Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 5, 2026

PHISHING AWARENESS AND DETECTION ABILITY AMONG SOCIAL MEDIA USERS

[1]Shehroz Ahmed Khan, [2]Muhammad Ali, [3]Hassan Hafiz Abdul Samad, [4]Hafiz Usman Ghani
[1]Department of Cyber Security Air University Multan Campus, Islamabad
[2]Department of Cyber Security Air University Multan Campus, Islamabad
[3]Department of Cyber Security Air University Multan Campus, Islamabad
[4]Department of Cyber Security Air University Multan Campus, Islamabad
[1]233644@students.au.edu.pk, [2]233645@students.au.edu.pk, [3]233647@students.au.edu.pk, [4]233616@students.au.edu.pk

DOI:-https://doi.org/10.5281/zenodo.20507689

Keywords
Phishing Awareness, Cybersecurity Education, Social Media Security, Detection Ability, Behavioral Protection Practices

Article History
Received: 16 May, 2026
Accepted: 25, May 2026
Published: 28 May, 2026

Corresponding Author: *

Abstract
Phishing attacks are among the most common and damaging cybersecurity threats in today's digital world, and they continue to grow more sophisticated with every passing year. Unlike technical attacks that target system vulnerabilities, phishing works by manipulating human behavior, making awareness and education the most important line of defense. University students, especially those studying computing and technology, are a particularly important group to study because they are highly active online and will soon enter professional roles where cybersecurity decisions carry real consequences. This study examines phishing awareness, detection ability, and behavioral protection practices among undergraduate and graduate students in Pakistan, a context that has received very little attention in existing cybersecurity research. A quantitative cross-sectional survey design was used, and data were collected through a structured questionnaire covering phishing awareness, detection ability, real-world scenarios, and behavioral practices. The findings indicate that students generally demonstrate a reasonable level of awareness of phishing threats and express confidence in their ability to detect them; however, their actual protective behaviours in daily online activity remain inconsistent and do not always align with their level of knowledge. Scenariobased responses further highlight that socially framed attacks and URL manipulation techniques can still mislead users. The study concludes that practical, scenario-based training and hands-on tool demonstrations are essential to bridge the gap between phishing awareness and effective protective behavior among Pakistani university students.

1. Introduction

Almost every aspect of daily life today depends on the internet, making digital platforms essential for communication, education, and social interaction. However, this rapid digital growth has also increased exposure to cybersecurity threats, especially for young users. Among these threats, phishing has become one of the most widespread and dangerous forms of cyberattack because it targets human behavior rather than technical systems. As online activity continues to rise, understanding how individuals respond to such threats has become increasingly important.

1.1 Background of the Research

Phishing is a type of social engineering assault where attackers pose as reliable organisations in order to trick victims into disclosing private information such passwords, bank account information, or personal identification numbers. Phishing is the main attack vector in most social engineering instances, and human involvement is responsible for about 68% of all cybersecurity breaches, according to the 2024 Verizon Data Breach Investigations Report. Social networking platforms have surpassed traditional email channels as the most exploited digital environment, making them a prime target for phishing attempts. Phishing-as-a-service (PhaaS) platforms' widespread use and the incorporation of artificial intelligence into attack techniques have greatly reduced the technical barrier for offenders. A growing percentage of corporate email compromise (BEC) attacks now involve AI-generated phishing communications, and in 2024, the financial impact of these risks hit all-time highs. Because of the growing threat landscape, cybersecurity awareness training is not only helpful but also necessary, especially for the next generation of computer professionals. Students in universities, especially those pursuing degrees in computer science and information technology, fall into two categories of interest: they are anticipated to become the next generation of cybersecurity professionals and are also extremely engaged with technology. However, empirical data regularly shows that preventive behavioural behaviours do not often follow from academic understanding with cybersecurity topics. The primary empirical concern of the current study is the disparity between awareness and behaviour. The awareness-behavior gap is repeatedly identified as the primary difficulty in phishing education by existing research, such as studies by Alshamrani et al. (2018), Salahdine and Kaabouch (2019), and Hassan et al. (2025). The significance of context-specific empirical research is shown by studies conducted in the South Asian setting, such as those by AlHamar et al. (2023) and Siddiqui et al. (2024), which confirm that institutional and geographical factors strongly impact students' risk profiles.

1.2 Problem Statement

There are still a number of significant gaps in both study and practice, despite the growing institutional and scholarly emphasis on cybersecurity education. There is little empirical data on phishing awareness among Pakistani university students, which prevents policymakers from creating effective, situation-specific courses. Furthermore, a substantial portion of current research focuses on technical detection methods while mainly ignoring the behavioural and emotional factors that make people vulnerable to phishing attempts. In the context of Pakistani higher education, there is also a dearth of trustworthy and validated instruments that assess the combined impact of awareness, detecting abilities, and behavioural intents. This clearly limits our ability to comprehend how pupils react to actual phishing situations. Additionally, students' perceptions and responses to such risks are influenced by cultural norms, digital habits, and educational exposure, all of which are rarely thoroughly examined. Developing more useful and effective awareness tactics requires addressing these aspects. By performing an empirical investigation of phishing knowledge and detection skills among students at a Pakistani university and investigating how well this awareness translates into safe and protective online behaviour, this study seeks to close these gaps.

