International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Awareness of Cybersecurity Among College Students

SWARAJ BHAGAT[1], PRATIK SHITOLE[2], PRANAV PHADATARE[3], DR. SWATI JOSHI[4]

1,2,3 Department of Computer Science, PVG's College of Science and Commerce
4 Research Guide, Department of Computer Science, PVG's College of Science and Commerce

Abstract - In today's digital world, students rely heavily on the internet for education, communication, and daily activities. However, increased online activity also increases exposure to cyber threats such as phishing attacks, hacking, and data theft. This study examines the level of cybersecurity awareness and online safety practices among college students.

A survey of 60 students was conducted to understand their password habits, use of two-factor authentication, awareness of phishing attacks, public Wi-Fi usage, and privacy practices. The findings reveal that while students possess basic awareness of cybersecurity threats, risky behaviors such as password reuse, frequent use of public Wi-Fi, and limited adoption of security measures remain common.

The study highlights the need for cybersecurity awareness programs to promote safer digital practices among students and reduce their vulnerability to cyber threats.

Keywords: Cybersecurity Awareness, Information Security, Online Privacy, Student Behavior, Phishing & Online Threats, Digital Safety

1.INTRODUCTION

The internet has become an essential part of students' lives. From attending online classes and submitting assignments to using social media and digital payments, students depend on digital platforms every day. While technology provides convenience and connectivity, it also exposes users to various cybersecurity risks.

Cyber threats such as phishing scams, identity theft, malware attacks, and unauthorized access to personal accounts are increasing rapidly. Students are particularly vulnerable because they frequently use public Wi-Fi networks, share personal information online, and often lack strong security practices.

Cybersecurity awareness refers to understanding online risks and adopting safe digital behaviors such as using strong passwords, enabling two-factor authentication, and protecting personal data. Awareness and safe practices are essential to prevent cybercrime and protect sensitive information.

This study aims to evaluate the level of cybersecurity awareness among college students and analyze their online safety behaviors. By identifying common risky practices and knowledge gaps, the study seeks to highlight the importance of cybersecurity education and promote safer internet usage among students.

2.RESEARCH MOTIVATION

The rapid growth of internet usage among students has increased exposure to cyber threats such as phishing, identity theft, and data breaches. Despite frequent digital interaction, many students lack adequate knowledge of safe online practices. Recent incidents of cyber fraud and misuse of personal data highlight the urgent need to assess cybersecurity awareness among young users. Understanding student's behavior and safety practices can help identify awareness gaps and promote safer digital habits.

3.RESEARCH AIM

This study aims to evaluate the level of cybersecurity awareness among college students and examine their online safety practices, including password management, phishing awareness, and use of security measures such as two-factor authentication.

4.LITERATURE REVIEW

The increasing reliance on digital technologies in education has made cybersecurity awareness an essential competency for students. Several studies have explored students' knowledge of cyber threats, online safety behavior, and vulnerability to cybercrime in academic environments.

Studies focusing on cybersecurity awareness among university students reveal that although students frequently use digital platforms, their understanding of cyber threats remains limited. Research examining student awareness levels indicates that many students are familiar with the term cybersecurity but lack practical knowledge about phishing attacks, identity theft, and data protection practices. These findings are supported by studies on cybersecurity awareness assessment and educational environments, which highlight a gap between basic awareness and practical security skills [Papers 1, 3, 8].

Research related to digital learning environments and distance education shows that the expansion of online learning platforms has increased students' exposure to cyber risks. The transition to virtual classrooms has created new vulnerabilities, including phishing attacks, unauthorized access, and data breaches. Studies conducted during digital education transformation emphasize that students became more frequent targets of cyber threats during remote learning periods [Papers 2 and 9].

Several empirical studies highlight unsafe online behaviors among students, particularly in password management and authentication practices. Weak password habits, reuse of credentials, and reluctance to enable two-factor authentication significantly increase security risks. Researchers have observed that while students may be aware of security recommendations, they often fail to implement safe practices consistently [Papers 6 and 7].

