IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

CYBERSECURITY AWARENESS AMONG COLLEGE STUDENTS

Ayush Jaiswal[1], Rishi Jha[2]

M.Sc. Information Technology – First Year, Pillai College of Arts, Commerce and Science Panvel, Navi Mumbai[1,2]

Abstract: Cybersecurity awareness is increasingly important for college students who use smartphones, social media, online learning platforms, cloud services and other internet-based applications. This study examines awareness of everyday cybersecurity practices, including password security, phishing recognition, multi-factor authentication, website verification, software updates and privacy settings. A descriptive questionnaire-based research design is presented. The study uses a model sample of 50 respondents and analyses the responses through frequencies, percentages and charts. The findings highlight areas of awareness as well as areas where additional cybersecurity education could be useful. The report concludes with practical recommendations concerning phishing awareness, authentication, passwords, privacy and cybersecurity training.

Keywords: Cybersecurity, Cybersecurity Awareness, College Students, Phishing, Password Security, Multi-Factor Authentication, Online Privacy

1. INTRODUCTION

1.1 Background of the Study

College students increasingly depend on digital services for academic work, communication, entertainment and personal activities. This creates a need for awareness of common cyber risks such as phishing, weak or reused passwords, unsafe links, poor privacy practices and outdated software.

1.2 Research Problem

The research problem is to examine the level of awareness that college students report regarding common cybersecurity risks and protective practices used in everyday online activities.

1.3 Objectives

1. To assess cybersecurity awareness among college students.
2. To examine awareness of phishing and suspicious links.
3. To study password and multi-factor authentication practices.
4. To examine privacy and software-update practices.
5. To identify areas where cybersecurity awareness education may be useful.

1.4 Scope

The study covers general cybersecurity awareness among college students, focusing on passwords, phishing, authentication, privacy, website verification, software updates and cybersecurity training.

1.5 Significance

The study can help identify common awareness gaps and provide a basis for practical cybersecurity education activities for students.

1.6 Limitations

The study is based on a limited sample of 50 respondents and uses self-reported responses. The findings therefore may not represent all college students.

2. LITERATURE REVIEW

Cybersecurity awareness involves knowledge and behaviour that can help users recognise and respond to digital risks. Phishing is a significant issue because attackers may imitate trusted services and persuade users to disclose credentials or other information. The National Institute of Standards and Technology (NIST) provides guidance on recognising and reducing phishing risk [1].

Password security is another important area. NIST guidance recommends strong authentication practices and notes that passwords are not phishing-resistant. It also provides guidance concerning password length and multi-factor authentication [1][2].

Multi-factor authentication provides an additional authentication factor beyond a password and can reduce the impact of a compromised password [2]. NIST's Digital Identity Guidelines also discuss authentication and authenticator management in detail [3].

The literature themes for this study are phishing awareness, password security, multi-factor authentication, privacy behaviour and cybersecurity education.

3. RESEARCH METHODOLOGY

3.1 Research Design

A descriptive survey design is used for the study. The purpose is to describe reported cybersecurity awareness and practices.

3.2 Population and Sample

The intended population is college students. The study uses a sample size of **50 respondents**.

3.3 Sampling Method

The study uses a convenient student sample for the academic project.

3.4 Data Collection Instrument

A structured questionnaire is used as the primary instrument. The questionnaire covers passwords, phishing, authentication, privacy, updates, training and awareness programmes.

3.5 Data Analysis

Responses are summarised using frequencies and percentages and presented through tables and bar charts. Percentage is calculated as: (Frequency ÷ 50) × 100.

