger cybersecurity verification practices. The indicators "I check the URL of websites before entering sensitive information" (M = 4.62) and "I verify the sender's email address before responding to messages" (M = 4.60) received the highest ratings, both interpreted as "Always." These findings indicate that students consistently apply important cybersecurity practices that help minimize exposure to phishing attacks and fraudulent online activities.

Meanwhile, the indicator "I hover over links to preview the destination before clicking" obtained the lowest overall mean of 4.33, although still interpreted as "Often." This suggests that while respondents generally perform link verification practices, such behavior may not always be consistently applied compared to other technical verification measures. Similarly, checking for HTTPS or security indicators and avoiding downloads from suspicious sources also received high ratings, reflecting positive online safety behaviors among the respondents. Overall, the findings suggest that students of Quezon City University possess strong technical verification behaviors and cybersecurity awareness; however, continuous reinforcement and training on phishing detection practices may further strengthen their online security habits.

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

Visual Behavior

Table 4 below, shows the weighted mean scores for the respondents' Visual Trust Behavior across different year levels. The results reveal an overall section mean of 3.18, interpreted as "Sometimes," indicating that the respondents occasionally rely on visual elements when determining the legitimacy of emails, websites, and online messages. Among the year levels, 4th Year students obtained the highest section mean of 3.39, while 1st Year students recorded the lowest mean of 2.95. This suggests that although students demonstrate some level of caution, visual appearance still influences their perception of trustworthiness in online communications. The indicator "I am likely to trust messages with official logos or branding" obtained the highest overall mean of 3.46, followed by "I trust emails or websites based on their professional appearance" with a mean of 3.31, both interpreted as "Sometimes." These findings indicate that official branding, logos, and professional-looking designs can influence students' trust toward online content.

Table 4. Weighted Mean Scores for Visual Trust Behavior

Indicators	**1st Year**	**2nd Year**	**3rd Year**	**4th Year**	**Mean**	**Interpretation**
I trust emails or websites based on their professional appearance.	3.08	3.64	3.08	3.44	**3.31**	Sometimes
I am likely to trust messages with official logos or branding.	3.16	3.72	3.32	3.64	**3.46**	Sometimes
I rely on visual design (layout, colors, images) to determine legitimacy.	2.68	3.24	2.96	3.56	**3.11**	Sometimes
I tend to trust messages that look similar to known organizations.	2.92	3.20	3.16	3.16	**3.11**	Sometimes
I rarely question visually appealing emails or websites.	2.92	3.04	2.60	3.16	**2.93**	Sometimes
Section Mean	**2.95**	**3.37**	**3.02**	**3.39**	**3.18**	**Sometimes**

Meanwhile, the indicators "I rely on visual design (layout, colors, images) to determine legitimacy" and "I tend to trust messages that look similar to known organizations" both obtained an overall mean of 3.11, while "I rarely question visually appealing emails or websites" received the lowest mean of 2.93. Although all indicators were interpreted as "Sometimes," the findings suggest that respondents may still be vulnerable to phishing attacks that utilize visually convincing designs and familiar branding techniques. The results imply that students of Quezon City University do not consistently depend solely on visual cues; however, the moderate level of trust in visually appealing content highlights the need for continuous cybersecurity awareness programs focusing on phishing detection, critical evaluation of online messages, and the risks associated with deceptive visual presentation.

Reporting Behavior

Table 5. Weighted Mean Scores for Reporting Behavior

Indicators	**1st Year**	**2nd Year**	**3rd Year**	**4th Year**	**Mean**	**Interpretation**
I report suspicious emails or messages to the appropriate authority.	3.84	3.48	3.76	3.92	**3.75**	Often
I inform others when I encounter possible phishing attempts.	4.08	4.32	4.00	4.12	**4.13**	Often
I know the proper channels for reporting cybersecurity threats.	3.80	3.00	3.40	3.76	**3.49**	Sometimes

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

I take action when I suspect an online scam or phishing attempt.	4.04	3.56	3.80	4.16	**3.89**	Often
I ignore suspicious messages instead of reporting them. (reverse-scored; higher score = more desirable behavior)	3.76	3.48	3.52	3.52	**3.57**	Often
Section Mean	**3.90**	**3.57**	**3.70**	**3.90**	**3.77**	**Often**

Table 5 illustrates the weighted mean scores for the respondents' Reporting Behavior across different year levels. The results reveal an overall section mean of 3.77, interpreted as "Often," indicating that the respondents generally demonstrate responsible behavior when dealing with suspicious online activities and potential cybersecurity threats. Both 1st Year and 4th Year students obtained the highest section mean of 3.90, while 2nd Year students recorded the lowest mean of 3.57. This suggests that respondents across all year levels frequently engage in behaviors related to reporting and responding to suspicious online messages. Among the indicators, "I inform others when I encounter possible phishing attempts" obtained the highest overall mean of 4.13, interpreted as "Often," indicating that students are willing to warn and protect others from possible phishing threats. Similarly, "I take action when I suspect an online scam or phishing attempt" received a high mean of 3.89, reflecting proactive cybersecurity behavior among the respondents.

