Strengthening Cybersecurity: The Influence of Student Behavior, Perceived Factors, and Mitigating Strategies on Phishing Attack Perception

Saleh Alqahtani[1] ✉[0000-0001-9051-319X], Priyadarsi Nanda[2][0000-0002-5748-155X] and Manoranjan Mohanty[3] [0000-0002-0258-4586]

[1] *Saudi Electronic University, Saudi Arabia*

[1] *University of Technology Sydney, Australia,* sm.alqahtani@seu.edu.sa

[2] *Faculty of Engineering and IT*

University of Technology Sydney, Australia, priyadarsi.nanda@uts.edu.au

[3]*Carnegie Mellon University, Qatar,*

mmohanty@cmu.edu

Abstract. Phishing attacks are among the most prevalent cyber-attack methods, leading to financial breakdowns, damaged reputations, and identity theft. This study focuses on cybersecurity aspects, emphasizing phishing attacks targeting university students. It aims to examine the characteristics, methods, and impacts of phishing attacks on students and their knowledge and awareness of these threats. The study identifies key factors contributing to the occurrence of phishing attacks and their influence on students' perceptions. Data were collected from 715 university students using a quantitative research approach. Key findings reveal that lack of awareness and failure to verify communications' authenticity significantly increase Phishing's vulnerability. The regression analysis revealed that Student Behavior, Perceived Factors, and Mitigating Strategies collectively explain 47.0% of the variance in Student Perception ($R^2 = 0.470$), with all predictors showing significant positive relationships: Student Behavior ($B = 0.169$, $p < 0.001$), Perceived Factors ($B = 0.392$, $p < 0.001$), and Mitigating Strategies ($B = 0.266$, $p < 0.001$). The study highlights the importance of human behavior in executing mitigation strategies, concluding that relying solely on technology-based solutions is insufficient to address the challenges posed by phishing attacks. The study recommends comprehensive educational initiatives, emphasizing the importance of verifying personal information sources and regularly updating software and hardware as effective mitigation strategies.

Keywords: Cybersecurity, Phishing Attacks, Mitigating Strategies, Online Safety, Students' Awareness, Perceived Factors.

1 Introduction

Each year, a growing number of incidents and breaches specifically target the vulnerabilities in human aspects of cyber security. The data breach investigations report (DBIR) provided by Verizon reveals that 82% of the studied breaches were attributable

to human activities or errors [1]. One often used technique for taking advantage of the human aspects of cyber security is known as a phishing attack. Phishing is a type of cyber-attack where the attacker deceives the victim into performing actions that cause harm to both the victim and the system. Phishing is an illicit activity that exploits individuals by using social engineering tactics to manipulate them [2]. [3] define phishing attack as a fraudulent attempt to imitate a trustworthy entity to obtain sensitive information. The definitions clearly suggest that Phishing is an act of fraud and deception however, the reason behind the attack may vary. Typically, the objective is to get financial information and steal system credentials or other sensitive data. Moreover, Phishing is utilized as a method of attack to execute further activities, such as ransomware attacks. Lately, there has been a targeted increase in phishing attacks against organizations, leading to substantial financial losses. These losses are primarily due to the costs of containing malware, reduced productivity, the expenses associated with addressing compromised credentials, and the financial burden of dealing with ransomware resulting from phishing attempts. In addition, firms may also experience reputational harm in the perception of their consumers and competitors [1].

In 2022, Phishing was identified as one of the most harmful ways of attack, with an average expense of $4.91 million per data breach. Phishing can be carried out through several channels utilizing different techniques. Three commonly used channels for Phishing are the internet, short messaging services, and cell phones [4]. Different vectors are used to execute the attack in each of these mediums. Common phishing methods assisted by the internet include email, eFax, instant messaging, social networks, websites, and Wi-Fi. Smishing and Vishing are targeted attack techniques utilized in short message platforms and voice communication. In this scenario, students need to thoroughly understand the possible harm caused by phishing assaults, as they will soon be the workforce responsible for operating the system. This research aims to investigate the level of knowledge that university students have about the features, techniques, and repercussions of phishing assaults.

This paper adds on existing literature by concentrating on how different factors, such as awareness and behavior after interrelating with the different measures that students use helps to evade phishing attacks. This study unlike previous researches focuses on the gap which shows that how non-technical students of universities observe and take into account the threats related to phishing and thus it provides a more detailed and inclusive examination across different subjects. Moreover, the study aimed to identify the factors that contribute to the occurrence of phishing attacks and examine how these factors influence students' perceptions of different forms of phishing assaults. In light of the objectives of this study, the following research question was formulated:

RQ. How do student behavior, perceived factors, and mitigating strategies influence university students' perceptions of phishing attacks?