1.3 Research Questions

This study is guided by the following research questions:

Main Research Question

• 1: What is the level of phishing awareness among undergraduate students? Supporting Research Question

• 2: To what extent can students identify phishing attempts and indicators?

• 3: What is the relationship between awareness levels and protective behavioral practices?

1.4 Study Importance

There are significant theoretical, practical, and policy-level ramifications to this research. The Knowledge-Attitude-Behavior (KAB) framework is theoretically applied to phishing in a Pakistani university setting, filling a gap left by the majority of previous research that concentrated on populations in the West or East Asia. Additionally, it provides empirical evidence on the relationship between awareness and actual detecting abilities and behaviour, emphasising the widespread disconnect between secure practices and knowledge, especially among technical students. By highlighting particular flaws like bad password practices, a lack of use of anti-phishing technologies, and trouble spotting manipulated URLs or social engineering techniques, the report offers educators and universities useful insights. Instead of depending on general awareness initiatives, these findings allow institutions to create personalised training. Additionally, other Pakistani universities can modify the survey instrument to gauge the awareness of their own students. The study provides the Higher Education Commission (HEC) with useful information to further digital literacy initiatives at the policy level. It recommends incorporating social engineering detection and phishing knowledge into standardised computing curriculum. Overall, the study highlights the necessity of providing students with both practical security behaviours and technical knowledge in an increasingly digital world.

1.4 Hypotheses

• H1: Students with greater phishing awareness demonstrate stronger phishing detection ability.

• $H0_1$: Phishing awareness has no significant relationship with detection ability.

• H2: Higher awareness levels are positively associated with protective behavioral intentions.

• $H0_2$: Awareness level has no significant effect on protective behavioral practices.

2. Review of Related Literature

2.1 Conceptual Background

Phishing is a type of cybercrime where attackers pretend to be trusted sources, like banks, universities, or social media platforms, to trick people into sharing sensitive information such as passwords or financial details. Today, phishing is not limited to emails; it also happens through SMS (smishing), phone calls (vishing), QR codes (quishing), and social media platforms. On social media, attackers often create fake login pages, send prize offers, or impersonate someone you know to spread malicious links.

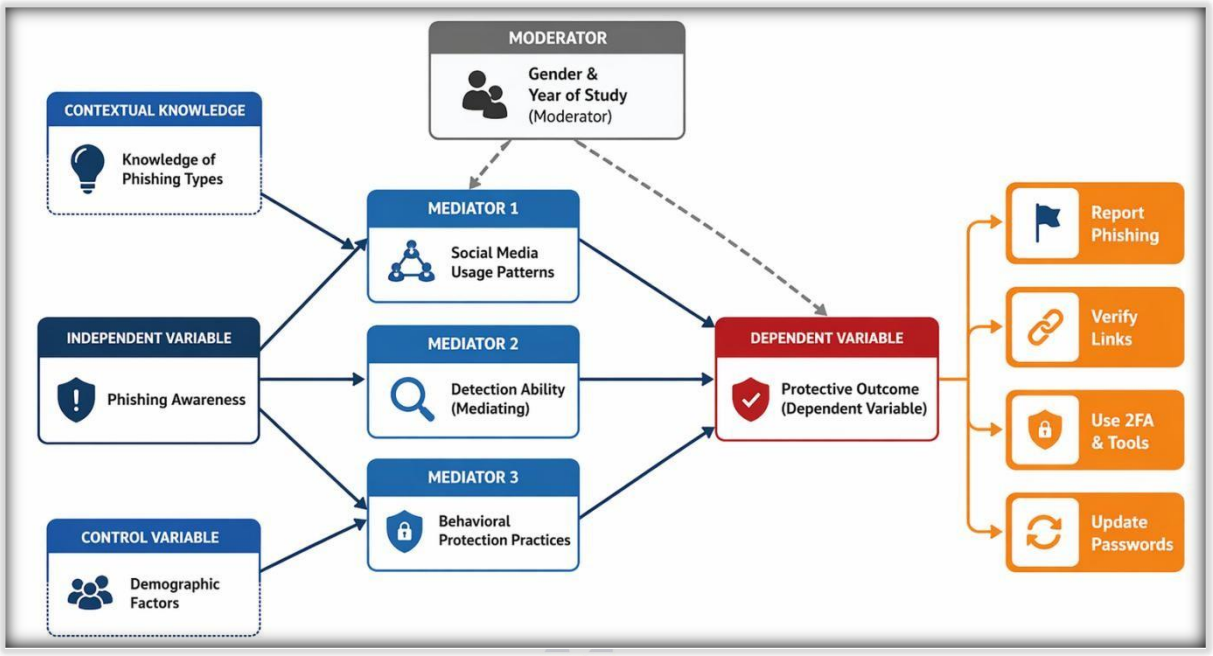
Phishing does not only depend on technical tricks, but also on human behavior. Attackers take advantage of how people think and react, such as creating urgency, using authority (like pretending to be a bank), or making people afraid of losing something. They also use techniques like fake website links or slightly changed URLs to make their attacks look real. Studies show that when users are given proper security awareness training, they become better at identifying phishing attempts. That is why this study looks at phishing not just from a technical side, but also from a human behavior perspective.

