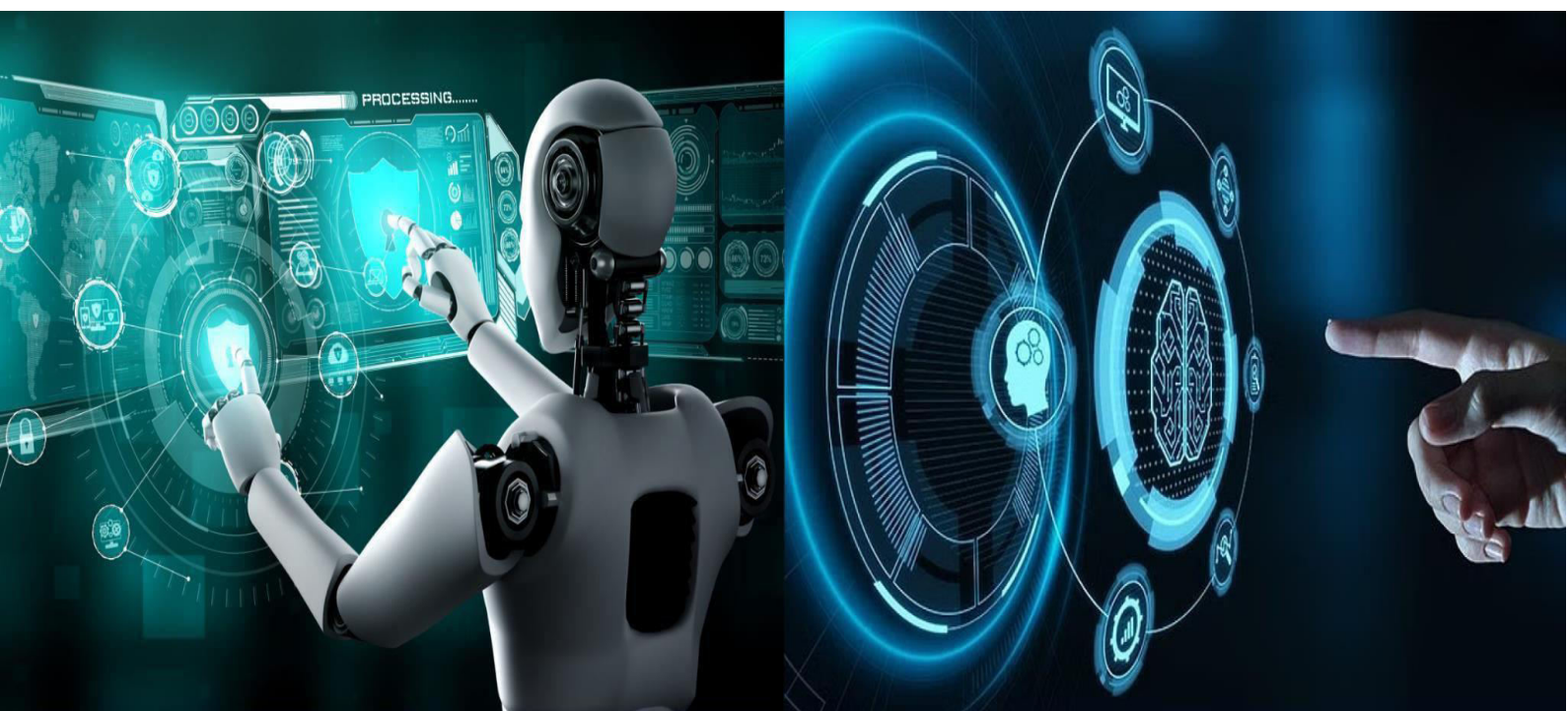


International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Cybersecurity Awareness among College Students

Vikram Sanjay Jadhav¹, Shamsundar Ashokrao Sable², Prajakta Ramchandra Badade³,
Aishwarya Ramesh Salunke⁴

Department of Master of Computer Application, Siddhant Institute of Computer Application, Savitribai Phule Pune University, Pune, Maharashtra, India¹⁻⁴