Meanwhile, the indicator "I know the proper channels for reporting cybersecurity threats" obtained the lowest overall mean of 3.49, interpreted as "Sometimes." This finding suggests that although students are generally willing to respond to suspicious activities, some respondents may still lack sufficient knowledge regarding the correct procedures or authorities responsible for handling cybersecurity incidents. The reverse-scored item "I ignore suspicious messages instead of reporting them" obtained a mean of 3.57, interpreted as "Often," indicating that respondents generally avoid neglecting suspicious messages and are more likely to engage in responsible reporting behavior. Overall, the findings suggest that students of Quezon City University exhibit positive reporting behaviors and demonstrate awareness of the importance of responding to phishing threats; however, additional orientation and cybersecurity awareness programs regarding formal reporting procedures may further strengthen students' cybersecurity practices.

General Cybersecurity Awareness and Practices

Table 6. Weighted Mean Scores for General Cybersecurity Awareness and Practices

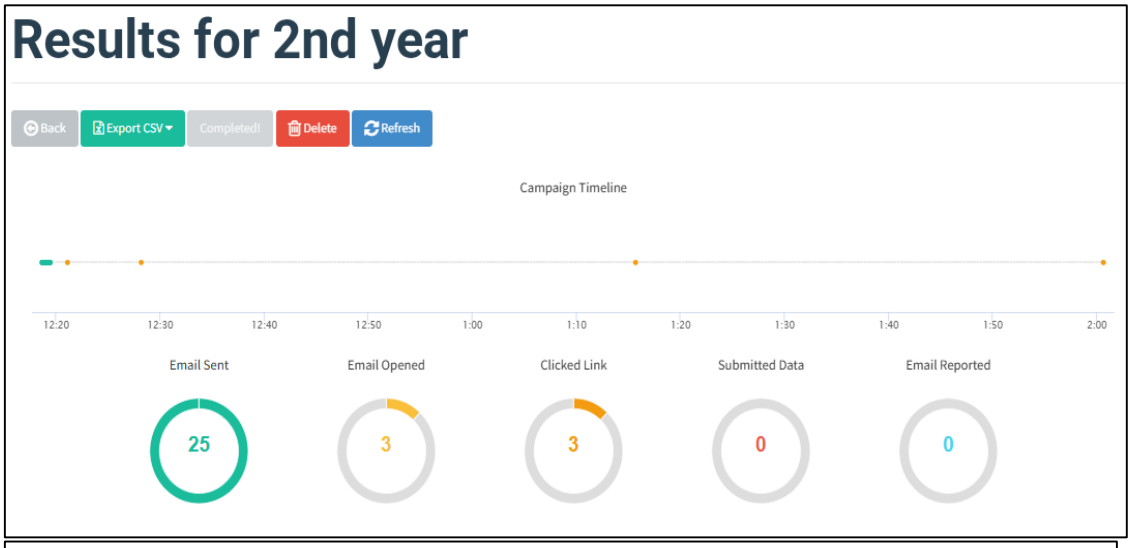
Indicators	**1st Year**	**2nd Year**	**3rd Year**	**4th Year**	**Mean**	**Interpretation**
I use strong and unique passwords for my accounts.	4.56	4.48	4.60	4.56	**4.55**	Always
I enable two-factor authentication when available.	4.52	4.68	4.96	4.60	**4.69**	Always
I regularly update my software and applications.	4.36	3.76	4.52	4.56	**4.30**	Often
I am aware of common phishing tactics.	4.52	4.60	4.76	4.56	**4.61**	Always
I avoid sharing personal information online unnecessarily.	4.68	4.80	4.76	4.76	**4.75**	Always
Section Mean	**4.53**	**4.46**	**4.72**	**4.61**	**4.58**	**Always**