2.2 Conceptual Framework

This study adopts an awareness-behavior framework to examine the relationship between phishing knowledge, detection skill, and protective behavioral intention. This approach explicitly addresses how information security knowledge translates into practical protective actions, in contrast to theoretical adoption models created for various technical contexts. The main argument is that awareness is a necessary but insufficient prerequisite for behavioural protection; students must be able to use their knowledge of phishing in real-time situations and consistently adopt defensive behaviours. The Knowledge-Attitude-Behavior (KAB) construct, which is frequently employed in studies

on information security education, is compatible with this model.

Conceptual Framework — Phishing Awareness to Protective Behavior



Conceptual Framework Components — Phishing Awareness to Protective Behavior

Component	Definition	Measurement
Phishing Awareness	Knowledge of phishing types, techniques, and social media risks	5-item Likert scale (B-section)
Detection Ability	Ability to identify phishing indicators, fake pages, suspicious URLs	5-item Likert + 4 scenarios
Behavioral Practice	Actual protective behaviors: URL checking, 2FA use, link avoidance	5-item Likert (E-section)
Protective Outcome	Password updates, reporting, awareness program participation	Binary + categorical items

2.3 Review of Empirical Studies

The literature on phishing awareness covers technical, behavioral, and educational perspectives. The following studies highlight key findings relevant to this research area.

Alshamrani et al. (2018) conducted a comparative evaluation of multiple phishing detection tools and reported noticeable variation in their effectiveness. Their findings also revealed that although users possessed general awareness of phishing, many lacked familiarities with protective tools, indicating a gap between knowledge and practical application.

In a related study, Almousa et al. (2018) explored preventive strategies across email, websites, and social media environments. The authors emphasized that user education remains the most practical and cost-effective defense,

particularly in developing regions where technical solutions alone are insufficient.

Salahdine and Kaabouch (2019) provided a comprehensive overview of social engineering attacks on social media. Their work highlighted how attackers exploit psychological triggers such as urgency and trust, making users more vulnerable in socially interactive environments.

Focusing on the academic sector, Al-Hamar et al. (2023) examined cybersecurity awareness among university students and staff. Their results indicated moderate overall awareness but limited specific knowledge of phishing, while also demonstrating that formal training significantly improves detection ability.

Siddiqui et al. (2024) investigated the role of social media in shaping cybersecurity awareness. The study suggested that exposure to security-related content can improve understanding, but it does not always lead to consistent safe behavior, reflecting a disconnect between learning and practice.

Similarly, Rahman et al. (2023) reviewed security awareness trends among social media users and noted that younger individuals, despite being highly active online, often engage in riskier behaviours. This finding challenges the assumption that digital familiarity ensures security awareness.

Chaudhry et al. (2025) introduced a forensic approach to analyzing phishing attacks on mobile and social platforms. Their work demonstrated the increasing sophistication of attacks, particularly those involving manipulated URLs and messaging applications.

Ahmad et al. (2023) focused on phishing tools designed for social media platforms and found that such tools are widely accessible and easy to use. This accessibility significantly increases the risk for students, as attackers require minimal technical expertise.

Khatri et al. (2025) used simulated phishing experiments to assess student vulnerability. The results showed that many participants failed to detect phishing attempts despite reporting confidence in their abilities, highlighting a clear gap between perceived and actual performance.

Hassan et al. (2025) examined the relationship between awareness and the use of antiphishing tools. Their findings indicated that awareness alone does not ensure protection unless it is supported by active use of security measures.

Aziz et al. (2025) explored the integration of artificial intelligence in phishing detection alongside user awareness. While AI tools showed promise, the study pointed out issues such as false positives and lack of user trust, which limit their practical effectiveness.

Finally, Nwosu et al. (2024) proposed a Knowledge-Attitude-Behavior model to improve phishing awareness. Their findings confirmed that structured educational interventions can positively influence both awareness and behavior, supporting the need for training-based approaches.

Summary of Selected Empirical Studies on Phishing Awareness and Detection

Author (Year)	Study Focus	Method	Key Findings	Relevance to Current Study
Alshamrani et al. (2018)	Phishing detection tools	Comparative analysis	Tools differ in effectiveness; users lack practical knowledge	Shows awareness vs. practice gap
Almousa et al. (2018)	Phishing prevention	Review study	User education is most effective defense	Supports awareness importance