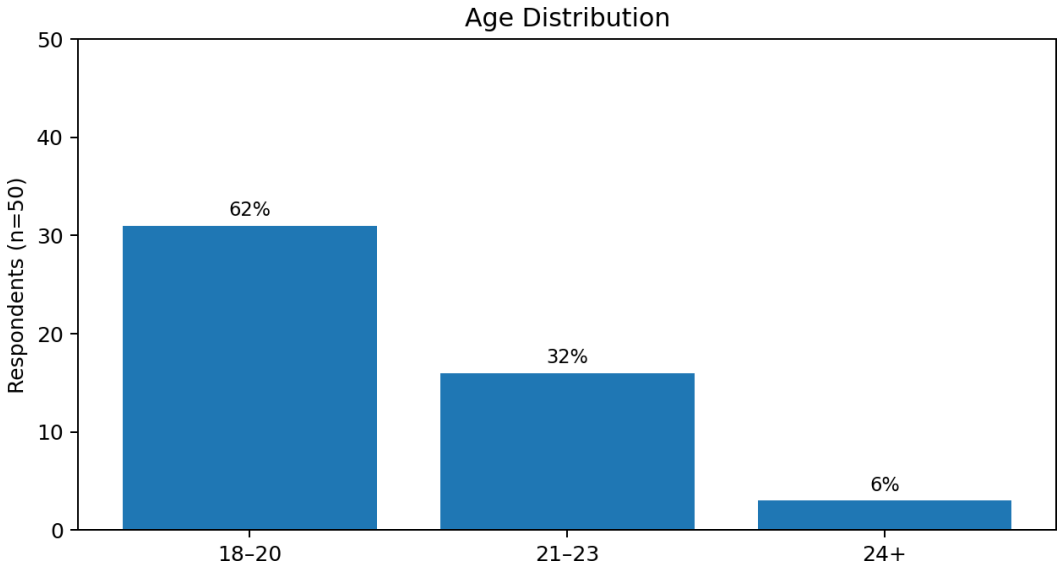
3.6 Ethical Considerations

The questionnaire should not request passwords, OTPs, bank details or other unnecessary sensitive information.

4. DATA ANALYSIS AND INTERPRETATION

4.1 Age Distribution

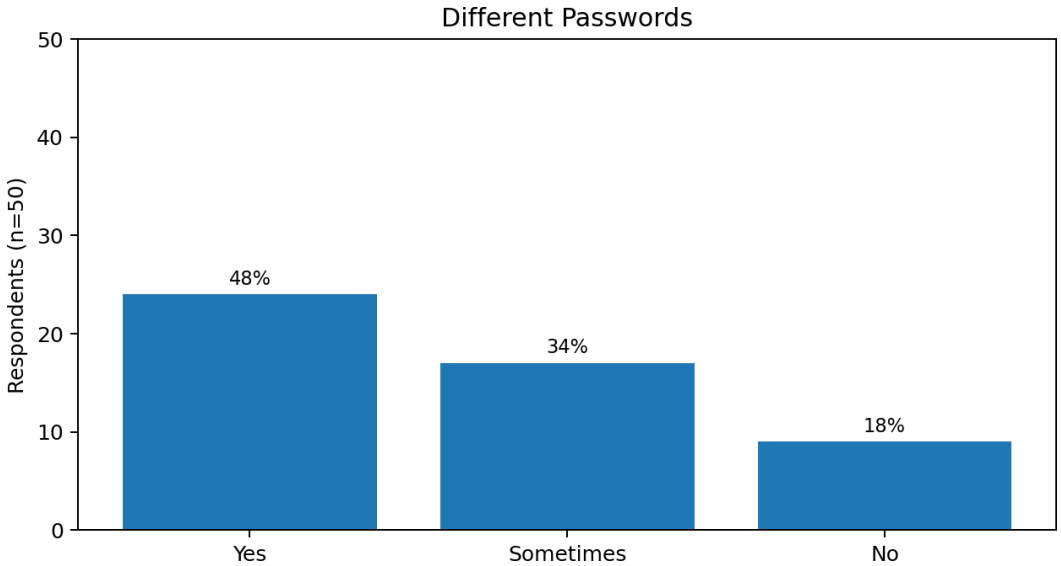
Response	Frequency	Percentage
18–20	31	62%
21–23	16	32%
24 or above	3	6%



Interpretation: The chart shows the distribution of responses for the selected question.