2 Literature Review

2.1 Types of Phishing Attacks

There are several techniques by which the attack might be carried out. The underlying motivation for all the categories is the same. The only difference between the different categories is related to the number of objectives and the methods used to obtain the information. Some commonly employed phishing attacks include deceptive Phishing, spear phishing, whaling attacks, email Phishing, social media phishing, and Fake QR code phishing. In deceptive Phishing, the attacker assumes the identity of a reputable organization or website to deceive the victim into providing sensitive information. This type of phishing attack involves duplicating the logo and design of a genuine email or website [5]. Deceptive phishing efforts may appear more convincing when they ask for personal information or confirmation of course registration [6]. In spear phishing, the perpetrator tailors the message initially. Spear phishing attempts are more intricate than traditional phishing attacks as the assailant conducts thorough research on the target and crafts a persuasive message. According to [7], spear phishing attacks can be successful because university students trust emails from professors, classmates, and administrators. Meanwhile, in whaling phishing, the phishers carry out whaling attacks by specifically targeting a senior executive, usually the CEO or someone of similar rank. Before launching an attack, the assailant would invest significant time in acquiring knowledge of the target. Subsequently, the assailant dispatches an email to the target to persuade the recipient to reveal confidential information [8].
On the other hand, in email phishing, attackers often assume the identity of reliable third parties to deceive their victims into divulging vital information. They could utilize captivating subject lines to create a sense of urgency, compelling you to take immediate action. Phishing via email is a prevalent and successful technique used by hackers to compromise the security of students [9]. Like email phishing, social media phishing is the construction of fake profiles or pages on social media platforms to deceive people [10]. Perpetrators may transmit harmful websites or private messages to deceive individuals into disclosing their personal data or login credentials. Additionally, phishing attacks that involve fake or altered QR codes are a common strategy used to trick and take advantage of individuals, particularly university students. QR Codes are the storage of different types of data, including different contact details, URLs of websites and instructions regarding payments. It uses 2D barcode technology, scanned using any device such as smartphones [11].

2.2 Phishing Detection Methods & Approaches

Since Phishing directly threatens losing one's identity and finances, it has a profound and prominent effect. It is pertinent to mention that to identify phishing attacks, phishing detection tools, and techniques are to be studied in detail. Thus, the negative effects of phishing attempts might be decreased. For such purposes, multiple phishing detection methods and approaches are utilized. For instance, a heuristic-based system known as the PhishCatch algorithm was designed to alert and identify users of phishing emails.

It develops phishing filters and rules in the algorithm by thoroughly examining phishing practices and policies. During testing, the software gave a catch rate of 80% and an accuracy of 99% [12]. Moreover, the researchers have developed machine-learning models using an extensive range of parameters. With the help of these models, researchers can easily detect and classify phishing web pages [13]. Machine learning (ML) is widely used for data analysis and has demonstrated significant potential in effectively addressing phishing attacks, surpassing traditional anti-phishing methods such as awareness seminars, visualization, and legal remedies [14]. Furthermore, Blacklist and Whitelist methods are also used to detect phishing where the URL is compared to a preset phishing URL. However, due to the lengthy time it takes to add a new phishing site to the blacklist, it can't cover all of them [15]. Same as above, [16] proposed a way to identify phishing cyber-attacks that revealed a client's susceptibility to harmful compounds, allowing protection breaches. Furthermore, heuristic-based methods are also used to identify fraudulent or legitimate websites. Heuristic-based tactics, also termed features-based strategies, work by selecting a set of distinguishing qualities that help define a website. PhishShield, a PC program by [17], analyzes phishing page URLs and content.

2.3 Most Common Phishing Vectors

According to [4], three communication channels, namely the internet, short messaging service, and voice, can be utilized to carry out a phishing assault. Various phishing vectors can be employed inside each of these mediums. Examples of phishing vectors commonly used on the internet include email, eFax, instant messaging, social media networks, websites, and Wi-Fi. Moreover, the attacker can utilize several technical methods to carry out the phishing assault on any of these channels. Some common attack vectors used to target a website are click-jacking, weaknesses in web browsers, cross-site scripting, and man-in-the-middle attacks [4]. The attacking vector that has received the most attention during the expansion of mitigation strategies is phishing through websites [1].

2.4 Anti-Phishing Guidelines and Recommendations

Organizations should consider and ensure strict implementation of security protocols, access control,s training and awareness programs, device strategies, and direction to lessen the effects of phishing attacks. Phishing knowledge can be further enhanced through training and awareness campaigns [19]. These goals are achieved through Seminars, discussions & virtual learning tools. For such purpose, an Endpoint security system could be introduced, which includes protection through antivirus, malware protection, host-based intrusion detection systems (HIDS), and email protection technologies [20]. Even with device infection, a strong firewall and architecture can limit access to enterprise networks, reducing cyber-attack risks [21], [22]. Moreover, it promotes backups, uses protection software, stops pop-ups, and updates computer hardware frequently [23]. Additionally, access control involves creating and implementing password and information transmission regulations. These deceptive online tripwires and