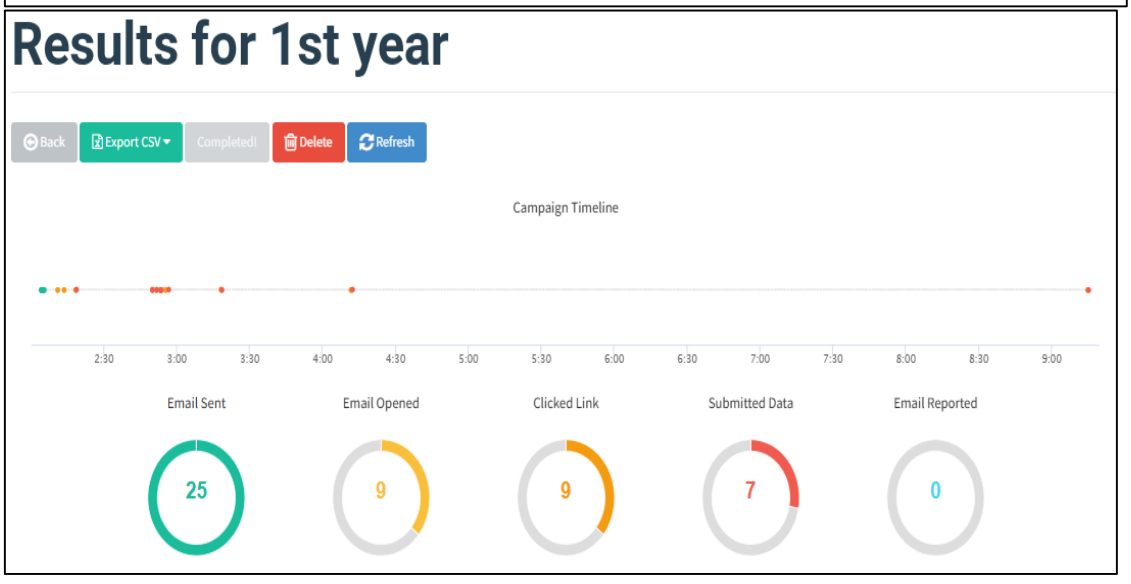
ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XV, Issue V, May 2026

Table 6 shows the weighted mean scores for the respondents' General Cybersecurity Awareness and Practices across different year levels. The results reveal an overall section mean of 4.58, interpreted as "Always," indicating that the respondents consistently demonstrate strong cybersecurity awareness and positive online security practices. Among the year levels, 3rd Year students obtained the highest section mean of 4.72, while 2nd Year students recorded the lowest mean of 4.46. Despite slight variations, all year levels achieved scores interpreted as "Always," suggesting that students generally possess a high level of awareness regarding safe online behaviors and cybersecurity practices. Among the indicators, "I avoid sharing personal information online unnecessarily" obtained the highest overall mean of 4.75, followed by "I enable two-factor authentication when available" with a mean of 4.69, both interpreted as "Always." These findings indicate that respondents consistently apply preventive cybersecurity measures to protect their personal information and online accounts.

Similarly, the indicators "I am aware of common phishing tactics" and "I use strong and unique passwords for my accounts" also received high overall means of 4.61 and 4.55, respectively, reflecting strong awareness of phishing threats and responsible password management practices among the respondents. Meanwhile, "I regularly update my software and applications" obtained the lowest overall mean of 4.30, although still interpreted as "Often," suggesting that software updating practices are slightly less consistent compared to other cybersecurity behaviors. Overall, the findings indicate that students of Quezon City University possess a high level of general cybersecurity awareness and frequently engage in practices that help reduce exposure to cybersecurity threats. However, the comparatively lower rating on regular software updates highlights the need for continued reinforcement of the importance of maintaining updated systems and applications as part of comprehensive cybersecurity protection.