4.2 Use of Different Passwords

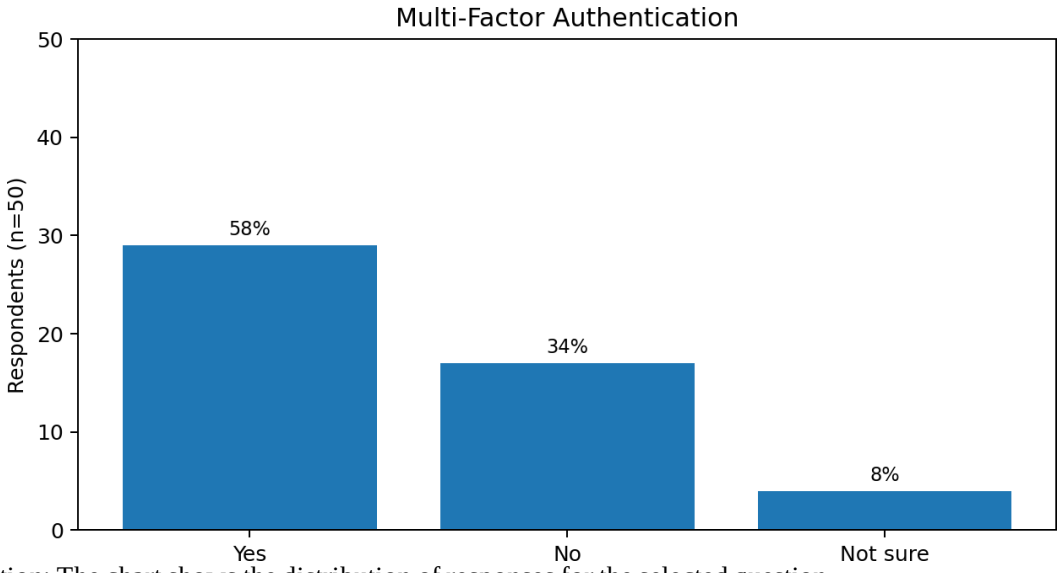
Response	Frequency	Percentage
Yes	24	48%
Sometimes	17	34%
No	9	18%



Interpretation: The chart shows the distribution of responses for the selected question.

4.3 Use of Multi-Factor Authentication

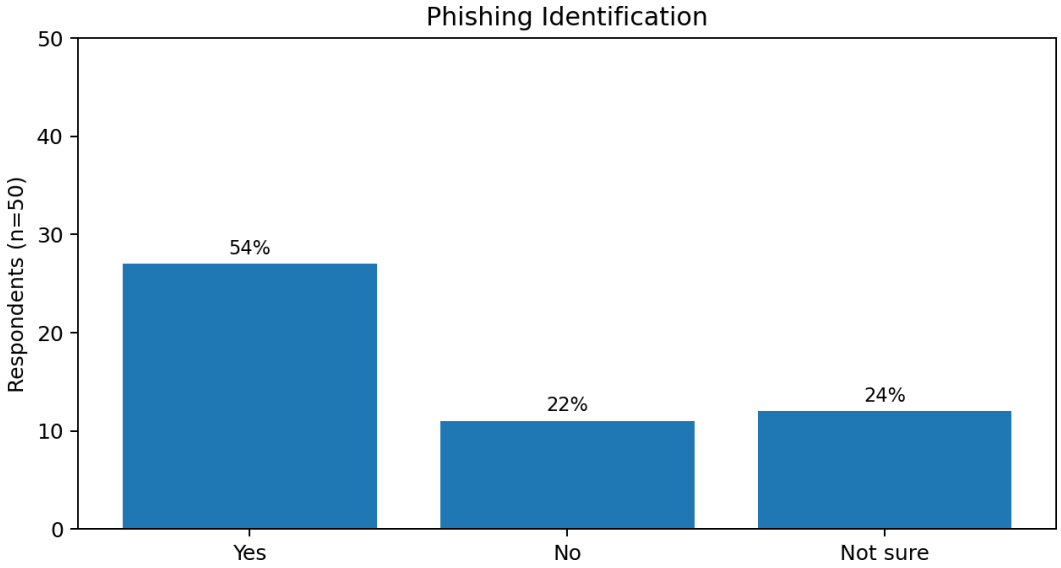
Response	Frequency	Percentage
Yes	29	58%
No	17	34%
Not sure	4	8%



Interpretation: The chart shows the distribution of responses for the selected question.