login rituals can extend web application authentication [24]. These methods are unaffected by password repetition and can be added to Microsoft Multi-Factor Authentication (MFA) systems to secure accounts during sophisticated phishing attacks [25]. Thus, businesses should follow these guidelines and implement appropriate policies to prevent Phishing. For instance, vulnerability management, threats, indicators of compromise, and best practices for exchanging, sharing, and processing privacy-sensitive data should inform cyber-security solutions [24]. Reinforcing password rules, reporting mechanisms, staff training, and physical security awareness on-site and personal devices is crucial to implementing these steps. A Standard Solution (SS) can help teams share power and provide consistent expert advice and phishing response protocols [26]. On the contrary, device policies must handle several stages of operation. Decision-makers must assess device lifespans, provide funds for lifecycle management, and maintain an up-to-date registry of all company equipment. To stay relevant, employees should avoid sharing information with strangers, avoid reciprocal exchanges, and offer accurate health and family information [27]. Moreover, End-users can prevent phishing attacks by using browser anti-phishing tools, validating links, and using their expertise [28]. Sensitive data should not be uploaded on public computers, and antivirus along with application updates is to be made on time [24]. Security breaches and identity theft can be avoided through strong authentication [19]. In conclusion, it is analyzed that awareness of mitigation policies is important for controlling phishing attacks and cyber security.

2.5 Hypotheses

Based on the literature, it is hypothesized that the student behavior, perceived threat awareness and mitigating strategies effects their vulnerability to phishing attacks. In order to be specific, we suggest that students with high level of awareness will generally have a much lower phishing vulnerability.

3 Materials and Methods

In this research, students' awareness at the Higher education level concerning phishing attacks was explored through quantitative research. It also focused on factors that lead to the prevalence of phishing attacks and their effect on students' perception of different phishing attacks. The study focused on different protocols and strategies for contradicting Phishing by using a questionnaire, according to research questions, to gather university students' responses. The upcoming section provides more details of the data collection process.

3.1 Data Collection Process

In this study, a questionnaire was used to gather information and assess the level of response and alertness among university students regarding phishing assaults. It consists of different sections to analyze students' understanding of phishing attacks. To address how students' perception was calculated and measured, we used a structured questionnaire with Likert-scale items ranging from 1 (strongly disagree) to 5 (strongly

agree) to capture students' awareness, susceptibility, and behavior toward phishing attacks. The average scores of responses were then used to quantify the overall perception for each construct. Participants were also asked about anti-phishing strategies. A thorough examination of existing data and literature lead to the creation of this questionnaire. It was done to guarantee its content's accuracy and relevancy. Protection Motivation Theory (PMT), described by Rogers (1975) focused on application in cybersecurity education, such as the work of Witte (1992). It also played an important role in analyzing the elements described by this tool. A pilot study was conducted to validate further the questionnaire, involving a sample of university students. It aims to evaluate the instrument's reliability. This study inspected the data through Cronbach's alpha, which assessed the internal coherence or reliability of a collection of scales or survey questions. Its score was 0.92, which indicated a high-reliability level and confirmed that the tool assesses students' insights into phishing efforts. To answer the research questions, 715 University Students worldwide using online stages and platforms were involved in this study.

3.2 Participant Profile and Sampling

The study used a sample of 715 students of universities from different academic subjects. The demographics of participant show that most respondents were male, comprising 70.1% of the total sample. In terms of age, more than one-third of the respondents were between 18 and 25 years old (34.5%), followed by the 26-30 age group, which accounted for 25.5% of the sample. Educationally, nearly half of the respondents held a Bachelor's degree (45.8%). Regarding country of residence, a significant proportion of respondents currently resided in Saudi Arabia (31.2%), followed by respondents from Australia (14.6%) and the United States (12.0%).

3.3 Statistical Technique

Several statistical techniques were employed to analyze the data collected from the university students. Initially, descriptive analysis was performed using the frequency, percentage, mean, and standard deviation. Furthermore, correlation analysis was conducted to examine the relationships between the key variables: Student Behavior, Perceived Factors, Mitigating Strategies, and Student Perception. This helped identify the strength and direction of associations among these variables. Subsequently, multiple regression analysis was performed to assess the impact of Student Behavior, Perceived Factors, and Mitigating Strategies on Student Perception. Data were analyzed in SPSS v.27.

4 Results and Analysis

4.1 Students' Awareness and Behavior Regarding Phishing Attacks

The survey responses indicate varying levels of awareness and caution among university students regarding phishing attacks. Many students are somewhat confident (30.2%) in recognizing phishing emails, while 23.6% are not confident. Most students receive unsolicited emails occasionally (41.2%) or rarely (28.5%), and a considerable number still click on links or download attachments from unknown senders occasionally (25.3%) or frequently (9.8%). Phishing attempts from unfamiliar sources claiming to be from universities or government institutions are also common, with 37.4% receiving such emails occasionally. While most students are unlikely to enter login credentials on suspicious websites (52.8% either extremely or somewhat unlikely), 24.8% remain at risk. Similarly, although most students are somewhat unlikely to provide personal information via email to unknown senders (52.1%), a notable 25.7% are somewhat or extremely likely to do so.