Salahdine & Kaabouch (2019)	Social engineering attacks	Survey/review	Psychological manipulation increases success of attacks	Explains human vulnerability
Al-Hamar et al. (2023)	Student awareness	Empirical study	Moderate awareness; training improves detection	Supports role of training
Siddiqui et al. (2024)	Social media & cybersecurity	Empirical study	Awareness does not always lead to safe behavior	Matches awarenessbehavior gap
Rahman et al. (2023)	Social media security awareness	Review study	Young users engage in risky behavior despite awareness	Supports behavioral risk findings
Chaudhry et al. (2025)	Phishing forensics	Analytical study	Attacks are becoming more sophisticated	Highlights evolving threat landscape
Ahmad et al. (2023)	Phishing tools on social media	Comparative study	Tools are easily accessible to attackers	Increases risk for students
Khatri et al. (2025)	Student phishing vulnerability	Experimental study	Students fail despite high confidence	Shows detection gap
Hassan et al. (2025)	Awareness & tool usage	Empirical study	Awareness alone is not sufficient for protection	Supports research problem
Aziz et al. (2025)	AI in phishing detection	Empirical study	AI helps but has trust and accuracy issues	Shows limits of technical solutions
Nwosu et al. (2024)	KAB model application	Model-based study	Training improves awareness and behavior	Supports theoretical framework
Verizon (2024)	Data breach analysis	Industry report	68% breaches involve human error	Justifies focus on human factors
Alqahtani et al. (2025)	Student behavior & phishing	Empirical study	Behavior strongly affects vulnerability	Supports behavior variable
Khatri et al. (2023)	Phishing awareness in students	Survey study	Awareness exists but practice is weak	Reinforces awarenessbehavior gap

3. Research Methodology

3.1 Research Design

This study used a quantitative survey design to understand phishing awareness, detection ability, and protective behavior among university students. A quantitative approach was chosen because the study focuses on collecting numerical data and analyzing students' responses in a simple and clear way.

The data were collected at one point in time, so the study follows a cross-sectional design. This was suitable because the aim was to observe the current level of awareness and behavior rather than changes over time.

The study mainly focuses on three variables. The first is phishing awareness, which shows how much students know about phishing attacks. The second is detection ability, which refers to how well students can identify phishing attempts. The third is behavioral practices, which includes the actions students take to protect themselves online, such as checking links or using security features. The study also looks at how these variables are connected with each other.

3.2 Population and Sampling

The target population of this study includes university students in Pakistan, especially those studying Computer Science and IT, as they are more active online and more relevant to the topic. A convenience sampling method was used to collect data. The questionnaire was shared through WhatsApp groups, university contacts, and friends to reach students easily. Only those students who were currently enrolled in a university and agreed to participate were included in the study. Incomplete responses were removed before analysis.

Demographic Profile of Respondents (N = 46)

Characteristic	Category	Frequency (n)	Percentage (%)
Age	16–18 years	3	6.5%
	19–21 years	15	32.6%
	22–23 years	22	47.8%
	24 or above	6	13.1%
Gender	Male	39	84.8%
	Female	7	15.2%
Education	Undergraduate	40	87.0%
	Graduate	6	13.0%
Field of Study	Computer Science / IT	38	82.6%
	Other Fields	8	17.4%
Social Media Hours	Less than 2 hours	4	8.7%
	2–4 hours	16	34.8%
	More than 4 hours	26	56.5%

3.3 Data Collection Instruments

A structured online questionnaire was used to collect data for this study, divided into seven sections. Section A collected basic demographic information such as age, gender, education level, field of study, and daily social media usage. Section B measured phishing awareness through five items asking respondents how familiar they are with phishing attacks, whether they know phishing happens on social media, and whether they can recognize suspicious links and risky online behaviours. Section C collected information about prior phishing experience, including whether respondents had previously heard of phishing, clicked a suspicious link, or been a victim of an attack. Section D assessed detection ability through five items measuring how well respondents can identify fake login pages, suspicious URLs, phishing messages, and impersonator profiles. Section E measured behavioral protection practices through five items covering actions like checking links before clicking, using twofactor authentication, and verifying sender identity. Section F

presented four real-world phishing scenarios and asked respondents to choose what they would do in each situation. All Likert-scale items used a five-point response scale ranging from one, which means Strongly Disagree, to five, which means Strongly Agree.

3.4 Data Collection Procedure

The survey was delivered online through Google Forms, which allowed respondents to submit their answers anonymously and securely. The survey link was shared over a period of five days through academic WhatsApp groups, university networks, and personal peer referral. Before starting the survey, respondents were shown a brief introduction explaining the academic purpose of the study, confirming that participation was completely voluntary, and assuring them that their responses would remain confidential. Respondents were required to confirm their informed consent before proceeding to the survey questions. All responses were automatically saved in Google Forms and later exported to Microsoft Excel for data cleaning and preparation before analysis.

3.5 Data Analysis Technique

Descriptive statistics were used to analyze all collected data, including frequencies, percentages, and mean scores for every demographic variable and Likert-scale item. To summarize each main construct, a composite mean score was calculated by averaging the scores of the items belonging to that construct. Mean scores were interpreted using four benchmarks: scores between 1.00 and 2.49 were classified as Low, scores between 2.50 and 3.49 as Moderate, scores between 3.50 and 4.49 as High, and scores between 4.50 and 5.00 as Very High. Scenario-based responses were analyzed using simple frequency distributions showing the percentage of correct and incorrect answers for each scenario. All analysis was carried out using Microsoft Excel and SPSS, with findings presented in tabular, graphical, and narrative form for each section of the questionnaire.