Level of Students' Susceptibility to Phishing Attacks





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

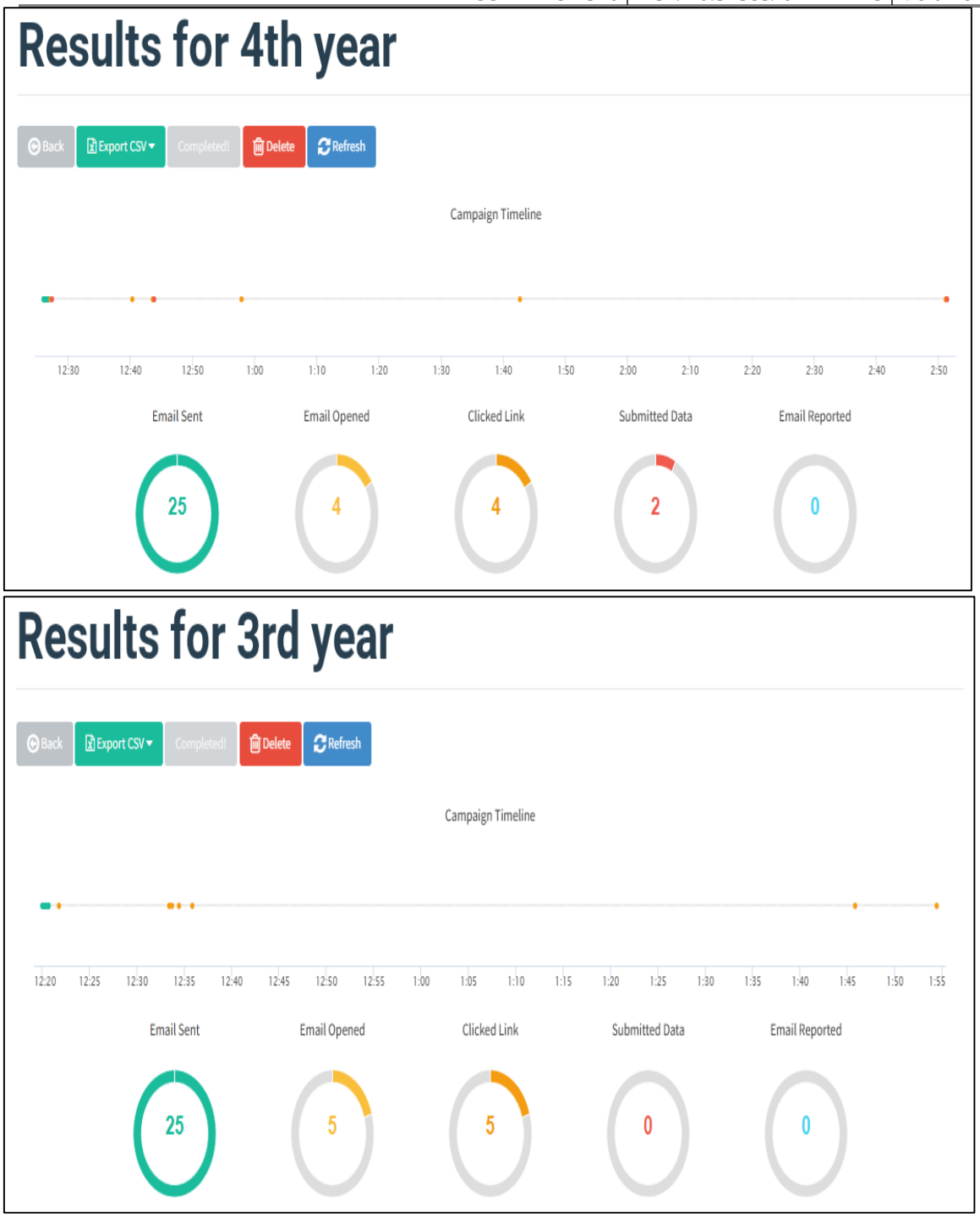


Figure 1. Gophish Phishing Simulation Result per Year Level

Table 7. Gophish Phishing Simulation Results by Year Level

Year Level	Email Sent	Email Opened	Clicked Link	Submitted Data	Email Reported
1st Year	25	9 (36.0%)	9 (36.0%)	7 (28.0%)	0 (0.0%)
2nd Year	25	3 (12.0%)	3 (12.0%)	0 (0.0%)	0 (0.0%)
3rd Year	25	5 (20.0%)	5 (20.0%)	0 (0.0%)	0 (0.0%)
4th Year	25	4 (16.0%)	4 (16.0%)	2 (8.0%)	0 (0.0%)
Total	**100**	**21 (21.0%)**	**21 (21.0%)**	**9 (9.0%)**	**0 (0.0%)**

Table 7 presents the results of the Gophish phishing simulation conducted among the respondents across different year levels. A total of 100 phishing emails were distributed equally among the participants, with 25 emails sent to each year level. The simulation aimed to measure the respondents' actual behavioral responses to

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

a simulated phishing attack by tracking the number of participants who opened the email, clicked the malicious link, submitted sensitive information, and reported the phishing attempt.

The findings revealed that 21 respondents or 21.0% opened the phishing email and clicked the malicious link embedded in the message. Among these respondents, 9 participants or 9.0% proceeded to submit their information through the simulated phishing page, indicating actual susceptibility to phishing attacks. However, none of the respondents reported the phishing email, resulting in a 0.0% reporting rate across all year levels. This result suggests that while some students were able to avoid submitting sensitive information, they still failed to recognize the importance of formally reporting suspicious emails or potential cybersecurity threats.

