Journal of Science Research International (JSRI)
ISSN: 2456-6365 (Online)

PHISHING ATTACKS AND THEIR PREVENTION TECHNIQUES

Shubhangi Pawar*, Harsheen Harpinder Kaur, Muskan Munawwar Jamdar, Siddhi Devendra Bhokare and Muskan Birendra Bisht

Department of Computer Science,

Pillai College of Arts, Commerce and Science (Empowered Autonomous), New Panvel

**Corresponding author E-mail: shubhangip@mes.ac.in*

Received: 20 January 2026	Revised: 22 February 2026	Accepted: 19 March 2026	Published: 15 April 2026

DOI: **https://doi.org/10.5281/zenodo.19609335**

Abstract:

Phishing attacks have become one of the most common and damaging cyber security threats in today's digital environment. This study aims to examine the nature of phishing attacks, identify commonly used phishing techniques, and analyze effective prevention methods to reduce cyber risks. The research follows a descriptive approach and uses both primary and secondary data sources. Primary data was collected through a structured questionnaire designed using Google Forms and distributed among college students. The survey focused on awareness levels, personal experiences, and preventive practices related to phishing attacks. Secondary data was gathered from academic journals, cyber security reports, and trusted online resources to support the study. The findings reveal that while most respondents are aware of phishing attacks, many users still fall victim due to lack of careful online behavior and limited use of security measures such as two-factor authentication. The study highlights that user awareness and timely education play a crucial role in minimizing phishing risks. The paper concludes that combining technological solutions with continuous cyber security awareness programs is essential to effectively prevent phishing attacks and enhance overall digital safety.

Keywords: *Phishing Attacks, Cybersecurity Awareness, Social Engineering, Online Safety, Prevention Techniques.*

1. Introduction

The rapid growth of digital technologies and internet services has transformed how people communicate, work, and access information. Platforms such as online banking, social media, and e-commerce have become a part of everyday life. However, this increased reliance on digital systems has also led to a rise in cybersecurity threats, particularly phishing attacks. Phishing is a type of cyberattack in which attackers impersonate trusted organizations or individuals to steal sensitive information such as passwords, financial details, and personal data.

These attacks usually occur through emails, messages, social media platforms, or fake websites and mainly target human behavior rather than technical system weaknesses.

This study aims to examine phishing attacks, understand their common techniques, and analyze prevention methods. It also evaluates the awareness and preventive behavior of college students, emphasizing the importance of combining technological security measures with user education to reduce phishing risks.

2. Literature review

Phishing attacks have become a significant concern in cybersecurity due to their increasing frequency and impact on users. Researchers describe phishing as a social engineering attack that targets human trust and decision-making rather than technical weaknesses in computer systems. Early studies mainly focused on detecting phishing emails and malicious websites by analyzing indicators such as suspicious URLs, email headers, and unusual website behavior, which helped in developing automated phishing detection tools.

Researchers have also highlighted the psychological aspects of phishing. Attackers often create urgency, fear, or authority in their messages to manipulate users into taking quick actions. Messages about account suspension, security alerts, or prize winnings are commonly used to trick users. With the rise of social media and mobile communication, phishing attacks have expanded to platforms such as social networking sites, SMS, and mobile applications, where users often trust messages from familiar sources.

Previous studies also discuss prevention methods such as spam filters, browser warnings, and anti-phishing software. However, many researchers emphasize that technical solutions alone are not enough. User awareness and proper training play an important role in preventing phishing attacks. Despite existing research, fewer studies focus specifically on awareness and preventive behavior among college students. This study aims to address this gap by examining students' awareness and highlighting the importance of education along with technical security measures.

3. Methodology

This study adopts a descriptive research design to examine phishing attacks and the effectiveness of various preventive techniques among college students. The primary aim of the research is to investigate users' awareness, personal experiences, and adoption of security practices related to phishing attacks. By using a combination of primary and secondary data, the study seeks to provide both empirical insights and theoretical support for understanding the current state of phishing awareness and prevention measures. Participation was voluntary, and no personal data was collected.