3.6 Study Limitations

This study has several limitations that should be kept in mind when interpreting the findings. First, the sample size of 46 respondents is relatively small, which limits the statistical strength of the results and reduces how broadly the findings can be applied to other populations. Second, a non-probability convenience sampling method was used, meaning the sample was not randomly selected and may not fully represent all Pakistani university students. Third, the cross-sectional design captured responses at only one point in time, so it is not possible to know whether awareness or behavior levels change over time. Fourth, all responses are self-reported, which means some respondents may have given answers that reflect how they want to be seen rather than how they actually behave online. Fifth, the survey was distributed mainly through digital channels, which may have attracted respondents who were already more digitally aware than the average student, potentially making the awareness scores appear slightly higher than they would be across the full student population.

4. Data Analysis and Results

This section presents a comprehensive analysis of data collected from 46 student respondents. Each sub-section provides tabular, graphical, and narrative interpretation for the key constructs: phishing awareness, detection ability, behavioral practices, and scenario-based responses.

4.1 Demographic Profile of Respondents

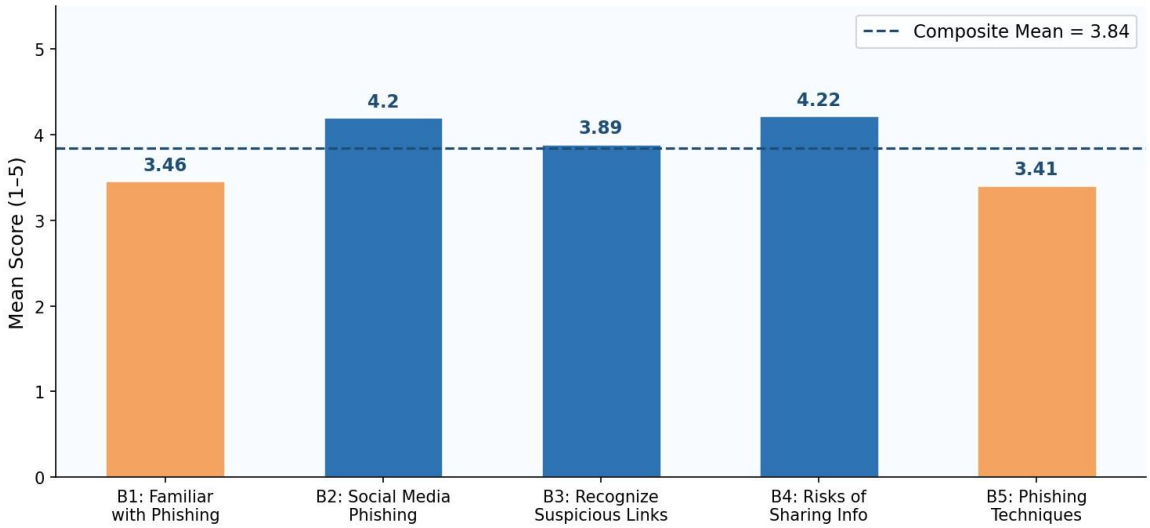
The sample is predominantly male (84.8%), consistent with gender distribution patterns in Pakistani STEM programs. The largest age cohort is 22–23 years (47.8%), reflecting the typical undergraduate demographic. The majority (82.6%) are pursuing Computer Science or IT degrees, ensuring baseline digital literacy. Notably, 56.5% of respondents spend more than four hours daily on social media, indicating high digital exposure and corresponding risk surface area.

4.2 Section B: Phishing Awareness

Phishing Awareness — Item-Level Descriptive Statistics (N = 46)

Item	Statement	Mean	Interpretation
B1	I am familiar with phishing attacks	3.46	Moderate
B2	I know phishing can happen on social media	4.20	High
B3	I can recognize suspicious links	3.89	High
B4	I understand risks of sharing personal info online	4.22	High
B5	I am aware of phishing techniques	3.41	Moderate
	Composite Awareness Mean	3.84	High

Phishing Awareness — Item-Level Mean Scores (N = 46)



The sample falls into the High awareness group with a composite awareness mean of 3.84. B4 (M = 4.22) and B2 (M = 4.20) received the highest ratings, demonstrating a thorough understanding of the dangers of disclosing personal information and social media phishing. These findings imply that, most likely as a result of unintentional internet exposure, kids have internalised broad, conceptual risk messages. However, B1 (M = 3.46) and B5 (M = 3.41) only achieved modest ratings, indicating that specific technique knowledge and deeper familiarity with phishing as a technical attack category are still lacking. According to more general research (Alshamrani et al., 2018; Hassan et al., 2025), informal digital literacy typically results in surface-level awareness without corresponding technical expertise. This pattern—high awareness of effects but modest knowledge of mechanisms—is consistent with this. Although 71.7% of respondents said they had heard about phishing before the survey, this does not always convert into high familiarity scores, demonstrating that prior exposure by itself does not ensure depth of knowledge.