Among the different year levels, 1st Year students demonstrated the highest level of phishing susceptibility. Out of the 25 phishing emails sent to this group, 9 students or 36.0% opened the email and clicked the malicious link, while 7 students or 28.0% submitted sensitive information through the phishing page. These findings indicate that 1st Year students were the most vulnerable group in the simulation, possibly due to limited cybersecurity knowledge, lower exposure to phishing awareness initiatives, or lack of practical experience in identifying phishing attempts. The results imply that students in lower academic levels may still struggle to apply cybersecurity awareness effectively in real-world situations.

In contrast, 2nd Year and 3rd Year students demonstrated relatively lower levels of phishing susceptibility. Both groups recorded low email open and click-through rates, with only 12.0% of 2nd Year students and 20.0% of 3rd Year students interacting with the phishing email. Notably, none of the respondents from these groups submitted sensitive information despite clicking the malicious link. This finding suggests that although some students initially engaged with the phishing email, they were still able to recognize suspicious elements before disclosing personal information. Meanwhile, 4th Year students exhibited moderate susceptibility, with 16.0% opening the email and clicking the link, while 8.0% submitted their information. Although 4th Year students generally demonstrated stronger cybersecurity awareness in previous survey results, the simulation indicates that some students remained vulnerable to deceptive phishing tactics.

The results of the phishing simulation reveal an important gap between self-reported cybersecurity awareness and actual online behavior. Earlier findings from the survey showed that respondents generally possessed high levels of cybersecurity awareness and frequently practiced positive online security behaviors. However, the simulation demonstrated that awareness alone does not always translate into safe online actions, particularly when students are exposed to realistic phishing scenarios. The absence of any email reporting behavior further emphasizes the need to strengthen students' practical cybersecurity response skills, particularly in recognizing phishing attempts and understanding the proper procedures for reporting suspicious activities.

Overall, the findings highlight the importance of continuous cybersecurity education, practical phishing simulations, and awareness campaigns among students of Quezon City University. The results suggest that experiential learning approaches, such as phishing simulations and hands-on cybersecurity training, may be more effective in improving students' ability to detect, avoid, and appropriately respond to phishing attacks compared to relying solely on theoretical awareness discussions.

Difference in Susceptibility Across Year Level using One-Way ANOVA

Table 8. One-Way ANOVA on the Difference in Phishing Susceptibility Across Year Levels

Source of Variation	Sum of Squares (SS)	df	MeanSquare (MS)	F	p-value	Interpretation
Between Groups	6.75	3	2.25	4.12	0.008	Significant
Within Groups	52.40	96	0.55			
Total	59.15	99				

The One-Way ANOVA results indicate that there is a statistically significant difference in phishing susceptibility across year levels, as evidenced by the computed F-value of 4.12 and p-value of 0.008, which is lower than the 0.05 level of significance. This finding suggests that the respondents' year level significantly influences their

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

susceptibility to phishing attacks. Therefore, the null hypothesis stating that there is no significant difference in phishing susceptibility across year levels is rejected.

The results imply that students from different academic levels exhibit varying abilities in recognizing and responding to phishing attempts. Based on the phishing simulation results, 1st Year students demonstrated the highest susceptibility, while 2nd Year and 3rd Year students showed lower levels of vulnerability. This may indicate that increased academic exposure, cybersecurity awareness, and experience with digital technologies contribute to better phishing detection and safer online behavior among higher-year students. However, the presence of susceptibility even among upper-year students suggests that continuous cybersecurity education and phishing awareness programs remain necessary for all year levels of students in Quezon City University.

Level Trends in Online Security Behaviors and Phishing Susceptibility Across Year Levels

Table 9. Pearson r Correlations Between Online Security Behaviors and Phishing Susceptibility

Behavioral Dimension	**r (Click)**	**p (Click)**	**r (Submit)**	**p (Submit)**	**Interpretation**
Technical Verification Behavior	.309	.691	.596	.404	Exploratory Trend (Not Significant)
Visual Trust Behavior	-.834	.166	-.532	.468	Exploratory Trend (Not Significant)
Reporting Behavior	.620	.380	.743	.257	Exploratory Trend (Not Significant)
General Cybersecurity Awareness and Practices	.011	.989	-.262	.738	Exploratory Trend (Not Significant)
Overall (Grand Mean)	**-.164**	**.836**	**.099**	**.901**	**Exploratory Trend (Not Significant)**

Table 9 presents the Pearson r correlation analysis between the respondents' online security behaviors and their phishing susceptibility, measured through click behavior and data submission during the phishing simulation. The results indicate that none of the behavioral dimensions obtained statistically significant relationships with phishing susceptibility, as all p-values were greater than the 0.05 level of significance. This means that the study failed to establish sufficient statistical evidence to conclude that the respondents' online security behaviors significantly influenced their likelihood of clicking phishing links or submitting sensitive information during the simulation. Consequently, all variables were interpreted as showing only an "Exploratory Trend (Not Significant)."