Public network usage and unsafe browsing habits have also been identified as major contributors to cybersecurity vulnerability. Students frequently access sensitive information using unsecured public Wi-Fi networks, increasing the risk of data interception and privacy breaches. Studies examining student vulnerability patterns confirm that risky internet usage behaviors remain common among young users [Papers 6 and 8].

Educational research further emphasizes the importance of cybersecurity awareness programs in improving safe digital behavior. Awareness sessions, training workshops, and curriculum integration have been shown to enhance students' ability to recognize cyber threats and adopt protective practices. Research on awareness strategies and training effectiveness demonstrates that structured cybersecurity education significantly improves online safety behavior [Papers 4, 5, and 10].

Recent research has also explored ethical awareness, resilience, and long-term cybersecurity preparedness among students. Studies on cybersecurity ethics and resilience highlight the need for developing responsible digital behavior and strengthening institutional cybersecurity culture. These works stress that awareness alone is insufficient without behavioral change and continuous education [Papers 11, 12, 13, and 14].

Despite growing efforts to improve cybersecurity education, the literature indicates that awareness levels among students remain moderate, and a gap persists between knowledge and real-world security practices. Students often understand cybersecurity concepts but do not consistently apply protective measures in their daily online activities [Papers 1, 6, and 7].

Therefore, there remains a need to assess cybersecurity awareness and evaluate actual online safety behaviors among students. The present study contributes to existing research by examining cybersecurity awareness, safety practices, and risk behaviors among college students through a structured survey approach.

5.RESEARCH METHODOLOGY

The study employed a **Quantitative, Descriptive, and Survey-Based Approach** to examine cybersecurity awareness and online safety practices among college students.

5.1 Research Design and Approach

• **Design:** A descriptive and survey-based design was used to observe and document students' cybersecurity awareness, online behavior, and safety practices without manipulating any variables.

• **Approach:** A quantitative approach was adopted, focusing on collecting numerical data through a structured online questionnaire to measure awareness levels, password security habits, internet safety behavior, and privacy practices.

5.2 Data Collection and Sampling

• **Data Collection Method:** Primary data was collected using a structured online survey created through Google Forms. The questions were developed based on insights from the literature review and covered key areas such as password security, device safety, phishing awareness, privacy protection, and the importance of cybersecurity education.

• **Sampling Technique:** Convenience sampling was employed, reaching respondents who were easily accessible through online platforms such as WhatsApp to ensure quick data collection from active student internet users.

• **Sample Size:** The sample included all students who voluntarily responded to the survey (N = 60).

5.3 Research Instrument and Analysis

• **Instrument:** The main tool was a structured questionnaire in Google Forms, featuring multiple-choice questions designed to assess password practices, online safety behaviors, awareness of cyber threats, privacy settings, and opinions regarding cybersecurity awareness programs.

• **Data Analysis Techniques:** Google Forms generated preliminary charts, graphs, and summary statistics (pie charts and percentage distributions). The responses were further compiled in Google Sheets for interpretation. The final analysis involved examining response patterns and comparing the findings with insights from the literature review to identify similarities, gaps, and areas needing improvement.

5.4 Implementation

This section explains how the study was carried out using a Google Forms survey consisting of **15 questions** related to cybersecurity awareness and online safety practices. The objective was to understand students' security habits, awareness of cyber threats, and privacy practices based on real responses. The study relied on students' experiences and perceptions rather than controlled experiments.

A structured questionnaire was designed to collect data on key factors influencing cybersecurity awareness, including:

• password security practices and use of strong passwords
• use of two-factor authentication
• public Wi-Fi usage and device update habits
• awareness of phishing scams and suspicious links
• privacy protection behaviors and social media settings
• experience with account hacking incidents
• importance of cybersecurity awareness and need for training programs

The questions were multiple-choice and choice-based to ensure clarity and ease of response.

Survey Distribution & Data Collection

The Google Form was shared with students through **WhatsApp** to ensure quick participation.