3.1. Research design

A descriptive and analytical approach was employed in this study. Descriptive research was chosen because it allows for the collection of factual, measurable information about participants' knowledge, experiences, and behavior without manipulating any variables. This design is particularly effective for understanding patterns, trends, and relationships within the data. The study also utilized analytical methods to systematically examine responses and draw meaningful insights about phishing awareness, exposure, and preventive strategies among students. This research design ensures that findings can accurately reflect real-world experiences and behaviors related to phishing attacks.

3.2. Participants

The study targeted college students enrolled in computer science, information technology, and related programs, as these students frequently use digital platforms and are more likely to encounter phishing threats. Participation in the survey was voluntary, and all participants were informed about the academic purpose of the study. A total of 40 students responded, providing a sufficient sample to analyze trends in awareness and behavior. To protect privacy, the study did not collect any personally identifying information, and all responses were kept anonymous. The sample included students from various age groups, genders, and academic streams, ensuring a diverse representation of digital users within the college environment.

3.3. Research instrument

The primary data collection tool was a structured questionnaire designed using Google Forms. The questionnaire consisted of 16 close-ended questions, carefully organized into four main sections:

i. Demographic Information – capturing age, gender, and course/stream to understand the background of participants.
ii. Awareness of Phishing Attacks – measuring participants' knowledge of phishing, sources of information, and perceived seriousness of the threat.
iii. Personal Experiences – examining encounters with phishing emails, messages, or links, including whether participants had clicked on suspicious links or shared sensitive information.
iv. Preventive Practices – evaluating security behaviors such as the use of antivirus software, two-factor authentication (2FA), checking sender details, and reporting phishing attempts.

The questionnaire was designed in simple and clear language to minimize confusion and encourage honest, accurate responses. Close-ended questions were preferred to facilitate quantitative analysis and to allow straightforward presentation of data in percentages, tables, and charts.

3.4. Data collection procedure

The survey was distributed via online communication platforms, including email, WhatsApp, and social media groups, which are commonly used by college students. Respondents were provided with a brief explanation of the research objectives and assured that their responses would be used strictly for academic purposes. The data collection period spanned one week, during which participants were encouraged to respond at their convenience. Google Forms automatically recorded and organized the responses, making the data collection process efficient and reducing the risk of human error. To ensure ethical compliance, participants were given the option to withdraw at any time, and they provided implicit consent by completing the survey. The anonymity and confidentiality of responses were strictly maintained, and no identifying information such as names, email addresses, or student IDs was collected.

3.5. Data analysis technique

The collected survey data was analyzed using descriptive statistics, mainly percentage analysis, and presented through tables, bar charts, and pie charts to show trends, frequencies, and patterns in participants' awareness, experiences, and preventive behaviors. Cross-tabulation was also used to examine relationships between variables such as age group, awareness levels, and preventive practices. This method provided a clear and objective presentation of results and is replicable, allowing future researchers to apply the same design and analysis to further study phishing awareness and prevention strategies.

4. Results

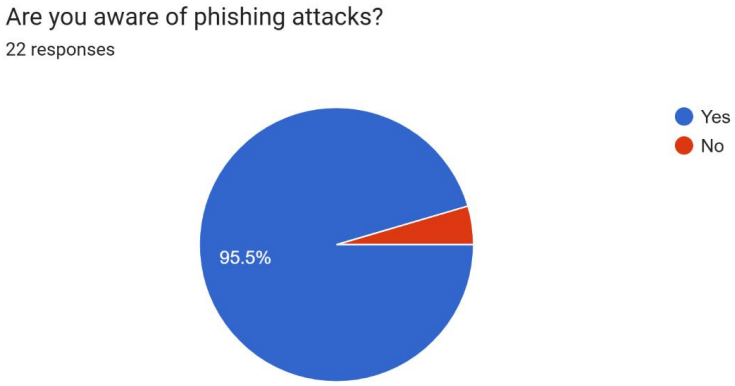
The survey collected responses from 22 participants to assess awareness, experiences, and preventive practices related to phishing attacks. The participants belonged to different age groups, genders, and academic streams. The findings are summarized below using tables for clarity.

