Awareness and Preparedness Against AI-Driven Phishing Attacks: A Quantitative Study Among University Students

Dr. Ahmed Abdallah Abaker Sabiel
Applied College, Department of Computer Science, Imam Mohammad Ibn Saud Islamic University (IMSIU), Riyadh, Saudi Arabia
ORCID: https://orcid.org/0009-0000-0172-093X

ABSTRACT
Artificial intelligence has enabled a new generation of phishing attacks that are personalized, scalable, and harder to detect. This study explores university students' awareness and preparedness against AI-driven phishing techniques, such as deepfakes and synthetic emails. Based on survey data from 300 students, results reveal moderate awareness but insufficient readiness, particularly among lower-year students. Notably, formal cybersecurity training showed no significant impact on preparedness. The study emphasizes the need for practical, simulation-based interventions integrated into academic curricula. These findings offer critical insights for enhancing cybersecurity education and strengthening institutional defenses against evolving AI-powered social engineering threats in academic environments.
Keywords: Artificial intelligence, Phishing attacks, Awareness, Preparedness, Cybersecurity, Training, Workshop, University, Students

1. Introduction

Phishing is a form of cyberattack that employs fraudulent emails, text messages, phone calls, or websites to mislead individuals into divulging confidential information, installing malware, or exposing themselves to cybercrime [1], [2]. Phishing attacks have increased in both frequency and sophistication in recent years. AI-powered phishing attack techniques, including machine learning, deep learning, hybrid learning, and scenario-based methods, enable attackers to extract sensitive information through impersonated emails and imitation websites [3]. While classical phishing relied on generic emails and easily identifiable indicators, the use of AI has enabled the creation of highly personalized and context-aware attacks that can evade traditional detection mechanisms. Attackers increasingly employ AI-generated content to craft human-like phishing messages, while deepfake technologies are used for voice and video impersonation by exploiting psychological vulnerabilities [4].

Recent advances in artificial intelligence have substantially enhanced the effectiveness of phishing attacks [5]. Large language models are capable of generating convincing, grammatically correct phishing messages in real time while mimicking the tone and structure of legitimate communications [6]. These models can be trained on publicly available data from social media and professional platforms, enabling attackers to tailor communications toward specific individuals or organizations. Moreover, AI-driven automation allows phishing campaigns to be conducted at scale with minimal human effort, significantly increasing attack success rates and reducing the window for detection and response [7]. As a result, the use of artificial intelligence in cybercrime has become a critical challenge, underscoring the need for adaptive security systems, increased public awareness, and continuous improvement in threat detection and prevention tools.

This study examines the susceptibility of university students to AI-driven phishing attacks and evaluates their awareness and preparedness in addressing such threats. With phishing methods continuously evolving through AI and machine learning, cyber attackers are increasingly capable of designing highly realistic and targeted attacks against unsuspecting users. University students, as intensive users of digital platforms for academic and social purposes, often lack formal cybersecurity training, making them particularly vulnerable to such attacks [8], [9].

Accordingly, this research investigates the extent to which university students are vulnerable to AI-based phishing attacks, their level of awareness of these risks, and the effectiveness of existing preventive measures. It evaluates students' understanding of various phishing techniques, including email spoofing, imitation websites, and deepfake-based communications, as well as their ability to recognize and respond to such threats. By surveying students from multiple academic institutions, this study identifies knowledge gaps and behavioral patterns and highlights the importance of integrating AI-aware cybersecurity training into higher education curricula to enhance institutional and individual digital resilience.

1.1. Motivation

Two critical motivational drivers underpinning this research project are, first, the pressing need to learn about how AI-driven phishing methods are becoming more sophisticated in design and more capable of targeting susceptible populations, specifically university students, who often connect online academically, financially, and socially without proper cybersecurity training or protective measures. Since AI empowers attackers to create highly tailored, misleading content such as emails, spurious websites, and even voice or video deepfakes, students are the easiest targets because they have maximum exposure to the digital world and little training in spotting such attacks. Secondly, there is a compelling need for this research to examine the level of awareness, behavioral trends, and readiness among university students in spotting and countering AI-powered phishing attacks. Through exploring the knowledge gaps, capacity building, and institutional support, the research seeks to highlight the necessity of incorporating cybersecurity training and AI-centered threat awareness into higher education curricula in order to achieve digital resilience in institutions of learning.

1.2. Research Gap

Despite the increasing number of publications focused on phishing attacks and cybersecurity threats, much of the current research is still theoretical in approach, based largely on conceptual discourse, expert opinion, or technical examination of detection mechanisms. Although these works add insightful viewpoints, they fail to adequately replicate the true awareness and readiness of end-users, most especially university students, who are a high-risk group because of their heavy use of digital media. In addition, existing literature is short on empirical evidence regarding students' knowledge about AI-based phishing methods, such as the application of deepfakes, language models, and behavioral targeting. Previous research also stays within the spheres of organizational or workplace environments, with a gap in the research regarding how schools and their students stand in relation to more advanced cyberattacks.

To address this gap, the present study employs a primary, data-driven approach by surveying 300 students across three universities. Through this empirical investigation, the research aims to assess students' awareness levels, evaluate their preparedness to respond to AI-enabled phishing attempts, and identify potential areas for educational intervention. This evidence-based approach allows for the generation of actionable insights that go beyond theoretical assumptions, providing a more grounded and generalizable understanding of vulnerabilities within the academic environment.

1.3. Contributions

This research provides empirical evidence regarding the emerging threat of AI-powered phishing attacks, this time concentrating on university students, an overlooked yet susceptible segment. Unlike most previous research, which aims to focus more on technical reports or theoretical accounts, this article conducts a data-based research approach relying on a survey questionnaire given to 300 students in three institutions.

The main strength of this research is that it focuses on students' real-world awareness, experience, and readiness in handling AI-driven phishing attacks. It goes beyond theoretical evaluations by

capturing quantifiable measures of students' knowledge of various types of phishing, such as email spoofing, imposter websites, and deepfake-based communication.
Additionally, this research identifies certain knowledge gaps and behavioral patterns that can make students more vulnerable to cyberattacks. By pointing out the limited cybersecurity training currently offered in university environments, the results emphasize the necessity for organized, AI-conscious educational interventions.
The study offers a pragmatic basis for future research on enhancing cybersecurity consciousness among students. Its empirical focus adds to an enhanced understanding of user-side weaknesses and aids in the formulation of focused strategies to enhance digital security in educational settings.