• A total of **60 respondents** completed the survey.
• Google Forms automatically recorded responses.
• Data was exported to Google Sheets and Excel for analysis.

The responses reflected real student behavior and awareness levels, making the findings suitable for interpretation.

5.5 Validation of Findings

Validation was ensured through:

• **Comparison with literature:** Findings showed trends similar to previous studies, including moderate awareness and risky online behaviors.
• **Theoretical alignment:** Results aligned with established cybersecurity awareness and safety behavior factors.

6.RESULTS

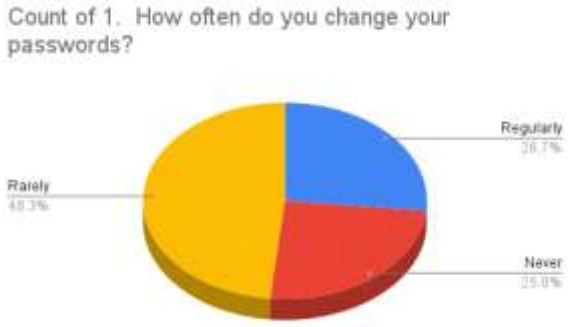

Fig -1: Above pie chart shows that 48.3% respondents rarely change their passwords, 26.7% change their passwords regularly, and 25.0% never change their passwords.

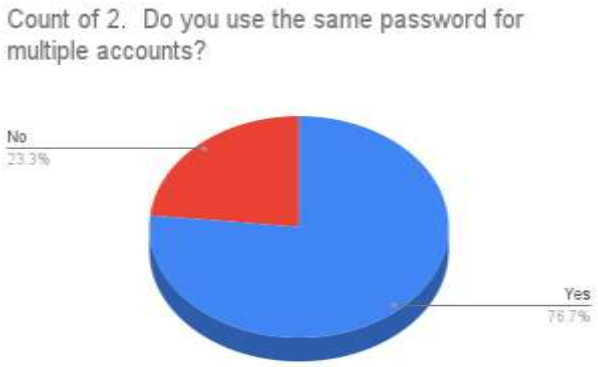

Fig -2: Above pie chart shows that 76.7% respondents use the same password for multiple accounts, while 23.3% respondents do not use the same password for multiple accounts.

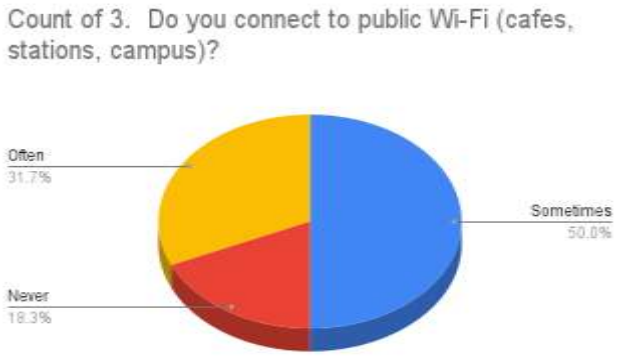

Fig -3: Above pie chart shows that 50.0% respondents sometimes connect to public Wi-Fi, 31.7% often connect to public Wi-Fi, and 18.3% never connect to public Wi-Fi.

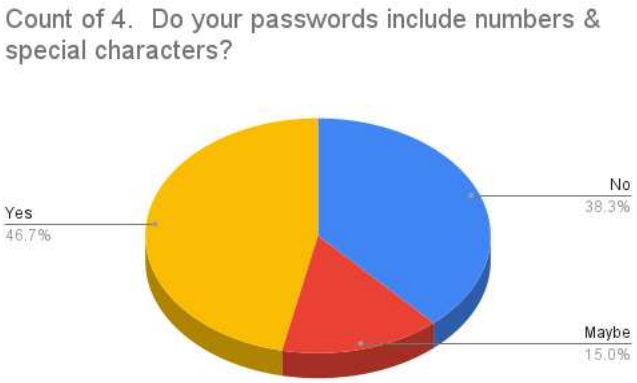

Fig -4: Above pie chart shows that 46.7% respondents' passwords include numbers and special characters, 38.3% respondents' passwords do not include numbers and special characters, and 15.0% respondents are not sure whether their passwords include numbers and special characters.