Regarding receiving emails requesting urgent action, 40.4% of students encounter these occasionally. Many are very cautious (32.3%) or moderately cautious (25.1%) when providing personal information online. However, the likelihood of reporting suspicious emails to the university's IT department is mixed, with 26% somewhat likely and 17.1% extremely likely but 33.1% unlikely to report. Awareness of common phishing red flags is moderate to high, yet a significant number of students are only slightly or not aware (36.5%). Regarding device management, a large portion (39.9%) do not take specific actions to avoid phishing attacks, although 35.6% seek help from technical support.

4.2 Understanding of Common Types of Phishing Attacks

The survey responses reveal university students' varying awareness and understanding of phishing attacks. Familiarity with spear phishing attacks is relatively low, with 35.3% strongly disagreeing and only 16.6% strongly agreeing. Similarly, 30.1% of students strongly disagree about understanding email spoofing, indicating a need for better education on this technique. Awareness of website spoofing is slightly higher, with 26.0% strongly agreeing, but 33.0% strongly disagree. Pharming attacks are less known, with 27.6% strongly disagreeing and 19.1% strongly agreeing. Awareness of smishing attacks is more balanced, with 25.0% strongly agreeing.

For vishing attacks, 29.3% of respondents strongly disagree about their familiarity, while 24.5% strongly agree. Social engineering awareness is mixed, with 25.4% strongly disagreeing and 19.4% strongly agreeing. Knowledge about malware-based Phishing shows a higher awareness level, with 26.6% strongly agreeing. Credential harvesting is understood by a notable portion of students, with 25.3% strongly agreeing, but 28.6% strongly disagree. Brand impersonation in phishing attacks has a mixed response, with 26.9% strongly agreeing and 28.6% strongly disagreeing. Awareness of invoice phishing and job offer scams is moderate, with about 24.4% to 23.6% strongly

agreeing. Social media phishing awareness is relatively high, with 27.0% strongly agreeing. Urgent account update requests in phishing attacks are moderately understood, with 24.7% strongly agreeing.

Figure 1 represents the mean values of university students' awareness and understanding of various common types of phishing attacks. Each type of phishing attack was rated on a scale from 1 (strongly disagree) to 5 (strongly agree). The analysis reveals that students generally have a moderate level of awareness about phishing attacks, with mean values ranging from approximately 2.5 to 4.0 across different attack types. The highest mean awareness is observed for "Password Reset Scams" and "Fake Online Stores," indicating that students are particularly cautious about resetting passwords and verifying online store authenticity. On the lower end, "Spear Phishing" and "Email Spoofing" have lower mean values, suggesting that students are less familiar with these sophisticated phishing techniques.

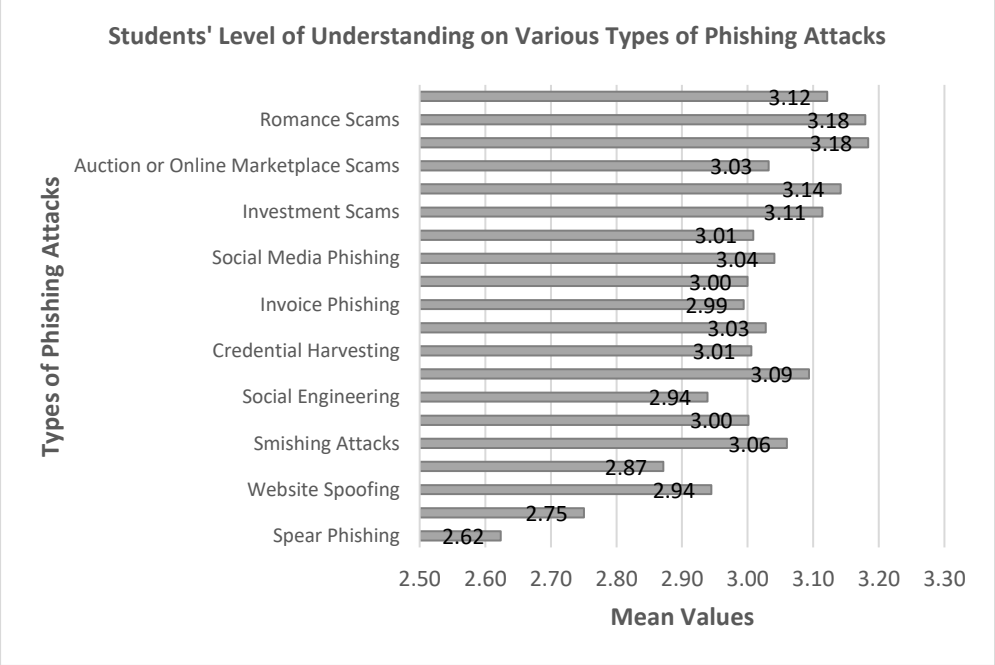

Figure.1 Mean Values of Level of Understanding of Common Types of Phishing Attacks

4.3 Factors Enhancing the Occurrence of Phishing Attacks

Table 1 presents the mean values and standard deviations of university students' perceptions regarding various factors that enhance the occurrence of phishing attacks. Each factor was rated on a scale from 1 (strongly disagree) to 5 (strongly agree). The survey responses highlight several factors that university students perceive as enhancing the occurrence of phishing attacks. The most significant factor identified is the "lack of awareness among university students," with 33.9% of respondents strongly agreeing.