1.4. Research Objectives

This research seeks to empirically examine the awareness, exposure, and readiness of university students towards AI-driven phishing attacks. It assesses how well students can identify and react to advanced phishing tactics like deep fakes, AI-created emails, and imitated websites that use AI to evade conventional detection mechanisms. Through the survey of 300 students from various institutions of higher learning, the study aims to identify key knowledge gaps, behavioral tendencies, and the demand for specific cybersecurity education in institutions of higher learning.
Moreover, this research investigates the wider implications of student vulnerabilities for institutional cybersecurity and suggests data-driven approaches to improve digital resilience through curriculum interventions. This study also seeks to add to the literature by providing empirical knowledge on end-user risk, an area that has traditionally been monopolized by theoretical or system-level discourse. The objective of this research, with their key focuses, is summarized in Table 1.

Table 1 Research Objectives and Key Focus Areas

Objective	Key Focus
Assess Student Exposure to AI-Phishing	Investigates how often and in what forms students encounter AI-enabled threats.
Evaluate Awareness and Preparedness Levels	Measures students' understanding of phishing techniques and their response behavior.
Identify Knowledge Gaps	Highlights deficiencies in cybersecurity education related to AI-driven threats.
Explore Institutional Implications	Examines how student vulnerabilities may affect broader academic cybersecurity.
Recommend Educational Interventions	Proposes strategies to integrate AI-aware cybersecurity training into curricula.
Provide Empirical Insights	Offers data-driven evidence to enrich the existing literature on phishing and AI.

2. Background

The rapid advancement of AI has significantly reshaped the landscape of cybersecurity, influencing both offensive and defensive strategies. Phishing, a cybercrime involving deceptive attempts to acquire sensitive information, has evolved drastically with the support of AI-based technologies. Tools such as ChatGPT or similar large language models can generate sophisticated, grammatically correct, and context-aware phishing messages, making it increasingly difficult for users to distinguish between legitimate and malicious content [10]. According to [11], the integration of AI into digital systems increases the risk of cyber threats such as phishing attacks, where AI-driven tools can imitate human behavior to deceive users more effectively. Attackers can exploit intelligent systems to analyze user data and craft personalized phishing messages, making them more

convincing than traditional scams. This highlights the growing need for ethical AI deployment and robust cybersecurity strategies.

Educational institutions are increasingly becoming prime targets for cybercriminals due to the valuable personal and institutional data they hold. Recent studies reveal that phishing in academic settings is becoming more socially engineered and personalized, utilizing AI tools to bypass spam filters and user suspicion [12]. Despite the existence of open-source phishing datasets such as PhishTank, users' ability to interpret and act on such data in real time remains limited [13]. These attacks remain an under-explored threat within university communities despite the increasing vulnerability of students to social engineering techniques.

Recent research continues to affirm that university students are particularly susceptible to phishing, especially in remote learning environments. Studies report limited practical skills among students despite general awareness [14], difficulties recognizing phishing messages in graphical assessments [15], and minimal influence of demographic variables on susceptibility [16]. Large-scale experiments further demonstrate that warnings alone do not significantly reduce engagement with phishing content [17], while regional studies emphasize the need for educational interventions [18]. Collectively, these findings indicate that technical defenses alone are insufficient and that comprehensive approaches—including training, behavioral assessment, and tailored awareness campaigns—are essential.

Current awareness programs often fail to keep pace with AI-enhanced phishing [19], and rule-based detection strategies remain inadequate against machine-generated messages [20]. Accordingly, this study quantitatively assesses awareness and preparedness among university students to inform targeted, student-focused cybersecurity interventions.

.

3. Methodology

3.1. Targeted Survey and Data Collection

This study utilized a targeted survey approach to gather data from university students across three universities, from the domains of Computer Science and Information Technology, and the universities were purposively selected because they offer comparable programs in this field. Stratified random sampling was employed, stratifying by year of study, gender, and sub-discipline, to ensure balanced representation across key demographics. A total of 300 students were selected to participate in the survey, which aimed to assess their awareness and preparedness regarding AI-driven phishing attacks. The survey was distributed through a combination of electronic methods, such as university-provided email lists and student portals, ensuring broad and efficient access to the targeted population.

The use of online platforms for survey distribution aligns with best practices in survey-based research and provides a cost-effective and time-efficient way to reach a large and diverse group of university students. According to previous studies, online surveys offer several advantages: speed and efficiency for global reach and rapid data collection, reduced costs through email and social media communication, and flexibility for collecting large amounts of anonymous data, mitigating social bias [21], [22] This method ensures that responses are collected from students across various academic backgrounds, making the sample reflective of the general university student demographic. For sampling, a stratified random sampling technique was employed to ensure representation across key student demographics, such as year of study, gender, and academic discipline. This approach enhances the reliability and external validity of the findings by accounting for potential differences in awareness and preparedness levels across various subgroups. The stratification ensures a balanced representation of students from different faculties, mitigating any bias that could arise from over-sampling a particular group.

The survey was designed to maintain participant anonymity, which is crucial for ensuring honest and unbiased responses. Previous research in the field of cybersecurity awareness has shown

that anonymity encourages participants to provide more candid answers, particularly when discussing sensitive topics such as their experiences with phishing [23]. Additionally, the four-week data collection period was chosen to maintain a balance between ensuring sufficient participation and reducing potential dropout rates. This timeframe aligns with best practices in survey research, allowing ample time for students to complete the survey while minimizing attrition.

3.2. Survey Structure

The survey instrument was carefully structured to address the research objectives and gather both quantitative and qualitative data. The survey featured a mix of Likert-scale questions, multiple-choice questions, and open-ended questions. The questionnaire was divided into six main sections (see Table 2) to capture a comprehensive understanding of student awareness and preparedness:

1. *Demographic Information*

This section gathered basic demographic information, including age, gender, year of study, and faculty. This data helped to assess any potential correlations between demographic factors and awareness or preparedness levels.

2. *Awareness of AI-Driven Phishing*

Respondents were asked to rate their familiarity with AI-driven phishing attacks, using a Likert scale (e.g., "I am aware of AI-based phishing techniques"). This section aimed to measure students' general knowledge about phishing and AI's role in facilitating these attacks.