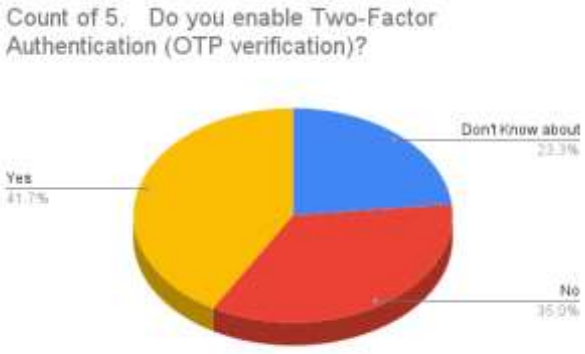

Fig -5: Above pie chart shows that 41.7% respondents enable Two-Factor Authentication (OTP verification), 35.0% respondents do not enable Two-Factor Authentication, and 23.3% respondents do not know about Two-Factor Authentication.

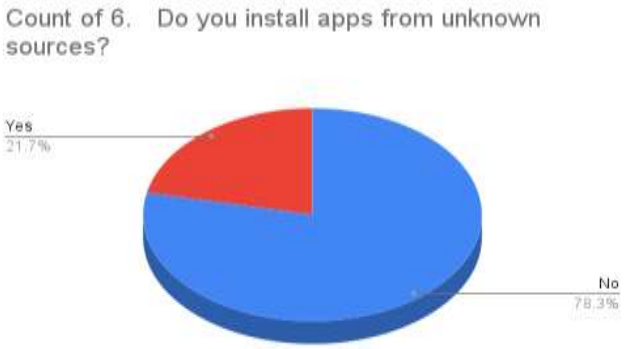

Fig -6: Above chart shows that 78.3% respondents do not install apps from unknown sources, while 21.7% respondents install apps from unknown sources.

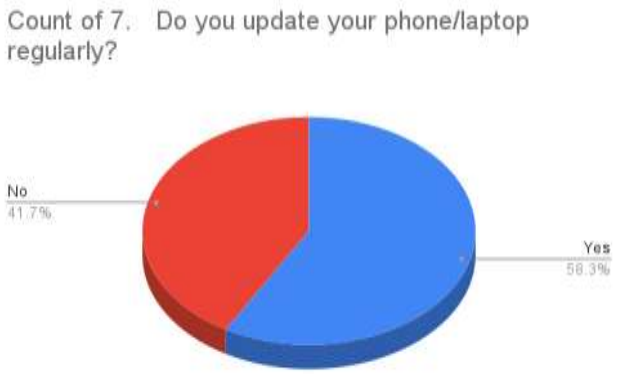

Fig -7: Above pie chart shows that 58.3% respondents update their phone/laptop regularly, while 41.7% respondents do not update their phone/laptop regularly.

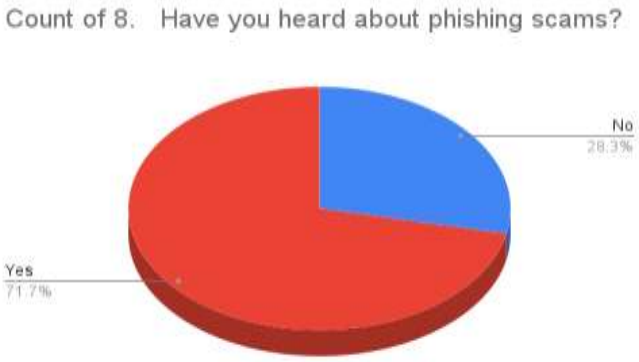

Fig -8: Above pie chart shows that 71.7% respondents have heard about phishing scams, while 28.3% respondents have not heard about phishing scams.