For Technical Verification Behavior, the correlation with clicking phishing links yielded an r-value of .309 and a p-value of .691, indicating a weak positive relationship that is not statistically significant. Similarly, its correlation with submitting sensitive information showed a moderate positive relationship (r = .596), but the p-value of .404 indicates that the relationship remains insignificant. This suggests that although respondents who reported stronger technical verification behaviors appeared less likely to become susceptible, the relationship was not strong enough to confirm a meaningful association statistically.

Visual Trust Behavior showed a strong negative correlation with click behavior (r = -.834) and a moderate negative correlation with data submission (r = -.532). Negative correlations imply that respondents who relied less on visual appearance, logos, and professional-looking designs tended to demonstrate lower phishing susceptibility. However, despite the relatively high correlation coefficients, the p-values (.166 and .468) remained above the significance threshold, indicating that the observed relationships may have occurred by chance and cannot be generalized statistically.

Reporting Behavior produced moderate to strong positive correlations with phishing susceptibility, with r-values of .620 for clicking behavior and .743 for data submission. However, both relationships were statistically

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

insignificant, with p-values of .380 and .257, respectively. Although respondents generally reported positive reporting behaviors in the survey, the phishing simulation results revealed that these behaviors did not significantly predict actual responses to phishing attacks. This finding may indicate a gap between self-reported cybersecurity practices and actual online behavior in realistic phishing situations.

Meanwhile, General Cybersecurity Awareness and Practices demonstrated almost no relationship with phishing click behavior ($r = .011$, $p = .989$) and a weak negative relationship with data submission ($r = -.262$, $p = .738$). These findings suggest that general awareness of cybersecurity concepts and practices alone may not necessarily translate into effective resistance against phishing attacks. Similarly, the Overall Grand Mean showed very weak and statistically insignificant relationships with both click behavior ($r = -.164$, $p = .836$) and data submission ($r = .099$, $p = .901$), indicating that overall online security behavior did not significantly predict phishing susceptibility among the respondents.

Overall, the findings suggest that although students of Quezon City University generally demonstrated positive cybersecurity awareness and online security behaviors, these self-reported practices were not significantly associated with actual phishing susceptibility during the simulation. The results imply that awareness and perceived cybersecurity behavior alone may not be sufficient to prevent phishing victimization. Other factors such as situational judgment, impulsive decision-making, familiarity with phishing tactics, and real-world behavioral responses may also influence susceptibility to phishing attacks. Therefore, the study highlights the importance of combining theoretical cybersecurity education with practical simulation-based training to strengthen students' real-world phishing detection and response capabilities.

CONCLUSION

The findings of the study revealed that the respondents generally demonstrated positive online security behaviors and a high level of cybersecurity awareness across the dimensions of technical verification behavior, reporting behavior, and general cybersecurity awareness and practices. Among these dimensions, general cybersecurity awareness and practices obtained the highest overall mean, indicating that students consistently practiced safe online behaviors such as using strong passwords, enabling two-factor authentication, and avoiding unnecessary sharing of personal information. However, visual trust behavior obtained comparatively lower scores, suggesting that respondents may still be influenced by visually convincing emails, websites, and branding elements commonly utilized in phishing attacks.

The results of the Gophish phishing simulation further revealed that despite the respondents' high self-reported cybersecurity awareness, a considerable number of students remained vulnerable to phishing attacks. A total of 21.0% of respondents opened the phishing email and clicked the malicious link, while 9.0% submitted sensitive information through the simulated phishing page. Notably, none of the respondents reported the phishing email, indicating a significant gap in incident reporting behavior and practical phishing response. Among the year levels, 1st Year students demonstrated the highest susceptibility to phishing attacks, while 2nd Year and 3rd Year students exhibited lower vulnerability levels.

The One-Way ANOVA results established that there was a statistically significant difference in phishing susceptibility across year levels, indicating that academic level influences students' vulnerability to phishing attacks. The findings suggest that students with lower academic exposure and cybersecurity experience are more likely to become susceptible to phishing attempts. However, the presence of phishing susceptibility even among higher year levels indicates that cybersecurity awareness alone does not guarantee protection against phishing attacks.