Table 1: Demographic Information of Participants

Demographic Variable	Category	Frequency
Age Group	Below 18	1
	18–20	14
	21–23	6
	Above 23	1
Gender	Male	8
	Female	14
Course / Stream	Computer Science	14
	IT	3
	Other	5

Table 2: Awareness of Phishing Attacks

Question	Response	Frequency	Percentage (%)
Are you aware of phishing attacks?	Yes	21	95
	No	1	5



Source of Initial Awareness	Frequency	Percentage (%)
College / Teachers	13	59
Social Media	4	18
News / Internet	3	14
Other	2	9

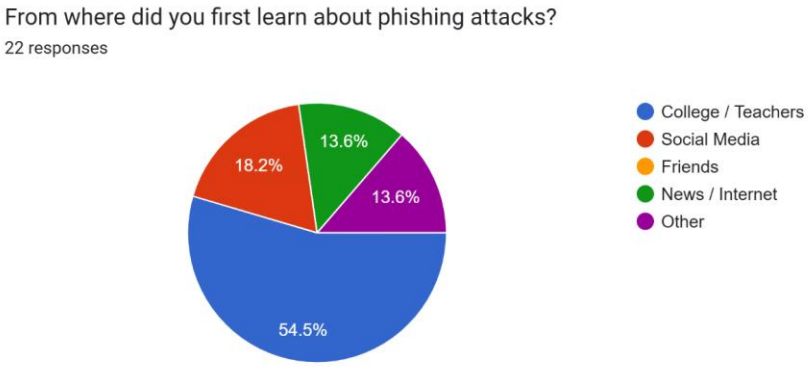


Table 3: Phishing Platforms as Perceived by Participants

Platform	Frequency	Percentage (%)
Email	5	23
Social Media	7	32
SMS / Messages	4	18
Phone Calls	1	5
All of the Above	5	23

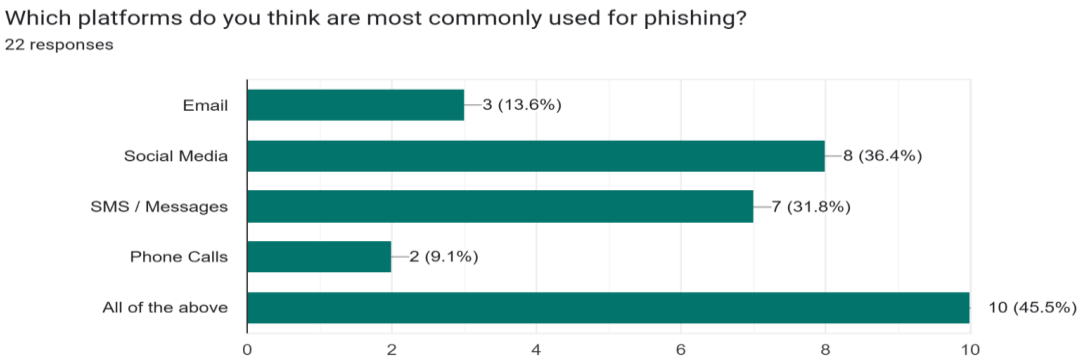
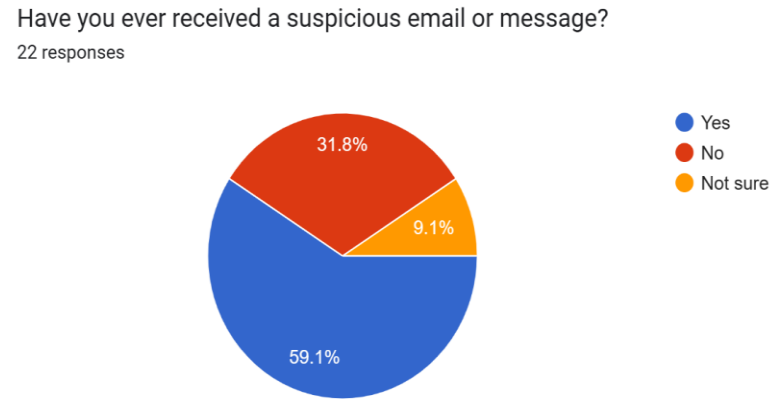
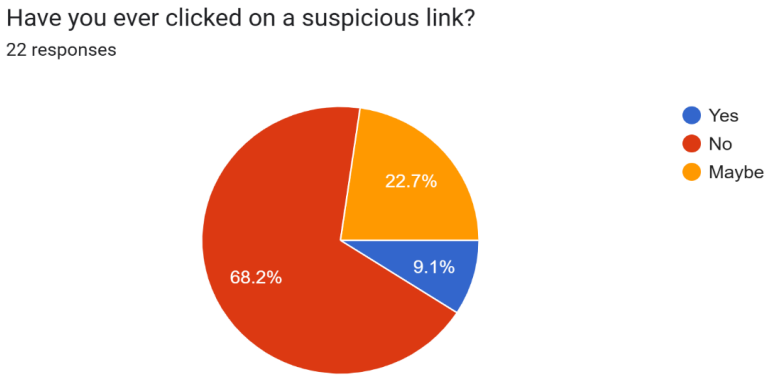