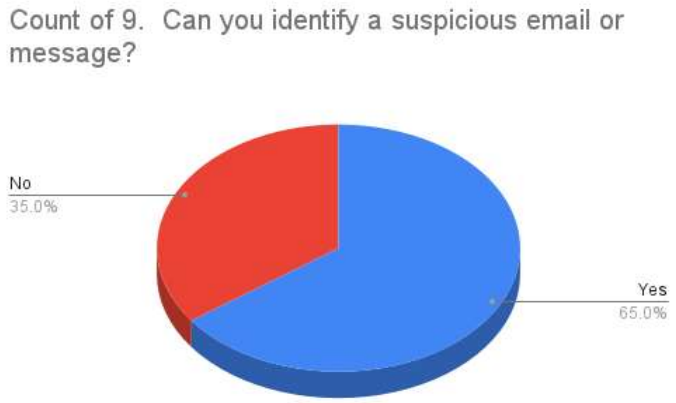

Fig -9: Above pie chart shows responses to the question It indicates that 65% of respondents can identify suspicious emails or messages, while 35% are unable to identify them.

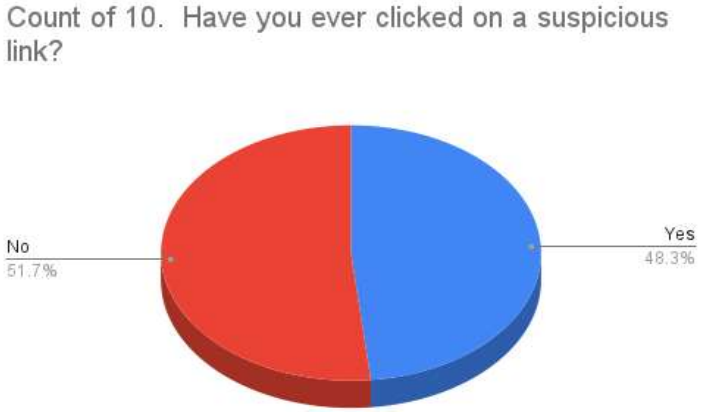

Fig -10: Above pie chart shows that 51.7% of the respondents have never clicked on a suspicious link, while 48.3% of the respondents have clicked on a suspicious link at some point.

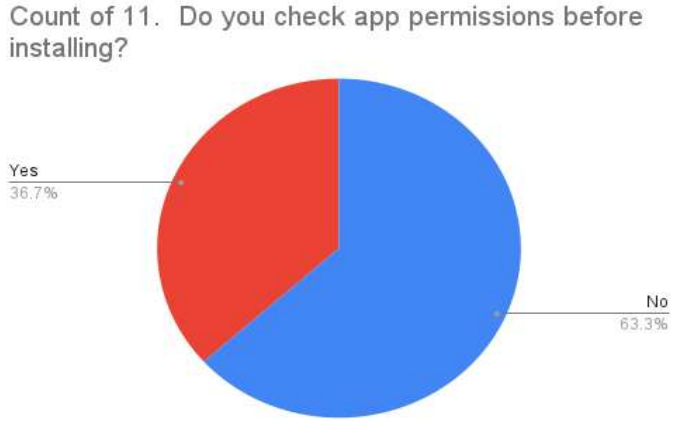

Fig -11: Above pie chart shows that 63.3% of the respondents do not check app permissions before installing applications, while 36.7% of the respondents check app permissions before installation.

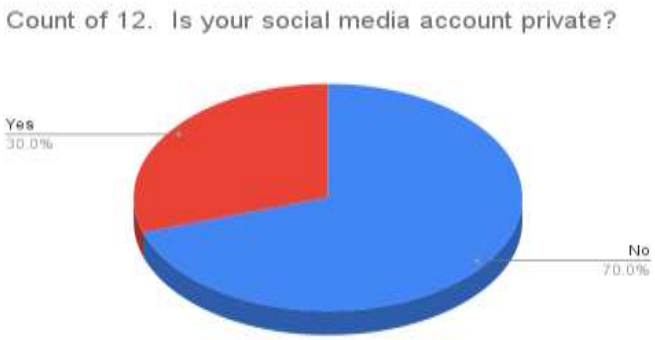

Fig -12: Above pie chart shows that 70% of the respondents do not keep their social media accounts private, while only 30% of the respondents have private social media accounts.