This suggests that improving awareness could significantly reduce phishing vulnerabilities.

Another notable factor is the "failure to verify the authenticity of communications," with 31.8% strongly agreeing that this increases vulnerability to phishing attacks. Similarly, "inadequate skills in handling phishing attacks" is recognized, with 30.8% strongly agreeing that it raises the likelihood of falling victim. In contrast, the factor with the lowest agreement is "the busy schedules of university students," with only 23.1% strongly agreeing that it makes them more susceptible to phishing attacks. This indicates that while busy schedules are a concern, they are not perceived as the most critical factor. The analysis indicates that students generally agree that a lack of awareness (mean = 3.47) and failure to verify the authenticity of communications (mean = 3.40) significantly contribute to the occurrence of phishing attacks.

Similarly, inadequate skills in handling phishing attacks (mean = 3.39) and limited scrutiny of email senders (mean = 3.36) are perceived as important factors. Other notable factors include the desire for financial assistance (mean = 3.34) and the use of urgency and fear tactics by attackers (mean = 3.27). The data also suggests that regular security updates (mean = 3.23) and peer influence (mean = 3.24) play significant roles in phishing susceptibility.

Table 1. Factors Enhancing Phishing Attacks Among University Students

Factors	Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree	Mean	SD
Lack of regular security updates heightens phishing risks for university students.	23.1%	10.2%	13.6%	26.9%	26.3%	3.23	1.515
Lack of awareness contributes to phishing attacks among university students.	17.7%	11.1%	12.1%	25.3%	33.9%	3.47	1.487
Blind trust in university emails increases students' vulnerability to phishing.	17.8%	11.5%	15.0%	23.8%	31.8%	3.40	1.476
Inexperience in handling phishing attacks raises students' likelihood of falling victim.	19.0%	11.4%	12.3%	26.6%	30.8%	3.39	1.491
Phishing tactics using urgency and fear are more effective on university students.	18.7%	12.0%	19.1%	24.5%	25.7%	3.27	1.440
Busy schedules make university students more prone to phishing attacks.	17.7%	16.1%	19.0%	24.2%	23.1%	3.19	1.414
Financial need increases students' vulnerability to phishing attacks.	17.2%	13.0%	16.6%	24.7%	28.5%	3.34	1.446
Overreliance on technology without proper security heightens phishing risks for students.	19.6%	11.4%	15.6%	28.0%	25.4%	3.28	1.455
Limited cybersecurity education leads to more phishing attacks on university students.	20.1%	13.7%	12.7%	26.0%	27.4%	3.27	1.494
Limited scrutiny of email senders increases students' susceptibility to phishing.	18.5%	11.2%	14.0%	27.7%	28.5%	3.36	1.463

University students' tendency to share personal information raises phishing risks.	19.6%	14.5%	16.9%	26.4%	22.6%	3.18	1.438
Lack of two-factor authentication (2FA) increases students' vulnerability to phishing.	18.8%	13.1%	16.8%	25.3%	26.0%	3.26	1.453
Peer influence enhances students' susceptibility to phishing attacks.	18.2%	12.7%	20.9%	23.6%	24.5%	3.24	1.422

4.4 Descriptive Analysis of Mitigating Strategies of Phishing Attacks

The survey responses illustrate university students' perceptions of various strategies to mitigate phishing attacks. A significant majority strongly agree (40.6%) that never sharing personal information unless the origin is confirmed is crucial. Similarly, 40.6% strongly agree that providing training and awareness programs on phishing attacks is an effective strategy. Exercising caution with emails from unknown or suspicious sources also received high agreement, with 37.1% strongly agreeing. Deleting phishing emails without opening them is considered the most effective strategy by 39.6% of respondents. Regular computer hardware and software updates are seen as effective by 36.4% of students. Introducing mandatory education on Phishing, especially for first-year students, received strong support, with 40.0% strongly agreeing. These findings suggest that a combination of education, proactive measures, and technical solutions are seen as essential strategies to mitigate phishing attacks among university students. Notably, a significant 40.6% of respondents strongly agree that providing training and awareness programs on phishing attacks is crucial, indicating a strong belief in the effectiveness of educational initiatives.