4.4 Ability to Identify Phishing

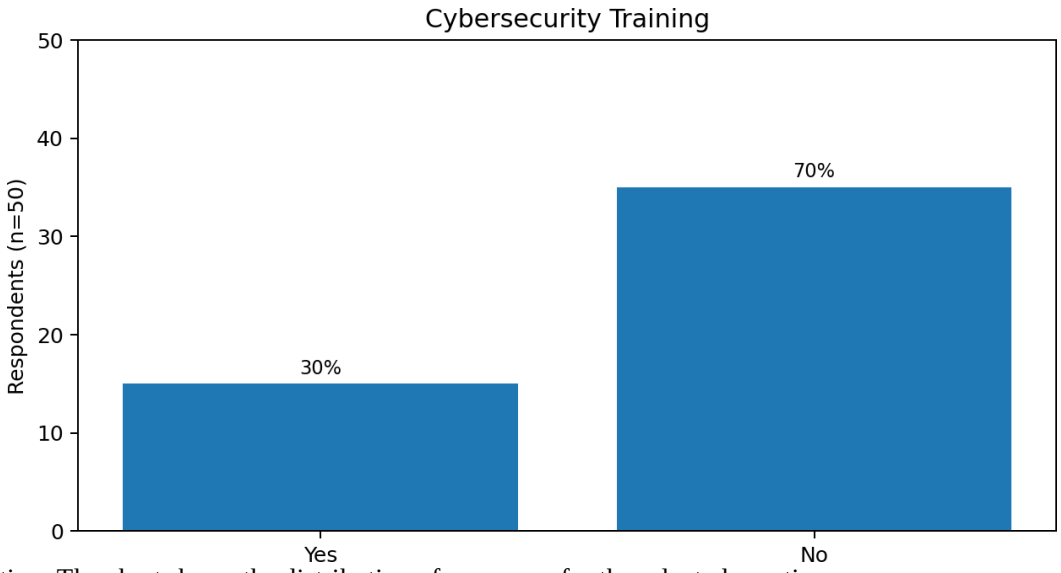
Response	Frequency	Percentage
Yes	27	54%
No	11	22%
Not sure	12	24%



Interpretation: The chart shows the distribution of responses for the selected question.

4.5 Cybersecurity Training

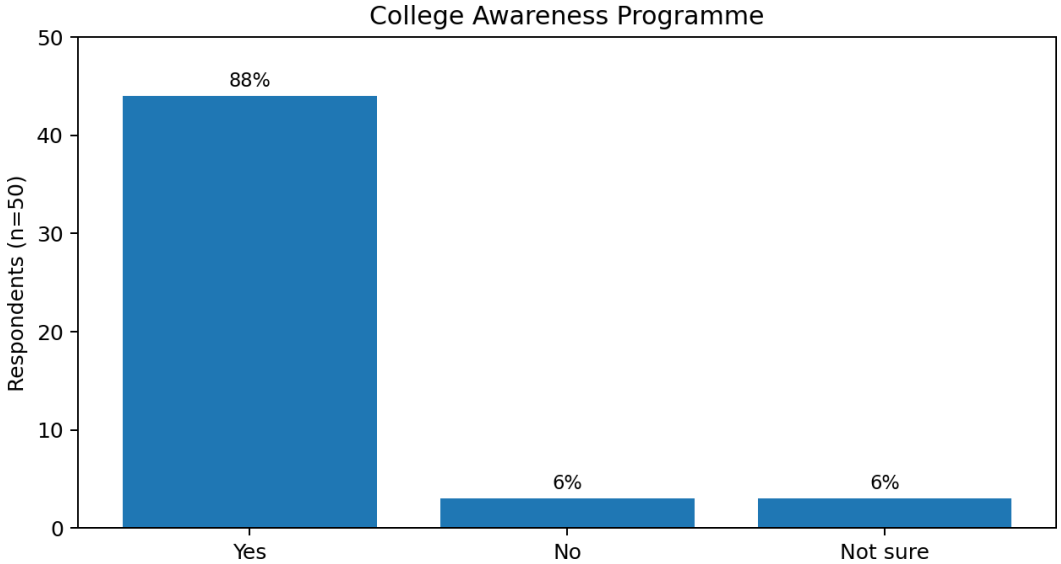
Response	Frequency	Percentage
Yes	15	30%
No	35	70%



Interpretation: The chart shows the distribution of responses for the selected question.