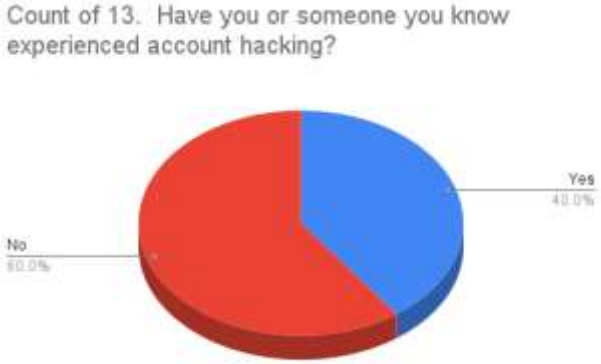

Fig -13: Above pie chart shows that 40% of the respondents have experienced account hacking either personally or through someone they know, while 60% of the respondents have not experienced any account hacking.

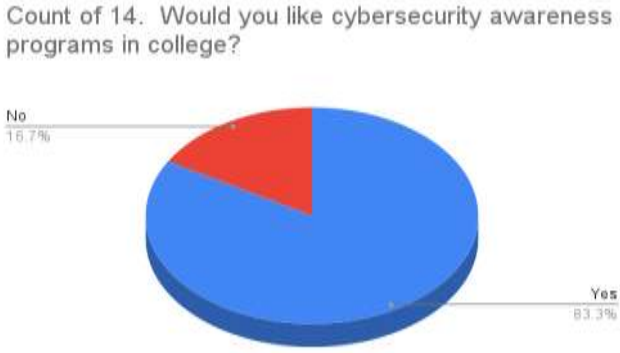

Fig -14: Above pie chart shows that a large majority of respondents (83.3%) would like cybersecurity awareness programs to be conducted in college, while only 16.7% of respondents are not interested in such programs.

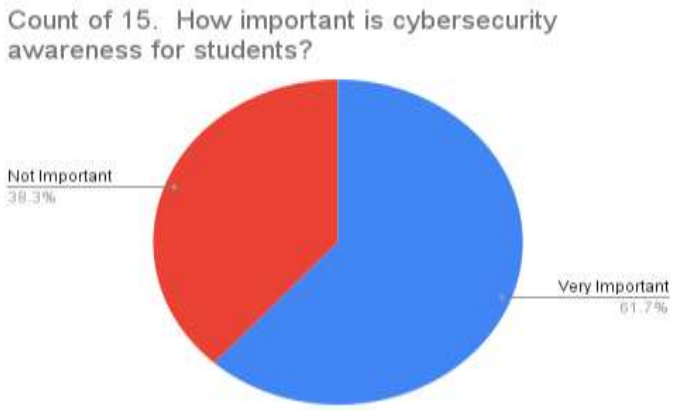

Fig -15: Above pie chart shows that 61.7% of the respondents consider cybersecurity awareness to be very important for students, while 38.3% of the respondents believe it is not important.

7.DISCUSSION

The findings from previous cybersecurity research and the present student survey converge around several important aspects of cybersecurity awareness and online safety behavior.

First, password security practices among students reveal significant vulnerability. **76.7% of respondents reported using the same password for multiple accounts**, and **48.3% rarely change their passwords while 25% never update them**. These behaviors substantially increase the risk of unauthorized access and data breaches. Prior cybersecurity studies consistently identify password reuse and infrequent updates as major contributors to account compromise, indicating that awareness does not always translate into safe practices.

Second, while some students adopt secure password practices, gaps remain in password strength awareness. Only **46.7% reported using passwords with numbers and special characters**, while **38.3% do not** and **15% are unsure**. This uncertainty suggests limited understanding of secure password construction, reinforcing findings from earlier research that users often overestimate their security practices.