4.5 Correlation Analysis

The correlation matrix (Table 2) reveals several significant relationships between the variables. The strongest relationship is observed between *Perceived Factors* and *Mitigating Strategies*, with a Pearson correlation coefficient of r=0.691 (p<.001), indicating a strong positive correlation. This suggests that as students perceive more factors contributing to phishing attacks, they also recognize more mitigating strategies to combat these attacks. On the other hand, the weakest relationship is between *Student Behavior* and *Perceived Factors*, with a Pearson correlation coefficient of r=0.354 (p<.001). While still significant, this correlation is relatively weaker compared to the others. The data indicate that while all variables are significantly correlated, the strength of these correlations varies.

Table 2. Correlation Matrix of Study Variables

Correlations

Variables	Student Behavior	Perceived Factors	Mitigating Strategies	Student Perception
Student Behavior	1			
Perceived Factors	.354**	1		
Mitigating Strategies	.362**	.691**	1	
Student Perception	.375**	.636**	.602**	1

**. Correlation is significant at the 0.01 level (2-tailed).

The regression analysis was conducted to examine the impact of Student Behavior, Perceived Factors, and Mitigating Strategies on Student Perception regarding phishing attacks. The model summary indicates that the three predictors (Student Behavior, Perceived Factors, and Mitigating Strategies) collectively explain 47.0% of the variance in Student Perception ($R^2 = 0.47$). The model explains approximately 47% of the variance in phishing avoidance behavior, which suggests a moderate fit of the model. The ANOVA results show that the regression model is statistically significant, $F(3, 681) = 201.645$, $p < 0.001$, indicating that the predictors significantly explain the variance in Student Perception. The coefficients table reveals the individual contribution of each predictor to the model. The unstandardized coefficient (B) for Student Behavior is 0.169 ($t = 4.409$, $p < 0.001$), indicating that for each unit increase in Student Behavior, Student Perception increases by 0.169 units, holding other factors constant. The unstandardized coefficient for Perceived Factors is 0.392 ($t = 10.152$, $p < 0.001$), indicating a strong positive relationship. The unstandardized coefficient for Mitigating Strategies is 0.266 ($t = 7.139$, $p < 0.001$), with a standardized coefficient (Beta) of 0.280, indicating a significant positive impact on Student Perception.

Table 3. Regression Analysis Results

Model	**Variables**	R-square	F	p	**Unstandardized**	**Standardized**	t	Sig.
					Coefficients			
1					B	Beta		
	(Constant)				0.267		2.045	0.041
	Student Behavior	0.47	201.650	<.001	0.169	0.133	4.409	<.001
	Perceived Factors				0.392	0.396	10.152	<.001
	Mitigating Strategies				0.266	0.280	7.139	<.001

a. Dependent Variable: Student. Perception

The regression equation indicates how changes in Student Behavior, Perceived Factors, and Mitigating Strategies affect Student Perception. Based on the regression analysis results, the regression equation can be formulated as follows:

Student Perception=0.267+0.169(Student Behavior)+0.392(Perceived Factors)+0.266(Mitigating Strategies)

5 Discussion

The study investigated the factors influencing university students' perceptions of phishing attacks and the effectiveness of mitigating strategies. The analysis provided several key insights into the relationships between student behavior, perceived factors, mitigating strategies, and overall student perception. The results show that while students are somewhat aware of "Social Media Phishing" and "Investment Scams," there remains a significant need for increased education and awareness efforts, particularly for less commonly understood phishing methods such as "Pharming Attacks" and

"Vishing Attacks." The data strongly supported the importance of educational initiatives. A substantial percentage of students agreed that providing training and awareness programs is crucial (40.6% strongly agreed). The finding is similar to [29], which emphasizes the importance of raising awareness among the students regarding cyber-security and phishing attacks.

The survey reveals several key insights into university students' perceptions of effective strategies to mitigate phishing attacks. Notably, a significant 40.6% of respondents strongly agree that providing training and awareness programs on phishing attacks is crucial, indicating a strong belief in the effectiveness of educational initiatives. Similarly, the same percentage strongly agrees that never sharing personal information unless its origin is confirmed is essential for preventing phishing attacks. This highlights the importance of verification and cautious behavior. Additionally, 39.6% of respondents consider deleting phishing emails without opening them as the most effective strategy, while 36.4% emphasize the need for regular updates to computer hardware and software. The establishment of a dedicated cybersecurity helpdesk is supported by 34.7% of students, underscoring the value of accessible support and guidance. These findings suggest that a combination of education, proactive measures, and technical solutions are seen as vital strategies to enhance cybersecurity and mitigate phishing risks among university students. [30], [31] presented the same findings that through taking certain educational measures and providing technical solutions, university students could be guided to fight against phishing attacks, hence improving cyber-security.

The correlation matrix reveals several significant relationships between the variables. The strongest relationship is observed between Perceived Factors and Mitigating Strategies, with a Pearson correlation coefficient of $r=0.691$ ($p<.001$), indicating a strong positive correlation. This suggests that as students perceive more factors contributing to phishing attacks, they also recognize more mitigating strategies to combat these attacks, which is consistent with the findings of [1], [32], [33].