3. *Preparedness for AI-Driven Phishing Attacks*

This section assessed students' preparedness in handling AI-driven phishing attacks. Likert-scale questions included items such as "I know how to verify the authenticity of an email" and "I regularly update my passwords." This section was designed to evaluate the effectiveness of students' self-protective behaviors.

4. *Experiences with Phishing Attacks*

Respondents were asked whether they had ever encountered a phishing attempt and to describe the nature of their experience. This section aimed to capture real-world exposure to phishing and to assess how students react when confronted with such attacks.

5. *Factors Influencing Preparedness*

This section explored various factors that might influence students' preparedness, including their level of digital literacy, past exposure to cybersecurity education, and personal behaviors. Open-ended questions allowed participants to share additional insights into the challenges they face in staying secure online.

Table 2: Survey Sections and Response Options

Section	Question	Response Options
Section 1: Demographic Information		
	1. Age	Under 18, 18-22, 23-26, 27+
	2. Gender	Male, Female, Prefer not to say
	3. Year of Study	1st Year, 2nd Year, 3rd Year, 4th Year, Postgraduate
	4. Faculty/Discipline	Engineering, Computer Science, Social Sciences, Business, Arts
Section 2: Awareness of AI-Driven Phishing Attacks	Please rate the following statements based on your awareness of phishing attacks. (1 = Strongly Disagree, 5 = Strongly Agree)	
	5. I am familiar with the term "phishing" and its risks.	1 = Strongly Disagree, 5 = Strongly Agree
	6. I am aware that AI can be used to create realistic phishing emails, websites, or even videos.	1 = Strongly Disagree, 5 = Strongly Agree
	7. I know the difference between traditional phishing attacks and AI-powered phishing attacks.	1 = Strongly Disagree, 5 = Strongly Agree
	8. I am aware of deepfake technology being used in phishing attacks (e.g., fake videos or voice recordings).	1 = Strongly Disagree, 5 = Strongly Agree
	9. I am familiar with the concept of personalized phishing attacks targeting individuals using their online data.	1 = Strongly Disagree, 5 = Strongly Agree
Section 3: Preparedness for AI-Driven Phishing Attacks	Please rate how confident you are in your ability to respond to phishing attempts. (1 = Not Confident, 5 = Very Confident)	
	10. I know how to verify the authenticity of an email or website.	1 = Not Confident, 5 = Very Confident
	11. I regularly update my passwords and use strong password practices.	1 = Not Confident, 5 = Very Confident
	12. I would be able to identify a phishing email or website if I encountered one.	1 = Not Confident, 5 = Very Confident
	13. I have taken steps to secure my online presence, such as enabling two-factor authentication.	1 = Not Confident, 5 = Very Confident

	14. If I received a suspicious email or message, I would report it to the appropriate authorities (e.g., IT support, university).	1 = Not Confident, 5 = Very Confident
Section 4: Experiences with Phishing Attacks	Please answer the following questions based on your personal experiences with phishing attacks.	
	15. Have you ever encountered a phishing attempt (email, website, social media, etc.)?	Yes, No
	16. If yes, what type of phishing attack did you encounter? (Check all that apply)	Phishing email, Fake website, Social media phishing, Voice-based phishing (e.g., phone call or voice messages
	17. How did you respond when you encountered a phishing attempt?	Ignored it, clicked on the link or opened the attachment, Reported it to IT support or the university
	18. Do you feel that you would recognize a phishing attempt if it were more sophisticated (e.g., AI-generated deepfakes, personalized emails)?	Yes, No, Not sure
Section 5: Factors Influencing Preparedness	Please answer the following questions based on your personal experiences and behaviors.	
	19. Have you received any cybersecurity training (e.g., in class, through university workshops, online courses)?	Yes, No
	20. How comfortable are you with using digital tools (email, websites, social media, etc.)?	Very uncomfortable, Uncomfortable, Neutral, Comfortable, Very comfortable
	21. How often do you take steps to secure your online accounts (e.g., updating passwords, using antivirus software, enabling 2FA)?	Never, Rarely, Occasionally, Often, Always
	22. What do you think is the most important step to take when responding to a phishing attempt?	Report it to IT support, delete the email or message, verify the authenticity before acting, ignore it, and move on.
Section 6: Open-Ended Questions		
	23. What challenges do you face when trying to identify and respond to phishing attacks?	[Open text field]
	24. In your opinion, what should universities do to improve students' awareness and preparedness against phishing attacks?	[Open text field]

4. Results

This section represents the analysis of collected data by 300 participants through a qualitative and quantitative survey. The results comprise descriptive and inferential statistics along with the qualitative and thematic assessment of open-ended questions.

4.1. Reliability Analysis

Reliability analysis was conducted to ensure internal consistency of the awareness and preparedness scale, and a Cronbach's alpha of 0.978 across 10 items confirmed excellent reliability, indicating that the items consistently measure the intended constructs. (see Table 3).

Table 3 Reliability Analysis of Scales

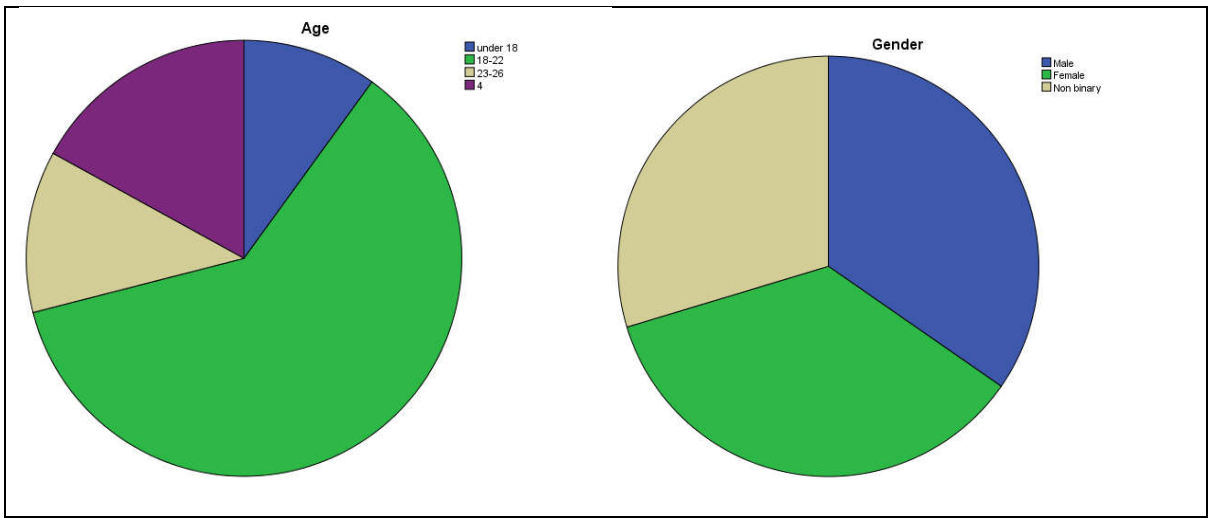
Reliability Statistics	
Cronbach's Alpha	N of Items
.978	10