Table 4: Experience with Phishing

Question	Yes	No	Maybe / Not sure	Percentage (Yes)
Received suspicious email/message	15	5	2	68
Clicked on suspicious link	6	13	3	27
Shared personal information unknowingly	5	14	3	23





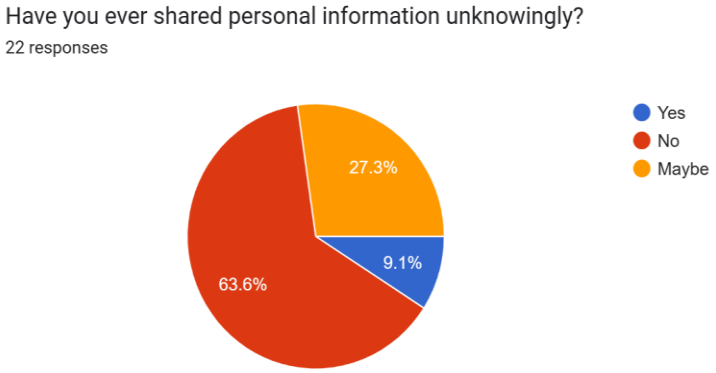
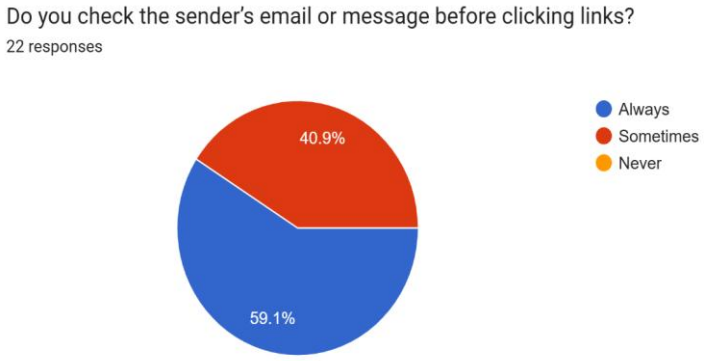


Table 5: Preventive Practices

Question	Always	Sometimes	No / Not aware	Percentage (Always)
Check sender details before clicking links	13	8	1	59
Use two-factor authentication (2FA)	13	4	5	59
Antivirus/security software installed	17	2	3	77
Report phishing emails/messages	8	7	7	36



