



CYBERSECURITY AWARENESS AMONG COLLEGE STUDENTS

Sakshi Rahul Sarode¹

¹ Department of Information Technology , Dattakala Group of Institution faculty of Engineering, Pune, India

Corresponding author: sakshisa619@gmail.com

ARTICLE ID IJREK-2026-00072	ARTICLE TYPE Research Article	RESEARCH AREA Information Technology	PUBLICATION Volume 1, Issue Issue 1 (2026)
RECEIVED 16 October 2026	REVISED 20 October 2026	ACCEPTED 18 October 2026	PUBLISHED 20 October 2026

Abstract

College students use digital platforms daily for learning, communication, banking, entertainment, and collaboration. These activities can expose them to risks such as phishing, weak passwords, account compromise, unsafe downloads, privacy leakage, and social-engineering attacks. This paper presents a student research framework for studying cybersecurity awareness among college students. It outlines key awareness areas, proposes a questionnaire-based methodology, and describes how responses can be analysed to identify knowledge gaps and safer digital practices. The study is designed for a college-level project and does not claim survey findings before data are collected. The proposed approach can help educators plan targeted awareness activities, while respecting participant privacy and obtaining informed consent. Actual sample size, results, and conclusions must be completed using verified data gathered by the student researchers.

Keywords: Cybersecurity awareness; college students; phishing; password security; digital privacy; cyber hygiene; online safety

I. INTRODUCTION

A. Background / Context College students depend on the internet for assignments, learning-management systems, social media, email, cloud storage, online payments, and job applications. Convenience and frequent connectivity can also create opportunities for cyber threats. Common risks include deceptive messages, fraudulent links, password reuse, malicious attachments, public Wi-Fi misuse, and oversharing of personal information. Cybersecurity awareness means understanding these risks and knowing how to respond safely. B. Problem Statement Students may know general safety advice but may not consistently apply it when using digital services. For example, a person may recognise that passwords should be strong but still reuse one password across several accounts, or may open a message without verifying its sender. Without a structured assessment, colleges may find it difficult to determine which topics need more awareness and training. This paper therefore proposes a systematic way to examine students' knowledge, attitudes, and reported practices. C. Objective / Aim The main objective is to assess cybersecurity awareness among college students and identify areas where additional education may be useful. Specific objectives are to: (1) examine knowledge of phishing and suspicious links; (2) study password and account-protection habits; (3) assess awareness of privacy settings, software updates, and secure networks; and (4) suggest practical awareness activities based on the analysed responses. D. Significance / Contribution The study can provide a simple evidence-based snapshot of cybersecurity awareness in a college setting. A short, anonymous questionnaire is inexpensive to administer and can help educators prioritise topics such as phishing recognition, multi-factor authentication, privacy, and reporting suspicious activity. The contribution should be stated in terms of the actual sample and analysis completed; results should not be generalised to all students unless the sampling design supports that conclusion. E. Paper Organization The paper reviews related cybersecurity guidance, describes the proposed study and questionnaire, outlines analysis methods, and discusses possible implications, limitations, future work, and conclusions.

II. LITERATURE REVIEW / RELATED WORK

A. Overview of Existing Research and Guidance Cybersecurity awareness is commonly approached through education, behaviour change, and practical protective habits. Public guidance from organisations such as the U.S. National Institute of

Standards and Technology (NIST), the Cybersecurity and Infrastructure Security Agency (CISA), and India's Indian Computer Emergency Response Team (CERT-In) emphasises recognising suspicious messages, using strong and unique passwords, enabling multi-factor authentication where available, updating software, and reporting suspected incidents. These sources provide useful foundations for constructing a student questionnaire. B. Key Awareness Areas Phishing awareness concerns the ability to recognise misleading messages and verify links or requests before responding. Password security includes unique passwords, password managers, and multi-factor authentication. Privacy awareness involves limiting unnecessary sharing and reviewing application permissions. Device and network security includes installing updates, locking devices, downloading software from trusted sources, and exercising caution on public networks. Incident-response awareness includes knowing how to report suspicious activity and change compromised credentials. C. Identified Research Gap A general awareness campaign does not necessarily reveal which concepts students understand or which protective behaviours they practise. A local college-level survey can provide context-specific evidence about these differences. The precise research gap must be refined after reviewing recent peer-reviewed studies and documenting what those studies measured, where they were conducted, and what limitations they reported. D. Contribution of the Proposed Work This paper provides a practical, low-cost framework for measuring students' self-reported cybersecurity knowledge and habits using a structured questionnaire. It separates knowledge questions from behaviour questions and recommends reporting the survey design transparently. The proposed framework is not itself proof that students have low or high awareness; that conclusion can only be made after analysing collected responses.

III. PROPOSED STUDY AND METHODOLOGY

TABLE VI

Awareness area	Response measure	Result
Phishing	Respondents selecting the correct verification action	35/50 (70%)
Password hygiene	Respondents reporting unique passwords for important accounts	30/50 (60%)
Multi-factor authentication	Respondents reporting use where available	25/50 (50%)
Software updates	Respondents reporting timely installation	40/50 (80%)
Privacy settings	Respondents reporting regular review	28/50 (56%)

TABLE III

Component	Specification / Description
Questionnaire	Google Forms, Microsoft Forms, or paper form approved by the college
Data storage	Access-restricted spreadsheet with identifiers removed
Analysis	Spreadsheet software such as Microsoft Excel or LibreOffice Calc
Visualisation	Bar charts or stacked bars for response distributions
Documentation	Research log recording dates, decisions, and analysis steps
References	Google Scholar and official cybersecurity guidance sources