4.2. Descriptive Statistics

Responses were collected from 300 university students and postgraduates. As shown in Table 4 and Figure 1, most participants were aged 18–26 (M = 2.36, SD = 0.879), with a balanced gender distribution (M = 1.95, SD = 0.802). The majority were from third year, fourth year, or postgraduate levels (M = 3.15, SD = 1.462), indicating a mature academic audience. Faculties such as Business, Arts, and Computer Science were well represented (M = 3.13, SD = 1.325). This diverse demographic distribution ensures the validity of findings and supports the investigation of awareness and preparedness levels across different academic backgrounds and stages, providing a strong foundation for assessing susceptibility to AI-driven phishing threats.

Table 4 Descriptive Statistics of Included Participants

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
Age	300	1	4	2.36	.879
Gender	300	1	3	1.95	.802
Year_of_Study	300	1	5	3.15	1.462
Faculty/Discipline	300	1	5	3.13	1.325
Valid N (listwise)	300				



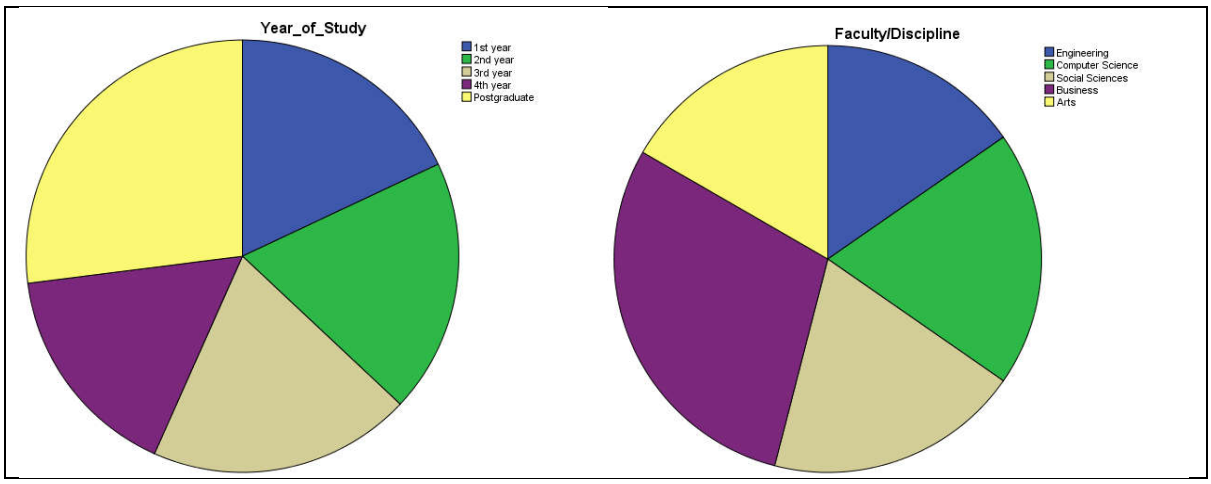


Figure 1 Descriptive Statistics of the Dataset

4.3. Other Tests

To evaluate the impact of cybersecurity training on students' awareness and preparedness regarding phishing threats, an independent samples t-test was performed across four key constructs. The analysis in Table 5 indicated no statistically significant differences between students who had received training and those who had not in terms of general phishing awareness ($t(298) = 0.717$, $p = .474$), awareness of AI-driven phishing techniques ($t(298) = 0.790$, $p = .430$), ability to identify phishing attempts ($t(298) = 0.552$, $p = .582$), and knowledge of authenticity verification procedures ($t(298) = 0.800$, $p = .424$). Effect size estimates were very small (Cohen's $d = 0.04–0.09$ across constructs), confirming that any differences between trained and untrained students were negligible. Additionally, Levene's test confirmed the assumption of homogeneity of variances in most cases. These results suggest that cybersecurity training, in its current form, may not sufficiently enhance students' practical awareness or preparedness, thereby underscoring the need for more targeted, application-oriented training interventions. The negligible effect sizes further indicate that the lack of statistical significance was not due to insufficient sample power, but rather reflects a genuinely minimal impact of training on these outcomes.

Table 5 Independent Sample T-test on cybersecurity training on students' awareness and preparedness regarding phishing threats.

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
Awareness_of_Phishing	Equal variances assumed	.092	.762	.717	298	.474	.076	.106	-.133	.286
	Equal variances not			.718	282.576	.473	.076	.106	-.133	.286

	assumed.									
Awareness_of_AI Phishing	Equal variances assumed	.204	.652	.790	298	.430	.085	.108	-.127	.298
	Equal variances not assumed.			.791	282.718	.429	.085	.108	-.127	.298
Ability_to_Identify_Phishing	Equal variances assumed	8.899	.003	.552	298	.582	.060	.108	-.153	.272
	Equal variances not assumed.			.542	258.446	.589	.060	.110	-.157	.276
Knowledge_of_Authenticity_Verification	Equal variances assumed	12.410	.000	.800	298	.424	.087	.108	-.126	.300
	Equal variances not assumed.			.779	247.561	.437	.087	.111	-.132	.305

To test the hypothesis that awareness and preparedness against phishing threats increase with year of study, a one-way ANOVA was conducted across four core dimensions. The results in Table 7 revealed statistically significant differences across year levels for all variables: general phishing awareness ($F(4, 295) = 150.84$, $p < .001$), awareness of AI-driven phishing ($F(4, 295) = 138.03$, $p < .001$), ability to identify phishing attempts ($F(4, 295) = 145.19$, $p < .001$), and knowledge of authenticity verification ($F(4, 295) = 132.76$, $p < .001$). Effect sizes were large, with η^2 values ranging from .64 to .67, indicating that year of study explained a substantial proportion of the variance in awareness and preparedness. These findings indicate a strong association between academic progression and increased awareness and preparedness. Students in higher academic years demonstrated significantly greater competence in recognizing and responding to phishing threats, supporting the proposed hypothesis.