4.6 Support for College Awareness Programme

Response	Frequency	Percentage
Yes	44	88%
No	3	6%
Not sure	3	6%



Interpretation: The chart shows the distribution of responses for the selected question.

5. FINDINGS

Based on the analysed sample of 50 respondents:

- 62% of respondents are in the 18–20 age group.
- 48% reported using different passwords for different important accounts, while 34% selected "sometimes".
- 58% reported using multi-factor authentication, while 34% reported not using it.
- 54% reported that they could identify a phishing attempt, while 24% were unsure.
- 30% reported having received formal cybersecurity awareness training.
- 88% supported regular cybersecurity awareness programmes at colleges.

ACKNOWLEDGEMENT

We express our sincere gratitude to our teachers and Pillai College of Arts, Commerce and Science for providing us with the opportunity to prepare this research project. We are thankful for the academic guidance and support that helped us understand research structure, methodology, data interpretation and referencing.

6. CONCLUSION

The study indicates that cybersecurity awareness is an important aspect of safe digital behaviour among college students. The findings show awareness of several protective practices, while also indicating areas where additional education may be useful, particularly phishing recognition, authentication and formal cybersecurity training.

7. RECOMMENDATIONS

1. Conduct periodic cybersecurity awareness sessions for students.
2. Provide practical demonstrations of phishing and suspicious links.
3. Encourage multi-factor authentication for important accounts.
4. Teach students how to create and manage long, unique passwords or passphrases.
5. Encourage timely software and security updates.
6. Include privacy and personal-data protection in digital-literacy activities.
7. Establish a simple process for reporting suspicious messages or cybersecurity incidents.

REFERENCES

[1] National Institute of Standards and Technology. (2025). *How Do I Create a Good Password?*
[2] National Institute of Standards and Technology. (2026). *Multi-Factor Authentication.*
[3] National Institute of Standards and Technology. (2025). *Digital Identity Guidelines: Authentication and Authenticator Management (SP 800-63B-4).*
[4] National Institute of Standards and Technology. (2025). *Phishing.*

APPENDIX – QUESTIONNAIRE

Research Topic: Cybersecurity Awareness Among College Students

Instruction: Select the answer that best represents your view. Do not provide passwords, OTPs, financial information or other sensitive personal information.

1. What is your age group? (18–20 / 21–23 / 24 or above)
2. How often do you use the internet? (Daily / Several times a week / Occasionally)
3. Do you use a different password for different important accounts? (Yes / Sometimes / No)
4. Do you use multi-factor authentication on any important account? (Yes / No / Not sure)
5. Can you identify a suspicious or phishing email/message? (Yes / No / Not sure)
6. What do you usually do with a link from an unknown sender? (Open it / Ignore it / Verify it first / Other)
7. Do you check the website address before entering login information? (Always / Sometimes / Never)
8. How often do you install software/security updates? (Immediately / Later / Rarely/Never)
9. Do you review privacy settings on social media or online accounts? (Regularly / Sometimes / Never)

 This work is licensed under a Creative Commons Attribution 4.0 International License

10. Have you received a suspicious message asking for personal/account information? (Yes / No / Not sure)
11. How confident are you in recognizing common cyber threats? (Very confident / Confident / Neutral / Not confident)
12. Have you received formal cybersecurity awareness training? (Yes / No)
13. Which cybersecurity topic would you like to learn more about? (Phishing / Passwords / Privacy / Online fraud / Other)
14. Should colleges conduct regular cybersecurity awareness programmes? (Yes / No / Not sure)