ABSTRACT: The quick use of digital technology in communication, education, and banking has made cybersecurity a global problem. Due to their heavy internet usage and lack of knowledge about online security procedures, college students are one of the most vulnerable demographics. Using a poll of 102 respondents, this study examines the degree of cybersecurity knowledge among college students. The study investigates how they respond to cyberthreats, use two-factor authentication, create secure passwords, and browse safely. The findings show that although students show a moderate understanding of cybersecurity fundamentals, dangerous practices including using the same password repeatedly, updating software irregularly, and not using 2FA are still common. The paper's conclusions point to the necessity of organized cybersecurity training, workshops, and institutional regulations in order to encourage students to use the internet in a safer manner.

KEYWORDS: Cybersecurity, Awareness, College Students, Phishing, Two-Factor Authentication, Safe Browsing, Cyber Threats, Education

I. INTRODUCTION

Cybersecurity has become a serious global concern in the current digital era. Students are particularly susceptible to cyber attacks because they depend on online platforms for social contact, banking, education, and communication. As digital natives, students commonly use public Wi-Fi, create weak passwords, and ignore software upgrades, among other risky behaviors. This study looks at college students' levels of cybersecurity awareness and finds discrepancies between their online conduct and security understanding. Recommending actions to raise awareness and build a more resilient student body is the goal.

II. RELATED WORK

Students' awareness of cybersecurity has been the subject of numerous studies. Despite having a significant level of digital exposure, Moallem [3] discovered that Silicon Valley pupils knew very little about cyberthreats. When Kumbhakar [1] studied Indian students in rural and urban regions, he found that the former had less awareness. Verma [6] emphasized the necessity of structured education programs and prevalent misconceptions among Indian students.

III. METHODOLOGY

The study used a quantitative and descriptive design. College students in a variety of subject areas were given a standardized Google Form questionnaire, and 102 of them responded. The survey evaluated the students' cybersecurity experiences, behaviors, and knowledge. Frequency counts, percentages, and graphical representations in the form of pie charts and bar graphs were used in the data analysis process.

IV. RESULTS AND DISCUSSION

Students' cybersecurity practices varied, according to the survey. Just 18% of respondents said they used strong, one-of-a-kind passwords, whereas 62% reused passwords across several accounts. 70% of people never enabled two-factor authentication, indicating a poor adoption rate. About 30% of respondents said they had been exposed to malware, while 48% said they had been the target of phishing efforts. Many students used public Wi-Fi or unprotected websites,



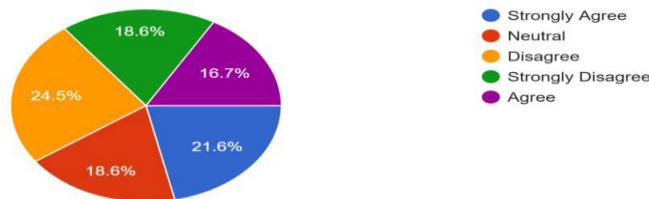
International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

demonstrating a lack of continuous adherence to safe browsing standards. These results imply that although students are aware of the dangers posed by cyberspace, their real-world procedures are still insufficient.

Figure 4.1: Password Practices Among Students (Pie Chart)

I regularly change my passwords.
102 responses



How students handle their internet account credentials is depicted in this image. Fewer people use strong, one-of-a-kind passwords, while many use the same ones for several accounts. A small percentage acknowledged using names or birthdays as weak, easily guessed passwords.

Interpretation: Students' vulnerability to account breaches is increased by the fact that password management is still one of the weakest aspects of cybersecurity hygiene.