Table 6 ANOVA Analysis

ANOVA						
		Sum of Squares	df	Mean Square	F	Sig.
Awareness_of_Phishing	Between Groups	167.768	4	41.942	150.836	.000

	Within Groups	82.029	295	.278		
	Total	249.797	299			
Awareness_of_AI Phishing	Between Groups	168.407	4	42.102	138.032	.000
	Within Groups	89.980	295	.305		
	Total	258.387	299			
Ability_to_Identify_Phishing	Between Groups	170.209	4	42.552	145.192	.000
	Within Groups	86.457	295	.293		
	Total	256.667	299			
Knowledge_of_Authenticity_Verification	Between Groups	166.289	4	41.572	132.758	.000
	Within Groups	92.377	295	.313		
	Total	258.667	299			

To test the hypothesis that response behavior to phishing attacks varies by gender, a Chi-Square test of independence was performed. The crosstabulation in Table 7 showed differences in how male, female, and other participants responded to phishing attempts. Among males (n = 104), 34 ignored the attempt, 38 clicked the link, and 32 reported it. Female participants (n = 107) showed a comparable distribution (ignored: 37, clicked: 40, reported: 30), while other participants (n = 89) were more likely to ignore the phishing (n = 38) and less likely to report it (n = 26). The Chi-Square test revealed no statistically significant association between gender and response to phishing, $\chi^2(df = 4, N = 300) = 3.03$, $p > .05$. Thus, the data do not support a gender-based difference in phishing response behavior. However, effect sizes were negligible (Cramér's V = .10 and .09, respectively), supporting the conclusion that gender was not meaningfully related to phishing responses or encounters.

Table 7 Chi Square Analysis of response behavior to phishing attacks varies by gender.

Crosstab					
Count					
		Response_to_Phishing			Total
		Ignored it	Clicked link	Report it	
Gender	Male	34	38	32	104
	Female	37	40	30	107
	Prefer not to say	38	25	26	89
Total		109	103	88	300

To assess whether phishing attack encounters differ by gender, a Chi-Square test of independence was conducted (see Table 8). The results yielded a Chi-Square value of $\chi^2(2, N = 300) = 2.58$, with a p-value greater than 0.05. This suggests that there is no significant association between gender and the likelihood of having encountered a phishing attack. While other participants reported a slightly higher incidence rate compared to males and females, the differences were not statistically meaningful.

Table 8 Chi Square Analysis of phishing attack encounters by gender

Crosstab				
Count				
		Encountered_Phishing_Attack		Total
		Yes	No	
Gender	Male	46	58	104
	Female	49	58	107
	Prefer not to say	49	40	89
Total		144	156	300

To examine the hypothesis that higher awareness of phishing is positively correlated with preparedness to respond, a Pearson correlation analysis was conducted among four key variables (see Table 9). The results revealed a strong, statistically significant positive correlation between general awareness of phishing and knowledge of authenticity verification ($r = .675$, $p < .001$), as well as between awareness and the ability to identify phishing attempts ($r = .685$, $p < .001$). Additionally, the correlations were large in magnitude ($r = .68$ for awareness with identification, $r = .68$ for awareness with verification), underscoring the strong link between awareness and preparedness. These findings support the hypothesis, indicating that as awareness increases, so does an individual's preparedness to detect and verify phishing threats. However, the correlation between awareness and actual security practices (e.g., password changes, 2FA) was weak and not statistically significant ($r = .085$, $p = .143$), suggesting that awareness alone may not translate into secure behavioral action.

Table 9 Pearson correlation analysis

Correlations					
		Awareness_of_Phishing	Knowledge_of_Authenticity_Verification	Ability_to_Identify_Phishing	Security_Measures_Taken
Awareness_of_Phishing	Pearson Correlation	1	.675**	.685**	.085
	Sig. (2-tailed)		.000	.000	.143
	N	300	300	300	300
Knowledge_of_Authenticity_Verification	Pearson Correlation	.675**	1	.988**	.022
	Sig. (2-tailed)	.000		.000	.708
	N	300	300	300	300
Ability_to_Identify_Phishing	Pearson Correlation	.685**	.988**	1	.009
	Sig. (2-tailed)	.000	.000		.871
	N	300	300	300	300
Security_Measures_Taken	Pearson Correlation	.085	.022	.009	1
	Sig. (2-tailed)	.143	.708	.871	
	N	300	300	300	300
**. Correlation is significant at the 0.01 level (2-tailed).					

The regression model in Table 10 shows a strong positive relationship between the predictors and preparedness to respond to phishing attacks, with an R = .690. The R Square value of .476 indicates that about 47.6% of the variance in preparedness can be explained by the combined influence of year of study, cybersecurity training, digital comfort, and security practices. The adjusted R^2 of .469 confirms the model's stability and generalizability. The overall effect size for the model was large (Cohen's f^2 = .91), with Year of Study uniquely accounting for nearly half of the explained variance (semi-partial $r^2 \approx$ .47). Other predictors contributed negligibly. Overall, these results suggest that these variables are meaningful predictors of students' preparedness against phishing threats.

Table 10 Relations Analysis by Regression Model

Model Summary				
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.690[a]	.476	.469	.678
a. Predictors: (Constant), Comfort_with_Digital_Tools, Security_Measures_Taken, Year_of_Study, Received_Cybersecurity_Training				

The regression analysis predicting Knowledge of Authenticity Verification was statistically significant overall, F(4, 295) = [insert F-value], p < .001, with an R^2 of .476, indicating that 47.6% of the variance in verification knowledge was explained by the predictors. As shown in Table X, Year of Study emerged as the only significant predictor (B = .437, β = .687, t = 16.28, p < .001), highlighting the strong positive influence of academic progression on students' preparedness. In contrast, Received Cybersecurity Training (B = −.060, β = −.032, p = .449), Security Measures Taken (B = .001, β ≈ .001, p = .982), and Comfort with Digital Tools (B = .030, β = .027, p = .522) were not significant predictors. These results suggest that formal training and self-reported behaviors contribute little beyond the experiential learning gained through advancing academic years. Along with the large ANOVA effect sizes across awareness variables (η^2 range = .64–.67), these findings demonstrate that academic progression is the dominant factor shaping students' awareness and preparedness against phishing threats.