The regression analysis indicates that all three predictors—Student Behavior, Perceived Factors, and Mitigating Strategies—significantly influence Student Perception of phishing attacks. Perceived Factors have the strongest impact, followed by Mitigating Strategies and Student Behavior. The overall model explains a substantial portion of the variance in Student Perception. It suggests that enhancing students' behavior, addressing perceived factors, and implementing effective mitigating strategies can significantly improve their perception and awareness of phishing attacks, which is similar to the findings of [1], [34], [35]. This underscores the importance of comprehensive educational and preventive measures in enhancing cybersecurity among university students.

5.1 Implication of study

This study has several implications in that it assists in giving students cyber-security education, which results in avoiding phishing attacks. By making the subject of cyber-security and phishing attacks a part of the curriculum, further awareness could be given

regarding the matter. This study determines how important it is for university students to remain vigilant with phishing attacks. The more familiar they are with Phishing, the more they will try to avoid such attacks. It gives awareness regarding the most common phishing attack types which are common now a days, along with the crucial factors which are responsible for the occurrence of such attacks. This study is also beneficial for higher education institutions, as they can create a cyber-security culture by making it a part of their policy documents in light of the findings. Thus, this study gives students more awareness to take certain safety measures, instead of relying upon the system.

5.2 Limitations of Study

The study also has limitations as it relied on self-reported data gathered from university students. Apart from that, as this was a quantitative study, the scope of findings is limited because of superficial results obtained through a quantitative survey questionnaire only. As with the ongoing advancements, new methods or types of phishing attacks might emerge that need to be tackled differently.

5.3 Conclusion and Future Recommendations

The study focuses on the unique role of different factors and actions in phishing vulnerability among students. This study provides findings that students' educational backgrounds have an important relation on phishing awareness and prevention strategies. It has also focused on wide range of academic subjects which has made it one of the first study which has offered detailed cross-disciplinary details.

This study aimed to explore the cyber –security awareness among university students, with special emphasis on their familiarity with phishing attacks. It explores the students' perceptions regarding the different types of phishing attacks, methods and factors responsible for the occurrence of such attacks. The findings suggest that enhancing student behavior, addressing perceived factors contributing to Phishing, and implementing effective mitigating strategies can significantly improve students' perceptions and awareness of phishing attacks. Educational institutions should focus on comprehensive educational programs, promote cautious behavior, and provide robust technical support and resources to protect students from phishing threats. This study provides the base for future researchers regarding raising awareness about cyber-security among students. Firstly, a longitudinal study could be planned to assess the effects of students' perception on their behavior towards dealing with phishing attacks. Such a study will also highlight the evolution of different types of phishing attacks and the methods to deal with them. Moreover, multiple online educational tools could be assessed to determine their use for raising cyber-security awareness among students.

References

1. Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation strategies against the phishing attacks: A systematic literature review. Computers & Security, 103387.

2. Chen, Y. H., & Chen, J. L. (2019). Ai@ ntiphish—machine learning mechanisms for cyber-phishing attack. IEICE Transactions on Information and Systems, 102(5), 878-887.
3. Sameen, M., Han, K., & Hwang, S. O. (2020). PhishHaven—An efficient real-time AI phishing URLs detection system. IEEE Access, 8, 83425-83443.
4. Chiew, K. L., Yong, K. S. C., & Tan, C. L. (2018). A survey of phishing attacks: Their types, vectors and technical approaches. Expert Systems with Applications, 106, 1-20.
5. Akazue, M. I., Ojugo, A. A., Yoro, R. E., Malasowe, B. O., & Nwankwo, O. (2022). Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria. Indonesian Journal of Electrical Engineering and Computer Science, 28(3), 1756-1765.
6. Liu, M., Zhang, Y., Liu, B., Li, Z., Duan, H., & Sun, D. (2021, December). Detecting and characterizing SMS spearphishing attacks. In *Proceedings of the 37th Annual Computer Security Applications Conference* (pp. 930-943).
7. Aleroud, A., Abu-Shanab, E., Al-Aiad, A., & Alshboul, Y. (2020). An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities. Journal of Information Security and Applications, 55. https://doi.org/10.1016/j.jisa.2020.102614
8. Ghazi-Tehrani, A. K., & Pontell, H. N. (2022). Phishing evolves: Analyzing the enduring cybercrime. In The New Technology of Financial Crime (pp. 35-61). Routledge.
9. Broadhurst, R., Skinner, K., Sifniotis, N., Matamoros-Macias, B., & Ipsen, Y. (2019). Phishing and cybercrime risks in a university student community. International Journal of Cybersecurity Intelligence & Cybercrime, 2(1), 4-23.
10. Parker, H. J., & Flowerday, S. V. (2020). Contributing factors to increased susceptibility to social media phishing attacks. South African Journal of Information Management, 22(1), 1-10.
11. Sharevski, F., Devine, A., Pieroni, E., & Jachim, P. (2022, September). Phishing with malicious QR codes. In Proceedings of the 2022 European Symposium on Usable Security (pp. 160-171).
12. Weider, D. Y., Nargundkar, S., & Tiruthani, N. (2009, July). Phishcatch-a phishing detection tool. In 2009 33rd annual IEEE international computer software and applications conference (Vol. 2, pp. 451-456). IEEE.
13. Gandotra, E., & Gupta, D. (2021). An efficient approach for phishing detection using machine learning. Multimedia security: algorithm development, analysis and applications, 239-253.
14. Abdelhamid, N., Thabtah, F., & Abdel-Jaber, H. (2017, July). Phishing detection: A recent intelligent machine learning comparison based on models content and features. In 2017 IEEE international conference on intelligence and security informatics (ISI) (pp. 72-77). IEEE.
15. Mohammad, R. M., Thabtah, F., & McCluskey, L. (2014). Predicting phishing websites based on self-structuring neural network. Neural Computing and Applications, 25, 443-458.
16. Jain, A. K., Parashar, S., Katare, P., & Sharma, I. (2020). Phishskape: A content based approach to escape phishing attacks. *Procedia Computer Science*, *171*, 1102-1109.
17. Rao, R. S., & Ali, S. T. (2015). Phishshield: a desktop application to detect phishing webpages through heuristic approach. Procedia Computer Science, 54, 147-156.
18. Ali, W., & Ahmed, A. A. (2019). Hybrid intelligent phishing website prediction using deep neural networks with genetic algorithm-based feature selection and weighting. IET Information Security, 13(6), 659-669.
19. Jampen, D., Gür, G., Sutter, T., & Tellenbach, B. (2020). Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences*, *10*(1), 33.