Third, adoption of advanced security measures remains moderate. Only **41.7% enable Two-Factor Authentication**, while **35% do not use it and 23.3% are unaware of it**. Previous studies highlight multi-factor authentication as one of the most effective methods for preventing unauthorized access, indicating that increasing awareness in this area could significantly improve digital security.

Fourth, internet usage behaviors expose students to potential cyber risks. A majority of respondents connect to public Wi-Fi networks, with **31.7% often** and **50% sometimes using public Wi-Fi**. Although most students avoid installing apps from unknown sources (**78.3% do not install such apps**), inconsistent device update practices remain a concern, as **41.7% do not regularly update their devices**. Research indicates that outdated software and unsecured networks significantly increase vulnerability to cyber attacks.

Fifth, awareness of online threats shows mixed but encouraging results. While **71.7% of respondents have heard about phishing scams**, only **65% can identify suspicious messages**. Moreover, **48.3% admitted to clicking suspicious links at some point**, demonstrating that awareness does not always prevent risky behavior. This gap between knowledge and action is widely noted in cybersecurity literature.

Sixth, privacy protection practices among students remain inadequate. A majority (**63.3%**) do not check app permissions before installation, and **70% do not keep their social media accounts private**. These behaviors increase exposure to data misuse and privacy violations. Previous research similarly emphasizes that young users often underestimate privacy risks when sharing personal information online.

Seventh, real-world exposure to cyber incidents is evident. **40% of respondents reported experiencing account hacking directly or through someone they know**, highlighting the growing prevalence of cyber threats affecting students.

Finally, students strongly recognize the importance of cybersecurity awareness. A majority (**61.7%**) consider cybersecurity awareness very important, and **83.3% support conducting awareness programs in colleges**. This positive perception aligns with prior research suggesting that structured awareness programs can significantly improve cybersecurity practices and reduce risk behaviors.

Overall, the findings indicate that while students possess basic cybersecurity awareness, risky practices such as password reuse, public Wi-Fi usage, and inadequate privacy protection remain common. These results support existing research highlighting a gap between cybersecurity knowledge and actual safety behavior. Therefore, implementing cybersecurity awareness programs and promoting safe digital practices are essential to enhancing students online security.

8.FUTURE SCOPE

Although this study provides valuable insights into student cybersecurity awareness, several opportunities exist for further research and improvement.

Future studies can:

- Increase the sample size to include students from multiple colleges or universities for broader generalization.
- Compare cybersecurity awareness across different academic disciplines, age groups, or education levels.
- Conduct longitudinal studies to measure changes in awareness before and after cybersecurity training programs.
- Include qualitative methods such as interviews or open-ended responses to gain deeper insights into student perceptions and motivations.

9.CONCLUSION

This study examined cybersecurity awareness and online safety practices among college students using a structured survey of 60 respondents. The findings indicate that although students possess basic knowledge of cybersecurity concepts, several risky behaviors remain prevalent in daily digital activities.

A significant proportion of students reuse passwords, rarely update them, and do not consistently adopt strong authentication measures such as two-factor authentication. While awareness of phishing scams is relatively high, nearly half of the respondents admitted to clicking suspicious links at some point, highlighting a clear gap between awareness and practical behavior. Similarly, privacy protection practices such as checking app permissions and maintaining private social media accounts are not widely followed.

The results also show that students frequently use public Wi-Fi networks and do not always update their devices regularly, which increases exposure to cyber threats. At the same time, the majority of respondents recognize the importance of cybersecurity awareness and strongly support the introduction of awareness programs in colleges.

Overall, the study concludes that students demonstrate moderate cybersecurity awareness; however, inconsistencies in secure behavior indicate the need for structured education and awareness initiatives. Strengthening practical knowledge and encouraging safe digital habits can significantly reduce cybersecurity risks among students.