Coefficients[a]								
Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.	95.0% Confidence Interval for B	
		B	Std. Error	Beta			Lower Bound	Upper Bound
1	(Constant)	2.487	0.251		9.905	0	1.993	2.981
	Received_Cybersecurity_Training	-0.06	0.079	-0.032	-0.758	0.449	-0.216	0.096
	Year_of_Study	0.437	0.027	0.687	16.277	0	0.384	0.49
	Security_Measures_Taken	0.001	0.045	0.001	0.023	0.982	-0.088	0.09
	Comfort_with_Digital_Tools	0.03	0.047	0.027	0.641	0.522	-0.062	0.122
a. Dependent Variable: Knowledge_of_Authenticity_Verification								

4.4 Open-ended questions

4.4.1. Challenges in Identifying Phishing

In the survey, the participants were asked to describe the challenges they face in identifying and responding to phishing attacks. As shown in Figure 2, the most frequently cited issue was a lack of knowledge on identifying sophisticated attacks such as AI-generated content and deepfakes, reported by 80 respondents. This was followed closely by a lack of training in recognizing phishing techniques (n = 70) and difficulty distinguishing between legitimate and fake sources (n = 60). A notable portion also cited overconfidence in recognizing phishing attempts (n = 50), indicating a potential gap between perceived and actual ability. Lastly, uncertainty about how to report phishing incidents was reported by

40 participants. These insights emphasize the need for structured, practical education and reporting protocols.

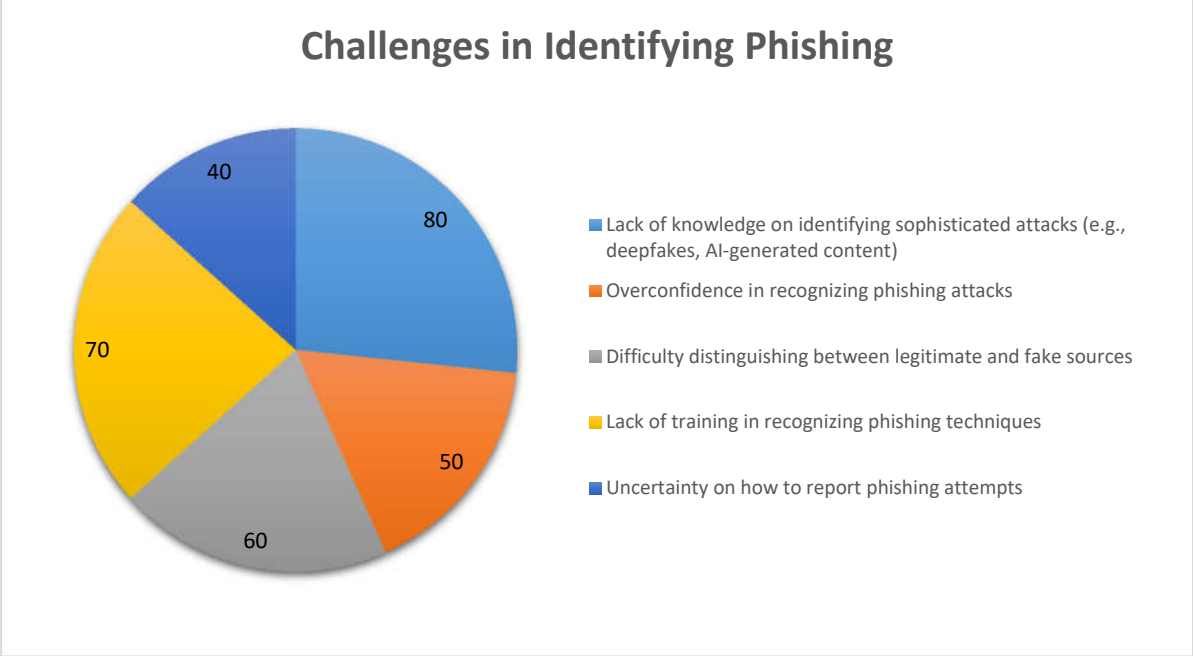


Figure 2 Analysis of Challenges in Identifying Phishing by Students

4.4.2. University Students' Suggestions

Participants were asked to propose ways universities could enhance student awareness and preparedness against phishing threats. As shown in Figure 3, the most frequently recommended measure was to organize mandatory cybersecurity workshops and training sessions (n = 100), underscoring the demand for structured learning opportunities. This was followed by calls to integrate phishing awareness into the curriculum (n = 80) and to provide regular updates and tips on identifying phishing attacks (n = 70). Fewer participants suggested implementing phishing simulation exercises (n = 30) and running awareness campaigns via email or digital platforms (n = 20). These responses collectively highlight a clear student preference for proactive, curriculum-integrated, and experiential learning strategies in cybersecurity education.