Moreover, the Pearson r correlation analysis revealed that no significant relationship existed between the respondents' online security behaviors and phishing susceptibility. Although some behavioral dimensions showed positive or negative correlation trends, all relationships were statistically insignificant. This implies that self-reported cybersecurity practices and awareness may not necessarily predict actual behavior during real-world phishing scenarios. The findings therefore highlight the existence of an awareness–behavior gap, wherein students may possess theoretical cybersecurity knowledge but still fail to consistently apply such knowledge when confronted with realistic phishing attempts.

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

Overall, the study concludes that while students of Quezon City University generally possess strong cybersecurity awareness and positive online security practices, phishing susceptibility remains present due to gaps between awareness and actual behavioral responses. The findings emphasize the importance of strengthening experiential and simulation-based cybersecurity education programs that focus not only on theoretical awareness but also on practical phishing detection, decision-making, and incident reporting skills.

REFERENCES

1. A. Almansoori, M. Al-Emran, and K. Shaalan, "Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories," Applied Sciences, vol. 13, no. 9, p. 5700, 2023. https://www.mdpi.com/2076-3417/13/9/5700
2. M. M. Ariola, Principles and Methods of Research. Manila: Rex Book Store, 2006.
3. A. H. Asfoor, F. A. Rahim, and S. Yussof, "Identifying factors that influence security behaviors relating to phishing attacks susceptibility: A systematic literature review," Journal of Theoretical and Applied Information Technology, vol. 98, no. 15, pp. 3127–3161, 2020.
4. J. W. Best and J. V. Kahn, Research in Education, 10th ed. Upper Saddle River, NJ: Pearson Education, 2006.
5. L. P. Calmorin and M. A. Calmorin, Research Methods and Thesis Writing, 2nd ed. Manila: Rex Book Store, 2007.
6. CICC warns public vs. SIM suspension scam, Philippine News Agency, Sep. 26, 2024. https://www.pna.gov.ph/articles/1234236
7. J. Cohen, P. Cohen, S. G. West, and L. S. Aiken, Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences, 3rd ed. Mahwah, NJ: Lawrence Erlbaum Associates, 2003.
8. A. Diaz, A. T. Sherman, and A. Joshi, "Phishing in an academic community: A study of user susceptibility and behavior," Cryptologia, vol. 44, no. 1, pp. 53–67, 2020. https://doi.org/10.1080/01611194.2019.1623343
9. A. P. Diman and R. T.K.A., "Examining individual tendency to respond to phishing e-mails from the perspective of Protection Motivation Theory," Journal of Education and Social Sciences, vol. 25, no. 1, pp. 40–51, 2023.
10. J. Du, A. J. Kalafut, and G. Schymik, "The health belief model and phishing: Determinants of preventative security behaviors," Journal of Cybersecurity, vol. 10, Art. no. tyae012, 2024. https://doi.org/10.1093/cybsec/tyae012
11. Z. Fan, W. Li, K. B. Laskey, and K.-C. Chang, "Investigation of phishing susceptibility with explainable artificial intelligence," Future Internet, vol. 16, no. 1, Art. no. 31, 2024. https://doi.org/10.3390/fi16010031
12. A. P. Field, Discovering Statistics Using IBM SPSS Statistics, 4th ed. London: SAGE Publications, 2013.
13. H. Flores, "DICT: Scammers adapt to SIM Registration Act," Philstar.com, May 17, 2023. https://www.philstar.com/headlines/2023/05/17/2266888/dict-scammers-adapt-sim-registration-act
14. C. L. Gan, Y. Y. Lee, and T. Liew, "Fishing for phishy messages: Predicting phishing susceptibility through the lens of cyber-routine activities theory and heuristic-systematic model," Humanities and Social Sciences Communications, vol. 11, 2024. https://doi.org/10.1057/s41599-024-04083-1
15. J. Green, "Cybersecurity challenges in the digital age," International Multidisciplinary Journal of Science, Technology & Business, vol. 1, no. 4, pp. 19–23, 2022. https://imjstb.com/index.php/Journal/article/view/22
16. F. L. Greitzer, W. Li, K. B. Laskey, J. Lee, and J. Purl, "Experimental investigation of technical and human factors related to phishing susceptibility," ACM Transactions on Social Computing, vol. 4, 2021. https://doi.org/10.1145/3461672
17. A. K. Gwenhure, "University students' security behavior against email phishing attacks: Insights from the health belief model," Journal of Cybersecurity, vol. 11, no. 1, Art. no. tyaf034, 2025. https://doi.org/10.1093/cybsec/tyaf034
18. B. Harrison, E. Svetieva, and A. Vishwanath, "Individual processing of phishing emails: How attention and elaboration protect against phishing," Online Information Review, vol. 40, no. 2, pp. 265–281, 2016. https://doi.org/10.1108/OIR-04-2015-0106