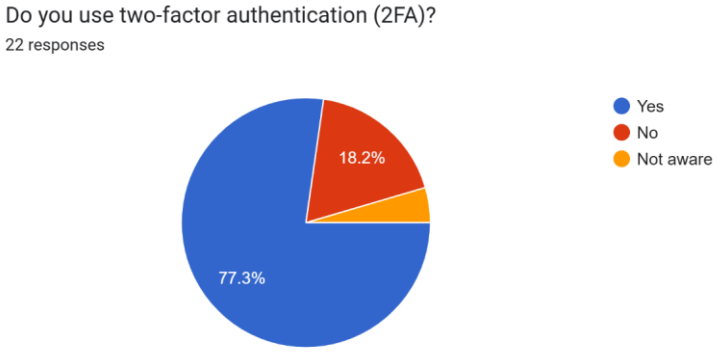
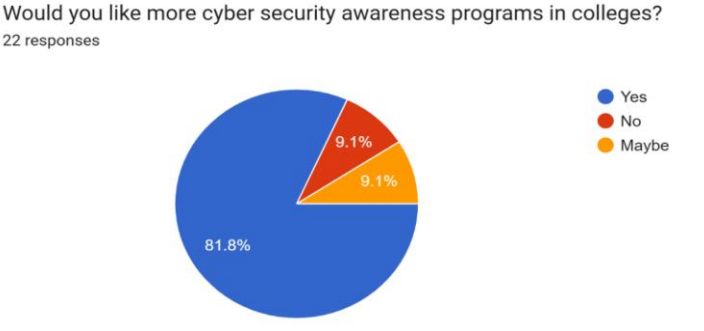


Table 6: Perception of Phishing Threats and Awareness Programs

Question	Response	Frequency	Percentage (%)
How serious are phishing attacks?	Very Serious	15	68%
	Serious	7	32%
Can user awareness reduce phishing attacks?	Yes	21	95%
	Maybe	1	5%
Desire for more cyber security programs in colleges	Yes	19	86%
	No	3	14%



Summary of findings

- Awareness: Nearly all participants (95%) were aware of phishing attacks, primarily learned through college/teachers.
- Platforms: Social media and email were identified as the most common platforms for phishing.
- Experience: Around 68% of respondents had received suspicious emails/messages, while 27% admitted clicking suspicious links.
- Preventive Practices: Majority use antivirus software (77%) and check sender details (59%). Use of two-factor authentication is moderate (59%). Reporting phishing messages is low (36%).
- Perception & Awareness: 68% of participants consider phishing attacks "very serious," and 95% agree that user awareness can reduce phishing risks. Most participants (86%) expressed interest in more cyber security programs.

5. Discussion

The study shows that while 95% of students are aware of phishing attacks, this awareness does not always result in safe behavior. 68% received suspicious messages and 27% clicked harmful links, showing that phishing often exploits human behavior. Many students take precautions such as using antivirus software (77%) and checking sender details (59%), but practices like two-factor authentication (59%) and reporting phishing attempts (36%) are less common. Most students recognize the seriousness of phishing (68%) and believe that greater awareness can reduce risks (95%), with 86% interested in cybersecurity awareness programs. Overall, the findings emphasize the need for stronger practical cybersecurity education, including awareness programs, hands-on training, and simulated phishing exercises to improve safe online behavior.

Conclusion

The study shows that although 95% of students are aware of phishing attacks, this awareness does not always translate into safe online behavior, as 68% received suspicious messages and 27% clicked harmful links. While many students use antivirus software (77%) and check sender details (59%), practices such as two-factor authentication (59%) and reporting phishing attempts (36%) are less common. Most students recognize the seriousness of phishing (68%) and believe that greater awareness can reduce risks (95%), with 86% interested in cybersecurity programs. Overall, the findings highlight the need for practical cybersecurity education, awareness programs, and simulated training to promote safer online behavior.

References

1. Alsharnouby, M., Alaca, F., & Chiasson, S. (2015). Why phishing still works: User strategies for combating phishing attacks. *International Journal of Human-Computer Studies, 82*, 69–82. https://doi.org/10.1016/j.ijhcs.2015.05.005
2. Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: Taxonomy of methods, current issues, and future directions. *Telecommunication Systems, 67*(2), 247–267. https://doi.org/10.1007/s11235-017-0334-z
3. Hong, J. (2012). The state of phishing attacks. *Communications of the ACM, 55*(1), 74–81. https://doi.org/10.1145/2063176.2063197
4. Milletary, J. (2005). *Technical trends in phishing attacks* (White paper). Software Engineering Institute, Carnegie Mellon University. https://www.sei.cmu.edu/library/technical-trends-in-phishing-attacks/
5. Khonji, M., Iraqi, Y., & Jones, A. (2013). Phishing detection: A literature survey. *IEEE Communications Surveys & Tutorials, 15*(4), 2091–2121. https://doi.org/10.1109/SURV.2013.032213.00009