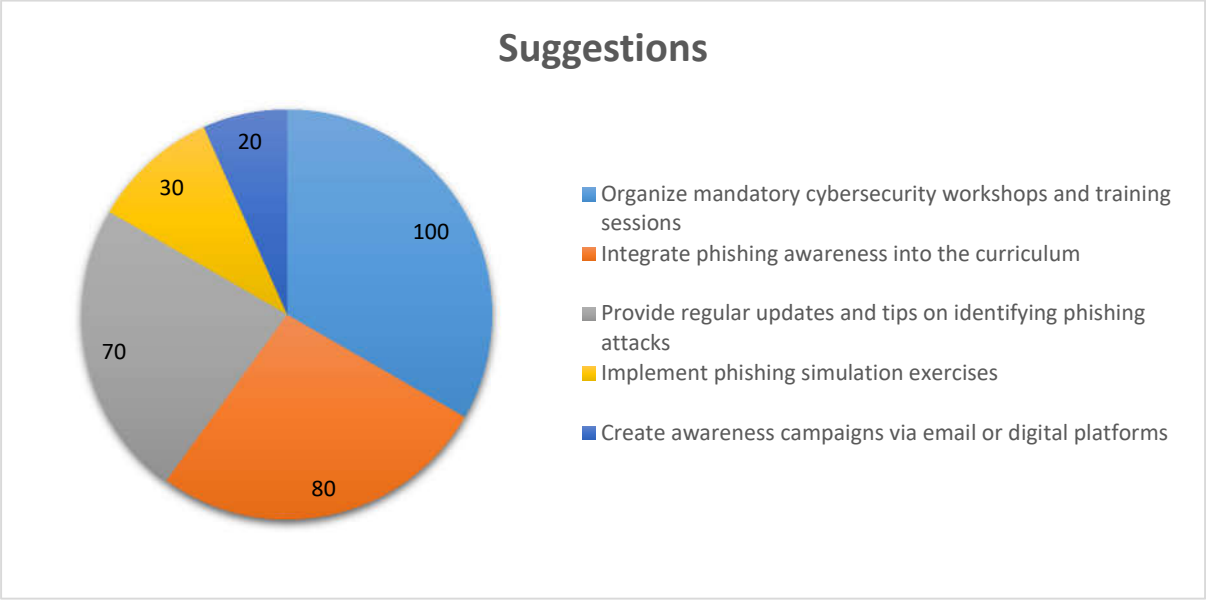


Figure 3 Analysis of Suggestions from Students for effective training and planning

5. Discussion

5.1. Analysis Summary

This study investigated how well university students understand and respond to AI-driven phishing attacks, based on responses from 300 participants. The results showed that while general awareness of phishing was fairly high, many students struggled with identifying advanced threats such as deepfakes and AI-generated emails. A strong positive correlation was found between phishing awareness and preparedness to respond ($r = .685$, $p < .001$), showing that students who are more aware are also more confident in dealing with phishing attempts. However, there was no significant difference in awareness or preparedness between students who had received cybersecurity training and those who had not ($p > .05$), suggesting that current training programs may not be effective enough. On the other hand, awareness and preparedness significantly increased with year of study ($p < .001$), with senior and postgraduate students scoring higher than first-year students.

However, this null finding is significant as it challenges the common assumption that formal training alone is sufficient to improve preparedness. A likely explanation is that many university training initiatives are delivered as isolated, lecture-style sessions that emphasize theoretical content while offering little opportunity for practice, which reduces their real-world applicability. In such cases, students may retain abstract knowledge of phishing but struggle to apply it when confronted with evolving, AI-driven threats. It is also plausible that students benefit more from cumulative digital experience gained as they progress through their academic programs than from these stand-alone training events, a pattern consistent with our regression results that identified year of study as the strongest predictor of preparedness. Taken together, the evidence suggests that training must be re-designed as an ongoing, interactive, and simulation-based process if it is to deliver measurable improvements in student resilience.

In open-ended responses, students identified major challenges such as a lack of practical training, overconfidence, and not knowing how to report phishing attempts. When asked how universities could help, most students recommended regular workshops, updated learning materials, and simulated phishing exercises. These findings highlight a clear need for universities to improve cybersecurity education by making it more hands-on, frequent, and aligned with real-world threats. The study also shows that increasing awareness alone is not enough; there must be stronger efforts to convert awareness into secure behavior. By implementing this analysis, educational institutions can better prepare their students and reduce digital risks across campus environments.

According to Hoxhunt's research, while AI-generated phishing emails currently represent a small fraction between 0.7% and 4.7% of total phishing attacks, the overall volume of phishing emails has been increasing. Furthermore, a study by SlashNext reported a staggering 1,265% increase in phishing attacks in 2023, attributing this surge to the rise of generative AI [24]. The analysis of the previously published studies showed that university students are among the most vulnerable groups to phishing attacks, particularly those who use AI. For instance, [14] found that students learning remotely were greatly vulnerable to phishing attacks, frequently confusing AI-generated messages and emails as genuine communication owing to their realism and time-sensitive nature. Their study indicated that even though students understood phishing as a principle, many of them did not possess the critical capabilities to detect or react to such attacks properly. These results align with the analysis of our study highlighting that although the general awareness among the students was high, there was a lack of practical preparedness in the verification techniques and required security measures. Similarly, according to (Broadhurst et al., 2020), first-year students were significantly more vulnerable to phishing attacks, highlighting the reliability of our results showing that awareness and preparedness increased with academic progression.

However, according to[27], traditional training programs and education are insufficient to prepare students for the rapidly evolving phishing attacks. The analysis of their study highlighted that current curricula often lack practical, interactive components necessary to build real-world resilience. This result aligns with the findings of our analysis, where participants recommended the inclusion of phishing training and hands-on workshops within university programs to enhance preparedness. According to this analysis, previous studies mostly focus on theoretical models or system-level solutions, with little real-world data on students' awareness and preparedness. Especially in the context of AI-driven phishing, there is a clear lack of recent empirical research on university students. This study addresses that gap by providing direct, data-based insights from students themselves.

5.1. Implications for Policy and Practice

The findings of this study highlighted important implications for universities and policymakers. The analysis highlighted an urgent need to include structured, simulation-based cybersecurity training in academic programs, making it a mandatory component that advances in complexity with each academic year. Such training should focus on real-life phishing scenarios, including AI-generated threats. Additionally, institutions should establish clear reporting channels and responsive feedback systems to support students in taking immediate action when encountering phishing attempts. By combining awareness, hands-on practice, and accessible support, universities can significantly reduce student vulnerability and strengthen the overall digital resilience of the academic environment.

5.2. Limitations

Several limitations were found in this study. Firstly, this study is limited to university students and may not reflect the awareness or preparedness levels of faculty or staff. Secondly, the sample was confined to a specific academic program, which may affect the generalizability of the results. Lastly, the study did not evaluate the long-term impact of cybersecurity training among the students. Therefore, to address these limitations, future research could explore cross-institutional comparisons and longitudinal outcomes effectively.