20. Mashtalyar, N., Ntaganzwa, U. N., Santos, T., Hakak, S., & Ray, S. (2021, July). Social engineering attacks: Recent advances and challenges. In *International Conference on Human-Computer Interaction* (pp. 417-431). Cham: Springer International Publishing.
21. Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: Threats, mitigation and approaches. *BMJ health & care informatics*, *26*(1).
22. Wash, R. (2020). How experts detect phishing scam emails. *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW2), 1-28.
23. Manjezi, Z., & Botha, R. A. (2019). Preventing and Mitigating Ransomware: A Systematic Literature Review. In *Information Security: 17th International Conference, ISSA 2018, Pretoria, South Africa, August 15–16, 2018, Revised Selected Papers 17* (pp. 149-162). Springer International Publishing.
24. Argaw, S. T., Bempong, N. E., Eshaya-Chauvin, B., & Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. *BMC medical informatics and decision making*, *19*, 1-11.
25. Moul, K. A. (2019, October). Avoid phishing traps. In *Proceedings of the 2019 ACM SIGUCCS Annual Conference* (pp. 199-208).
26. Althobaiti, K., Jenkins, A. D., & Vaniea, K. (2021). A case study of phishing incident response in an educational organization. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2), 1-32.
27. Venkatesha, S., Reddy, K. R., & Chandavarkar, B. R. (2021). Social engineering attacks during the COVID-19 pandemic. *SN computer science*, *2*, 1-9.
28. Sadiq, A., Anwar, M., Butt, R. A., Masud, F., Shahzad, M. K., Naseem, S., & Younas, M. (2021). A review of phishing attacks and countermeasures for internet of things-based smart business applications in industry 4.0. *Human behavior and emerging technologies*, *3*(5), 854-864.
29. Aldawood, H., & Skinner, G. (2018, December). Educating and raising awareness on cyber security social engineering: A literature review. In *2018 IEEE international conference on teaching, assessment, and learning for engineering (TALE)* (pp. 62-68). IEEE.
30. Cheng, E. C., & Wang, T. (2022). Institutional strategies for cybersecurity in higher education institutions. *Information*, *13*(4), 192.
31. Sharma, R., & Thapa, S. (2023). Cybersecurity awareness, education, and behavioral change: strategies for promoting secure online practices among end users. *Eigenpub Review of Science and Technology*, *7*(1), 224-238.
32. Sarker, O., Jayatilaka, A., Haggag, S., Liu, C., & Babar, M. A. (2024). A Multi-vocal Literature Review on challenges and critical success factors of phishing education, training and awareness. *Journal of Systems and Software*, *208*, 111899.
33. Waqas, M., Hania, A., Yahya, F., & Malik, I. (2023). Enhancing Cybersecurity: The Crucial Role of Self-Regulation, Information Processing, and Financial Knowledge in Combating Phishing Attacks. *SAGE Open*, *13*(4), 21582440231217720.
34. Kori, D., & Naik, R. (2023). Information Security Awareness Among Postgraduate Students: A Study of Mangalore University. In *Handbook of Research on Technological Advances of Library and Information Science in Industry 5.0* (pp. 270-286). IGI Global.
35. Baki, S., Qachfar, F. Z., Verma, R. M., Kennedy, R., & Jones, D. N. (2024). Real-Time, Evidence-Based Alerts for Protection from Phishing Attacks. *IEEE Transactions on Dependable and Secure Computing*, (01), 1-15.