Demographic Profile of Respondents (N = 46)

Characteristic	Category	Frequency (n)	Percentage (%)
Age	16–18 years	3	6.5%
	19–21 years	15	32.6%
	22–23 years	22	47.8%
	24 or above	6	13.1%
Gender	Male	39	84.8%
	Female	7	15.2%
Education	Undergraduate	40	87.0%
	Graduate	6	13.0%
Field of Study	Computer Science / IT	38	82.6%
	Other Fields	8	17.4%
Social Media Hours	Less than 2 hours	4	8.7%
	2–4 hours	16	34.8%
	More than 4 hours	26	56.5%

3.3 Data Collection Instruments

A structured online questionnaire was used to collect data for this study, divided into seven sections. Section A collected basic demographic information such as age, gender, education level, field of study, and daily social media usage. Section B measured phishing awareness through five items asking respondents how familiar they are with phishing attacks, whether they know phishing happens on social media, and whether they can recognize suspicious links and risky online behaviours. Section C collected information about prior phishing experience, including whether respondents had previously heard of phishing, clicked a suspicious link, or been a victim of an attack. Section D assessed detection ability through five items measuring how well respondents can identify fake login pages, suspicious URLs, phishing messages, and impersonator profiles. Section E measured behavioral protection practices through five items covering actions like checking links before clicking, using twofactor authentication, and verifying sender identity. Section F

presented four real-world phishing scenarios and asked respondents to choose what they would do in each situation. All Likert-scale items used a five-point response scale ranging from one, which means Strongly Disagree, to five, which means Strongly Agree.

3.4 Data Collection Procedure

The survey was delivered online through Google Forms, which allowed respondents to submit their answers anonymously and securely. The survey link was shared over a period of five days through academic WhatsApp groups, university networks, and personal peer referral. Before starting the survey, respondents were shown a brief introduction explaining the academic purpose of the study, confirming that participation was completely voluntary, and assuring them that their responses would remain confidential. Respondents were required to confirm their informed consent before proceeding to the survey questions. All responses were automatically saved in Google Forms and later exported to Microsoft Excel for data cleaning and preparation before analysis.

3.5 Data Analysis Technique

Descriptive statistics were used to analyze all collected data, including frequencies, percentages, and mean scores for every demographic variable and Likert-scale item. To summarize each main construct, a composite mean score was calculated by averaging the scores of the items belonging to that construct. Mean scores were interpreted using four benchmarks: scores between 1.00 and 2.49 were classified as Low, scores between 2.50 and 3.49 as Moderate, scores between 3.50 and 4.49 as High, and scores between 4.50 and 5.00 as Very High. Scenario-based responses were analyzed using simple frequency distributions showing the percentage of correct and incorrect answers for each scenario. All analysis was carried out using Microsoft Excel and SPSS, with findings presented in tabular, graphical, and narrative form for each section of the questionnaire.

3.6 Study Limitations

This study has several limitations that should be kept in mind when interpreting the findings. First, the sample size of 46 respondents is relatively small, which limits the statistical strength of the results and reduces how broadly the findings can be applied to other populations. Second, a non-probability convenience sampling method was used, meaning the sample was not randomly selected and may not fully represent all Pakistani university students. Third, the cross-sectional design captured responses at only one point in time, so it is not possible to know whether awareness or behavior levels change over time. Fourth, all responses are self-reported, which means some respondents may have given answers that reflect how they want to be seen rather than how they actually behave online. Fifth, the survey was distributed mainly through digital channels, which may have attracted respondents who were already more digitally aware than the average student, potentially making the awareness scores appear slightly higher than they would be across the full student population.

4. Data Analysis and Results

This section presents a comprehensive analysis of data collected from 46 student respondents. Each sub-section provides tabular, graphical, and narrative interpretation for the key constructs: phishing awareness, detection ability, behavioral practices, and scenario-based responses.

4.1 Demographic Profile of Respondents

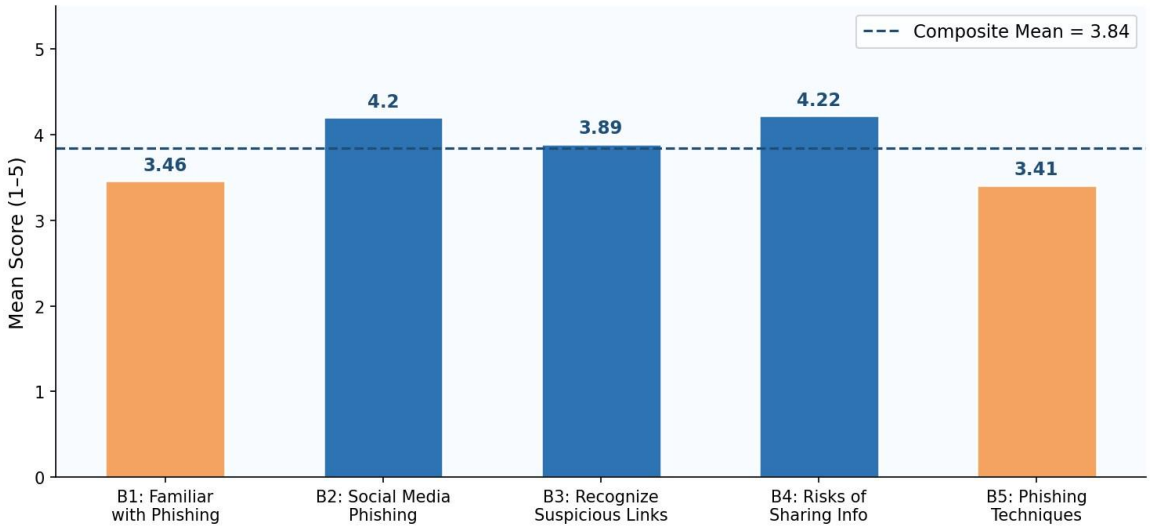
The sample is predominantly male (84.8%), consistent with gender distribution patterns in Pakistani STEM programs. The largest age cohort is 22–23 years (47.8%), reflecting the typical undergraduate demographic. The majority (82.6%) are pursuing Computer Science or IT degrees, ensuring baseline digital literacy. Notably, 56.5% of respondents spend more than four hours daily on social media, indicating high digital exposure and corresponding risk surface area.