Figure 4.2: Use of Two-Factor Authentication (2FA) (Pie Chart)

I enable two-factor authentication (2FA) on important accounts
102 responses

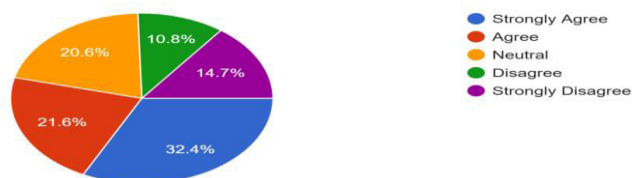


According to the 2FA adoption chart, the majority of students either don't enable 2FA or use it sporadically. Just a tiny portion of respondents said they enabled it for every account.

Interpretation: Students are reluctant to use 2FA because they are unaware of it or think it will be inconvenient, even though it is a widely accessible and efficient security mechanism.

Figure 4.3: Safe Browsing Practices (Pie Chart)

I check website security (HTTPS) before entering sensitive information.
102 responses





International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

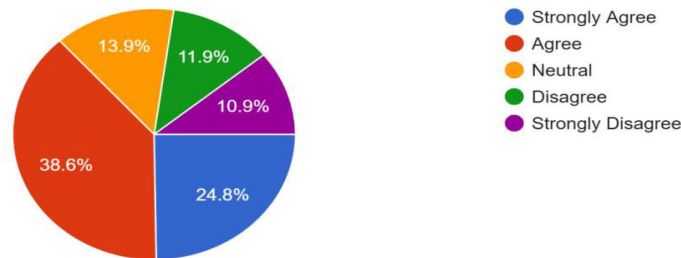
The usage of safe browsing practices, such as avoiding dubious links, confirming websites, or utilizing secure (HTTPS) platforms, is highlighted in this graph. Only a minority regularly adhered to these principles, and the majority acknowledged ignoring them.

Interpretation: Students continue to engage in unsafe browsing, which increases their risk of coming into contact with malware and phishing scams.

Figure 4.4: Updating of Software and Applications (Pie Chart)

I keep my devices and apps updated regularly.

101 responses



Only a small percentage of students update their devices on a regular basis, according to the software update practices figure. A significant percentage completely ignore updates, while many only update seldom and typically only when requested.

Interpretation: This shows a lack of knowledge of how machines with out-of-date software are vulnerable to viruses and attacks.

V. CONCLUSION

According to the survey, college students generally engage in risky behaviors including password reuse, neglecting software updates, and poor adoption of 2FA, while having a moderate understanding of cybersecurity fundamentals. Colleges could hold workshops, include cybersecurity sections into their curricula, and encourage gamified awareness tools in order to close these gaps. Policies like the requirement for 2FA on academic portals should also be enforced by institutions. In order to protect individual safety and create a workforce that is digitally resilient, it is imperative that students' awareness of cybersecurity be strengthened.

REFERENCES

- [1] P. Kumbhakar, 'Cybersecurity awareness among higher education students in India: A comparative study of rural and urban populations,' *Indian Journal of Educational Technology*, vol. 19, no. 3, pp. 110–125, 2025.
- [2] J. Bottyan, 'Cybersecurity awareness among university students,' *Journal of Information Security Education*, vol. 15, no. 2, pp. 45–56, 2023.
- [3] A. Moallem, 'Cybersecurity awareness among Silicon Valley students: Perceptions and practices,' *International Journal of Information Security and Privacy*, vol. 13, no. 4, pp. 1–16, 2019.
- [4] R. Hobbs, 'Cybersecurity awareness in higher education institutions: A study of faculty and staff training,' *International Journal of Cyber Studies*, vol. 11, no. 1, pp. 22–35, 2023.
- [5] CERT-In, 'Cybersecurity guidelines for students and educational institutions,' Computer Emergency Response Team – India, 2024. [Online]. Available: <https://www.cert-in.org.in>
- [6] V. Verma, 'Cybersecurity awareness among Indian college students,' *JJTU Journal of Computer Applications*, vol. 8, no. 1, pp. 55–65, 2023.
- [7] World Economic Forum, 'Global Risks Report: Cybersecurity and Digital Trust,' WEF Publications, 2024.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

 9940 572 462  6381 907 438  ijircce@gmail.com



www.ijircce.com

Scan to save the contact details