6. Conclusion

This study explored university students' awareness and preparedness against AI-driven phishing attacks. Based on responses from 300 participants, findings showed that while general awareness was moderate, many students lacked the practical skills to detect advanced threats like deepfakes and AI-generated emails. A strong correlation was found between awareness and preparedness, but no significant difference was found between trained and untrained students, highlighting gaps in current cybersecurity education. Open-ended responses revealed key challenges, including a lack of practical exposure and reporting knowledge. Senior students showed better preparedness than juniors, indicating improvement with academic progression. The study emphasizes the need for universities to integrate hands-on, simulation-based cybersecurity training into curricula to ensure students are not only informed but equipped to respond to evolving digital threats.

Acknowledgement

I would like to express my sincere gratitude to Imam Mohammad Ibn Saud Islamic University (IMSIU) for providing the necessary resources and support throughout the course of this study. I would also like to thank my colleagues and the university's faculty for their valuable feedback and assistance in refining the study. Special thanks go to the students who participated in the survey, whose contributions were essential to this research.

References

[1] A. Karim et al., "Phishing detection system through hybrid machine learning based on URL," IEEE Access, vol. 11, pp. 36805–36822, 2023.
DOI: https://doi.org/10.1109/ACCESS.2023.3267964

[2] M. Usman et al., "A survey on representation learning efforts in cybersecurity domain," ACM Computing Surveys, vol. 52, no. 6, 2019.
DOI: https://doi.org/10.1145/3363034

[3] M. Amidu, Phishing in the Era of AI: Evolution, Creation, Detection, and Countermeasures, Ashesi University, 2024.

[4] M. S. Liaqat et al., "Exploring phishing attacks in the AI age," Journal of Computing & Biomedical Informatics, vol. 7, no. 2, 2024.

[5] I. Naseer, "The role of artificial intelligence in detecting and preventing cyber and phishing attacks," European Journal of Advances in Engineering and Technology, vol. 11, no. 9, pp. 82–86, 2024.

[6] A. Siemerink et al., “The dual-edged sword of large language models in phishing,” in Proc. Nordic Conf. Secure IT Systems, 2024.
DOI: https://doi.org/10.1007/978-3-031-57543-3_9

[7] A. Kumar, “Next-generation approaches to detecting and preventing AI-generated phishing scams,” Eastern European Journal for Multidisciplinary Research, vol. 2, no. 1, pp. 83–99, 2023.

[8] R. Shillair et al., “Cybersecurity education, awareness raising, and training initiatives,” Computers & Security, vol. 119, p. 102756, 2022.
DOI: https://doi.org/10.1016/j.cose.2022.102756

[9] I. M. Taha et al., “The impact of students’ cybersecurity vulnerability behavior on e-learning obstacles,” Organizacija, vol. 58, no. 1, pp. 85–104, 2025.
DOI: https://doi.org/10.2478/orga-2025-0006

[10] M. Bethany et al., “Large language model lateral spear phishing,” arXiv preprint arXiv:2401.09727, 2024.
[11] J. F. Jimmy, “Emerging threats: The latest cybersecurity risks,” Valley International Journal Digital Library, vol. 1, pp. 564–574, 2021.

[12] E. Morrow, “Scamming higher ed: An analysis of phishing content and trends,” Computers in Human Behavior, vol. 158, p. 108274, 2024.
DOI: https://doi.org/10.1016/j.chb.2024.108274

[13] Siemerink, A., Jansen, S., & Labunets, K. (2024). The Dual-Edged Sword of Large Language Models in Phishing. Nordic Conference on Secure IT Systems,

[14] B. Nyasvisvo and J. M. Chigada, “Phishing attacks: A security challenge for university students studying remotely,” African Journal of Information Systems, vol. 15, no. 2, 2023.

[15] M. Andrić, M. Horvat, and M. Žagar,
“Phishing email detection using visual similarity and user perception: Evidence from a student population,” Information Security Journal: A Global Perspective, vol. 31, no. 5, pp. 257–270, 2022. DOI: https://doi.org/10.1080/19393555.2022.2036857
[16] R. E. Yoro et al., “Assessing contributor features to phishing susceptibility,” Int. J. Electr. Comput. Eng., vol. 13, no. 2, p. 1922, 2023.
DOI: https://doi.org/10.11591/ijece.v13i2.pp1922-1932

[17] J. G. Mohebzada et al., “Phishing in a university community,” in Proc. Int. Conf. Innovations in Information Technology (IIT), 2012.
DOI: https://doi.org/10.1109/IIT.2012.6404488

[18] B. Elnaim and H. Al-Lami, “The current state of phishing attacks against Saudi university students,” IJCATR, vol. 6, no. 1, pp. 42–50, 2017.
DOI: https://doi.org/10.7753/IJCATR0601.1007

[19] B. Baadel, A. Chehab, and M. Kayssi,“Cybersecurity awareness and training programs: Limitations and challenges in countering advanced phishing attacks,”2021.

[20] S. Heartfield, G. Loukas, and D. Gan,“You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks,”in Proc. IEEE Symposium on Security and Privacy (SP), 2016, pp. 312–328.DOI: https://doi.org/10.1109/SP.2016.23

[21] D. A. Dillman et al., Internet, Phone, Mail, and Mixed-Mode Surveys, 2014.
DOI: https://doi.org/10.1002/9781118925057

[22] R. Tourangeau and T. Yan, “Sensitive questions in surveys,” Psychological Bulletin, vol. 133, no. 5, pp. 859–883, 2007.
DOI: https://doi.org/10.1037/0033-2909.133.5.859

[23] M. J. Kayomb, “Phishing attack awareness amongst users at a university of technology in the Western Cape,” M.S. thesis, Cape Peninsula University of Technology, Cape Town, South Africa, 2024.

[24] M. Cartier,“AI phishing attacks: How big is the threat?,” Hoxhunt, Industry Report, 2025. [Online]. Available: https://hoxhunt.com/blog/ai-phishing-attacks

[25] R. Broadhurst et al., “Phishing risks in a university student community,” Trends & Issues in Crime and Criminal Justice, no. 587, 2020.

[26] I. M. Taha, R. H. Abd Ali, and A. A. Abbas, “The impact of students’ cybersecurity vulnerability behavior on e-learning obstacles,” Organizacija, vol. 58, no. 1, pp. 85–104, 2025. DOI: https://doi.org/10.2478/orga-2025-0006

[27] M. F. Ansari et al., “Prevention of phishing attacks using AI-based cybersecurity awareness training,” 2022.