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to **Dr. Swati Joshi**, our research guide, for her continuous guidance, encouragement, and valuable suggestions throughout the development of this research work. Her support and insightful feedback helped us understand the subject more deeply and significantly improved the quality of this study.

We are truly thankful for her time, patience, and motivation during the entire research process. We would also like to thank the Department of Computer Science at PVG's College of Science and Commerce for providing a supportive academic environment and the necessary resources that helped us successfully complete this research work.

REFERENCES

[1] Bhatnagar, N., & Pry, M. (2020). Student attitudes, awareness, and perceptions of personal privacy and cybersecurity in the use of social media: An initial study. *Information Systems Education Journal (ISEDJ), 18*(1), 48-57.

[2] Molestane, T., & Tsibolane, P. (2020). Mobile information security awareness among students in higher education: An exploratory study. In *2020 Conference on Information Communications Technology and Society (ICTAS)* (pp. 1-6). IEEE.

[3] Moallem, A. (2019). Cyber security awareness among college students. In T. Z. Ahram & D. Nicholson (Eds.), *Advances in human factors in cybersecurity: Proceedings of the AHFE 2018 international conference on human factors in cybersecurity* (pp. 79-87). Springer International Publishing.

[4] Goliath, S., Tsibolane, P., & Snyman, D. (2025). Exploring the cybersecurity-resilience gap: An analysis of student attitudes and behaviors in higher education. In *Proceedings* (pp. 1-10).

[5] Kshetri, N., Vasudha, & Hoxha, D. (2023). knowCC: Knowledge, awareness of computer & cyber ethics between CS/non-CS university students. In *2023 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)* (pp. 504-510). IEEE.

[6] Sarita, K., Kaur, K., Kaur, P., & Kaur, S. (2022). Review of learning strategies for cybersecurity awareness among students in online teaching era. *Journal of Applied Technical and Educational Sciences, 12*(2), 1-12.

[7] Al Shabibi, A. M., & Al-Suqri, M. N. (2023). Cybersecurity awareness among students during the COVID-19 digital transformation of education: A case study at the Muscat (Oman) schools. In H. M. K. Al Naimiy, M. Bettayeb, H. M. Elmehdi, & I. Shehadi (Eds.), *Future trends in education post COVID-19: Teaching, learning and skills driven curriculum* (pp. 39-49). Springer Nature Singapore.

[8] Manohar, S. S., Garg, A., & Havaldar, A. (2023). Study of awareness of cyber security in educational organization. *International Journal of Advance Research, Ideas and Innovations in Technology, 9*(2), 1-7.

[9] Umerubab, Gul, H., Rahman, F., Aslam, S., Khan, S. M., & Bakht, M. (2025). Awareness of cybersecurity measures and students' academic performance. *The Psychology of Management and Organization, 23*(1), 1-11.

[10] Mittal, C. (2024). An empirical study on cybersecurity awareness, cybersecurity concern, and vulnerability to cyber-attacks. *IJSRM, 12*(4), EC-2024-1147.

[11] Benhsain, W., & Boujrouf, S. (2023). Cybersecurity awareness among students: A case study of three fields of study. *Journal of Education and Learning (EduLearn), 17*(3), 421-429.

[12] Shaikh, S. (2025). Cybersecurity awareness among students: A research review. *Scholarly Research Journal for Interdisciplinary Studies, 13*(81), 212-219.

[13] Al Zaidy, A. (2025). Measuring cybersecurity awareness of students: A study of state college students. *Journal of Information Technology, Cybersecurity, and Artificial Intelligence, 2*(1), 17-40.

[14] Hnaif, A. A., Derbas, A. M., & Almanasra, S. (2023). Cybersecurity integration in distance learning: an analysis of student awareness and attitudes. *Indonesian Journal of Electrical Engineering and Computer Science, 32*(2), 1057-1066.

[15] Bottyan, L. (2023). Cybersecurity awareness among university students. *Journal of Applied Technical and Educational Sciences, 13*(3), 1-11.