4.2 Section B: Phishing Awareness

Phishing Awareness — Item-Level Descriptive Statistics (N = 46)

Item	Statement	Mean	Interpretation
B1	I am familiar with phishing attacks	3.46	Moderate
B2	I know phishing can happen on social media	4.20	High
B3	I can recognize suspicious links	3.89	High
B4	I understand risks of sharing personal info online	4.22	High
B5	I am aware of phishing techniques	3.41	Moderate
	Composite Awareness Mean	3.84	High

Phishing Awareness — Item-Level Mean Scores (N = 46)



The sample falls into the High awareness group with a composite awareness mean of 3.84. B4 (M = 4.22) and B2 (M = 4.20) received the highest ratings, demonstrating a thorough understanding of the dangers of disclosing personal information and social media phishing. These findings imply that, most likely as a result of unintentional internet exposure, kids have internalised broad, conceptual risk messages. However, B1 (M = 3.46) and B5 (M = 3.41) only achieved modest ratings, indicating that specific technique knowledge and deeper familiarity with phishing as a technical attack category are still lacking. According to more general research (Alshamrani et al., 2018; Hassan et al., 2025), informal digital literacy typically results in surface-level awareness without corresponding technical expertise. This pattern—high awareness of effects but modest knowledge of mechanisms—is consistent with this. Although 71.7% of respondents said they had heard about phishing before the survey, this does not always convert into high familiarity scores, demonstrating that prior exposure by itself does not ensure depth of knowledge.

6. Conclusion

The main objective of this study was to examine the level of phishing awareness and detection ability among university students in Pakistan, and to explore whether awareness of phishing threats actually leads to protective behavior in daily online activity. Data were collected from 46 student

respondents through a structured online questionnaire covering phishing awareness, detection ability, behavioral protection practices, and scenario-based decision making.

The results of this study confirm what the research questions anticipated — that a clear and consistent gap exists between what students know about phishing and how they actually behave online. Students demonstrated a high level of phishing awareness and reported strong confidence in their ability to detect phishing attempts, yet their behavioral protection practices fell in the moderate range. Many respondents had previously clicked on suspicious links, a significant portion had never received any formal phishing training, and more than half did not update their passwords regularly. These findings together show that knowledge of a threat does not automatically produce the habit of defending against it.

The scenario-based section of the study further strengthened this conclusion by showing that socially-framed attacks and URL manipulation techniques still successfully deceived a portion of respondents, even among students studying in technology-related programs. This confirms that awareness at a general level is not enough — students need specific, practical training that prepares them for the kinds of phishing attacks that are most common on social media platforms today.

This study makes several contributions. It provides baseline empirical data on phishing awareness and behavior from a Pakistani university context that was previously missing from the literature. It also offers a reusable survey instrument that other institutions can adapt to measure similar constructs among their own students. Most importantly, it gives universities, educators, and policymakers a clear and evidence-based picture of where the gaps are, so that training programs and institutional policies can be designed to address the specific weaknesses that actually exist rather than the ones that are simply assumed. Preparing the next generation of computing professionals to not just understand cybersecurity threats but to consistently act against them is both an academic responsibility and a matter of broader national importance.

7. Recommendations

Based on the findings of this study, several recommendations are offered for universities, educators, and policymakers. Air University Multan Campus and similar institutions should make phishing awareness training a required part of computing degree programs rather than leaving it as optional, with a specific focus on scenario-based exercises that cover social media attacks, URL inspection, and fake login page recognition, since these were the areas where students performed weakest. Faculty members should go beyond theoretical instruction and include hands-on demonstrations of anti-phishing tools in their courses, as tool adoption rates among respondents were notably low despite high self-reported awareness. The Higher Education Commission of Pakistan should consider making digital literacy and phishing awareness standardized learning outcomes across all undergraduate computing programs so that every student receives proper training regardless of which institution they attend. Finally, future researchers should replicate this study with larger and more geographically diverse samples, and explore experimental or longitudinal designs that can measure whether awareness interventions actually produce lasting changes in student behavior over time.