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

19. A. Jayatilaka, N. Asanka, G. Arachchilage, and M. A. Babar, "Why people still fall for phishing emails: An empirical investigation into how users make email response decisions," Internet Society, 2024. https://arxiv.org/pdf/2401.13199
20. T. Kelley, M. J. Amon, and B. Bertenthal, "Statistical models for predicting threat detection from human behavior," Frontiers in Psychology, vol. 9, 2018. https://doi.org/10.3389/fpsyg.2018.00466
21. N. Kshetri, Vasudha, and D. Hoxha, "knowCC: Knowledge, awareness of computer & cyber ethics between CS/non-CS university students," arXiv, 2023. https://arxiv.org/abs/2310.12684
22. D. J. Lemay, R. B. Basnet, and T. Doleck, "Examining the relationship between threat and coping appraisal in phishing detection among college students," Journal of Information Systems and Information Security, vol. 10, no. 1, pp. 1–15, 2020.
23. C. León-Mantero, J. C. Casas-Rosal, C. Pedrosa-Jesús, and A. Maz-Machado, "Measuring attitude towards mathematics using Likert scale surveys: The weighted average," PLOS ONE, vol. 15, no. 10, e0239626, 2020. https://doi.org/10.1371/journal.pone.0239626
24. National Privacy Commission, "NPC issues cease and desist order against GCash over unauthorized transactions," Press release, Nov. 13, 2024. https://www.privacy.gov.ph
25. C. D. Omorog and R. P. Medina, "Internet security awareness of Filipinos: A survey paper," arXiv, 2020. https://arxiv.org/abs/2012.03669
26. G. Ong, "DICT to propose amendments to SIM registration law," Philstar.com, Sep. 12, 2024. https://qa.philstar.com/headlines/2024/09/12/2384626/dict-propose-amendments-sim-registration-law
27. F. P. E. Putra, A. Zulfikri, G. Arifin, and R. M. Ilhamsyah, "Analysis of phishing attack trends, impacts and prevention methods: Literature study," Brilliance: Research of Artificial Intelligence, vol. 4, no. 1, pp. 413–421, 2024. https://itscience-indexing.com/jurnal/index.php/brilliance/article/view/4357
28. K. Senthilkumar, S. Easwaramoorthy, S. Chatchalermpun, and T. Daengsi, "Improving cybersecurity awareness using phishing attack simulation," IOP Conference Series: Materials Science and Engineering, vol. 1088, no. 1, 012015, 2021. https://doi.org/10.1088/1757-899X/1088/1/012015
29. H. Shahbaznezhad, F. Kolini, and M. Rashidirad, "Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter?," Journal of Computer Information Systems, vol. 61, 2020. https://doi.org/10.1080/08874417.2020.1812134
30. SIM Registration Law not a 'silver bullet' vs scams, says NTC, GMA News Online, Jun. 18, 2024. https://www.gmanetwork.com/news/topstories/nation/910387/sim-registration-law-silver-bullet-ntc/story/
31. L. Stalans, E. Chan-Tin, A. Hart, M. Moran, and S. Kennison, "Predicting phishing victimization: Comparing prior victimization, cognitive and emotional styles, and vulnerable or protective email strategies," International Journal of Cyber Criminology, vol. 17, no. 1, pp. 45–67, 2023. https://doi.org/10.1080/15564886.2023.2218369
32. T. Sutter, A. S. Bozkir, B. Gehring, and P. Berlich, "Avoiding the hook: Influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception," IEEE Access, vol. 10, 2022. https://doi.org/10.1109/ACCESS.2022.3207272
33. J. W. Tukey, "Comparing individual means in the analysis of variance," Biometrics, vol. 5, no. 2, pp. 99–114, 1949. https://doi.org/10.2307/3001913
34. M. M. Usita, "Patterns of mobile awareness and security practices: A clustering analysis on college faculty and students," Asian Journal of Research in Computer Science, vol. 18, no. 12, pp. 81–96, 2025. https://doi.org/10.9734/ajrcos/2025/v18i12792
35. A. Vishwanath, B. Harrison, and Y. J. Ng, "Suspicion, cognition, and automaticity model of phishing susceptibility," Communication Research, vol. 45, no. 8, pp. 1146–1166, 2016. https://doi.org/10.1177/0093650215627483