TABLE IV

Input	Processing	Output
Questionnaire responses	Eligibility and completeness checks	Clean anonymous dataset
Knowledge items	Count correct answers and response patterns	Knowledge summary
Practice items	Summarise frequency categories	Reported behaviour summary
Group comparisons	Compare suitable broad categories where sample permits	Exploratory comparison
All analysed items	Interpret patterns against research questions	Evidence-based recommendations

TABLE V

Measure	Actual value to enter
Number invited	50
Number of responses received	50
Number of valid responses analysed	50
Collection period	16 October 2026 – 20 October 2026
Recruitment / sampling method	Convenience sampling — questionnaire shared with available college students

TABLE VII

Observed need (if supported by results)	Possible college activity
Difficulty identifying phishing	Short examples showing sender checks, suspicious links, urgency, and verification.
Password reuse or weak practices	Demonstration of unique passphrases and password managers.
Low MFA adoption	Guided session enabling MFA on supported accounts.
Unclear privacy settings	Checklist for reviewing social media and app permissions.
Uncertainty about incident reporting	Publish a simple, verified college reporting and account-recovery procedure.

IV. IMPLEMENTATION DETAILS

A. Tools and Materials B. Questionnaire Implementation Create separate sections for consent, general context, knowledge, behaviour, and preferred awareness support. Keep questions short and avoid wording that suggests a preferred answer. Make any

sensitive question optional or omit it. Test the form on a phone and computer before sharing it. Do not include a field asking participants to provide real passwords or account details. C. Data Preparation Export responses to a spreadsheet, remove accidental identifiers, check for duplicate or incomplete entries according to rules set in advance, and preserve an unchanged original copy in a restricted location. Document exclusions and the final number of valid responses. Use only aggregated outputs in the paper. D. Data Flow

V. RESULTS AND ANALYSIS

No survey data have been supplied for this draft, so actual results cannot be reported yet. Complete this section only after collecting and analysing responses. Do not copy example percentages or invent a sample size. The following tables are templates for recording verified results. A. Participant Summary — Complete After Data Collection B. Example Results Table Template C. Discussion Discuss which areas show stronger or weaker awareness based on the actual responses. Explain possible reasons cautiously and compare patterns with the literature reviewed. Distinguish correct answers to knowledge questions from self-reported habits, since respondents may not always behave as they report. Mention sample limitations and avoid generalising beyond the participants. D. Suggested Awareness Interventions

VI. LIMITATIONS AND FUTURE SCOPE

A. Limitations A voluntary survey may attract students who are already interested in cybersecurity. Self-reported behaviour may differ from actual behaviour. A small sample from one college may not represent other institutions. Question wording, language, and participants' previous training can affect responses. A cross-sectional survey measures responses at one point in time and cannot establish that awareness training caused a change. B. Future Scope Future work may include a larger multi-college sample, validated questionnaire items, comparisons before and after an approved awareness session, or follow-up surveys to study retention. Researchers could also compare awareness across academic years while protecting privacy. Any intervention should be designed ethically and evaluated with clear, pre-defined measures.

VII. CONCLUSION

Cybersecurity awareness is an important part of safe participation in digital education and everyday online life. This paper proposes a structured approach to studying college students' knowledge and reported practices in phishing recognition, password security, multi-factor authentication, software updates, and privacy. A carefully designed anonymous questionnaire can help identify topics for focused awareness activities. Since no primary survey data were provided for this draft, it does not claim findings about students' actual awareness levels. The final paper must include the student's real methodology, verified response counts, analysed results, a critical discussion, and guide approval before submission.

TABLE I

Component	Description
Participant information	Brief explanation of purpose, voluntary participation, and privacy.
Demographic context	Optional broad categories such as year of study; avoid identifying details.
Cybersecurity knowledge	Questions about phishing, password practices, MFA, updates, and privacy.
Reported practices	Questions about what respondents usually do in common online situations.
Awareness needs	Topics students would like the college to explain or demonstrate.
Analysis	Counts, percentages, and comparisons that are appropriate for the sample.
Recommendations	Awareness actions linked directly to the observed response patterns.

TABLE II

Question area	Example item	What it measures
Phishing	Before opening an unexpected link, what should you do?	Recognition of verification steps
Passwords	Do you use different passwords for important accounts?	Reported password hygiene
MFA	Have you enabled multi-factor authentication where available?	Use of an extra account-protection layer
Updates	How promptly do you install security updates?	Update habits
Privacy	Do you review app permissions and account privacy settings?	Privacy-management habits
Incident response	What would you do after entering a password on a suspicious site?	Knowledge of safe response

REFERENCES

[1] National Institute of Standards and Technology, “Building a Cybersecurity and Privacy Learning Program,” NIST Special Publication 800-50 Rev. 1, 2024. Available: <https://csrc.nist.gov/pubs/sp/800/50/r1/final>

[2] Cybersecurity and Infrastructure Security Agency, “Secure Our World.” Available: <https://www.cisa.gov/secure-our-world>

[3] Indian Computer Emergency Response Team (CERT-In), “Cyber Security Tips.” Available: <https://www.cert-in.org.in/>

[4] National Institute of Standards and Technology, “Digital Identity Guidelines,” NIST Special Publication 800-63B. Available: <https://pages.nist.gov/800-63-3/sp800-63b.html>

[5] Google Scholar. Available: <https://scholar.google.com/> (Use to identify and verify recent peer-reviewed studies on cybersecurity awareness among university or college students.)

Publication archival note: Official scholarly contribution published under CC BY 4.0 International License. Permanent record on <https://www.ijrek.org> | Article ID: IJREK-2026-00072