References

Ahmad, S., et al. (2023). Comparative analysis of phishing tools on social media sites. ResearchGate, Publication 372765611.

Al-Hamar, Y., et al. (2023). Analysis of social engineering awareness among students and lecturers. IEEE Access, 11. https://doi.org/10.1109/Access.2023.10238721

Almousa, M., et al. (2018). Preventive techniques of phishing attacks in networks.

Alqahtani, S., et al. (2025). Strengthening cybersecurity: The influence of student behavior on phishing attack perception. Lecture Notes in Computer Science, Springer.

Alshamrani, M., et al. (2018). A comparative analysis and awareness survey of phishing detection tools. Proceedings of the IEEE International Conference on

Computing, Electronics and Communications Engineering. https://doi.org/10.1109/iCCECE.2018.8256835

Aziz, R., et al. (2025). AI-based phishing detection and student cybersecurity awareness. Journal of Cybersecurity Education.

Aziz, R., et al. (2025). AI-based phishing detection and student cybersecurity awareness. Big Data and Cognitive Computing, 9(8), 210.

Chaudhry, N., et al. (2025). Phishing forensics: A systematic approach to analyzing mobile and social media fraud. ResearchGate, Publication 392241284.

Hassan, T., et al. (2025). Enhancing phishing resilience in academia: The mediating role of anti-phishing tools. IEEE Xplore. https://doi.org/10.1109/conf.2025.10871376

Khatri, S., et al. (2023). Phishing attack awareness among college students. IEEE Conference Proceedings.

Khatri, S., et al. (2025). Phishing attack awareness among college students. IEEE Xplore.

Nwosu, C., et al. (2024). Enhanced model for increasing vocational students' awareness against phishing. IEEE Xplore.

Proceedings of the IEEE International Conference on Intelligent Systems. https://doi.org/10.1109/ICIS.2018.8550081

Rahman, A., et al. (2023). A review on social media issues and security awareness among users. ResearchGate, Publication 400190484.

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. Future Internet, 11(4), 89. https://doi.org/10.3390/fi11040089

Siddiqui, R., et al. (2024). The role of social media in raising awareness of cybersecurity risks. ResearchGate, Publication 383369236.

Verizon. (2024). Data breach investigations report 2024. Verizon Communications Inc.

Appendix: Survey Questionnaire

Phishing Awareness and Detection Survey

Instructions: Please respond honestly to each question. Likert items are rated on a scale of 1 (Strongly Disagree) to 5 (Strongly Agree). Your responses are completely anonymous and confidential.

Section A: Demographics

A1. What is your age? [] 16–18 [] 19–21 [] 22–23 [] 24 or above

A2. Gender: [] Male [] Female [] Prefer not to say

A3. Education Level: [] Undergraduate [] Graduate [] Other

A4. Field of Study: [] Computer Science / IT [] Other

A5. Daily social media hours: [] Less than 2 hrs [] 2–4 hrs [] More than 4 hrs

A6. Platforms used: [] WhatsApp [] Facebook [] Instagram [] Twitter/X [] TikTok [] Other

Section B: Phishing Awareness (1 = Strongly Disagree → 5 = Strongly Agree)

Item	Statement	1	2	3	4	5
B1	I am familiar with phishing attacks					
B2	I know that phishing can happen on social media platforms					
B3	I can recognize suspicious links when I see them					
B4	I understand the risks of sharing personal information online					
B5	I am aware of different phishing techniques used by attackers					

Section C: Prior Experience

C1. Have you heard of phishing before this survey? [] Yes [] No

C2. Have you ever clicked on a suspicious link? [] Yes [] No

C3. Have you ever been a victim of a phishing attack? [] Yes [] No

C4. Do you think you can identify a phishing attempt? [] Yes [] Maybe [] No

C5. Which are phishing indicators? [] Unknown sender [] Urgent message [] Suspicious links [] Spelling mistakes [] Requests for personal info

Section D: Detection Ability (1 = Strongly Disagree → 5 = Strongly Agree)

Item	Statement	1	2	3	4	5
D1	I can identify fake login pages on social media platforms					
D2	I always check URLs carefully before clicking on them					
D3	I can detect phishing messages based on their content and style					

D4	I can identify fake or impersonator profiles on social media					
D5	I consistently avoid clicking on links from unknown sources					

Section E: Behavioral Protection Practices (1 = Strongly Disagree → 5 = Strongly Agree)

Item	Statement	1	2	3	4	5
E1	I click on links in messages without checking them first					
E2	I share my personal information (name, number, etc.) online freely					
E3	I accept friend requests from people I do not know					
E4	I always verify the identity of the sender before responding					
E5	I use security features such as two-factor authentication (2FA)					

Section F: Training and Attitudes

F1. Do you update your passwords regularly? [] Yes [] No

F2. Have you ever received phishing awareness training? [] Yes [] No

F3. Where did you learn about phishing? [] University [] Internet [] Social Media [] Friends [] Other

F4. Do you think phishing awareness programs are necessary? [] Yes [] No