International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

An Analytical Study on Cybersecurity Awareness Among College Students

Rujuli R. Satao[1], Sakshi B. Panchalwar[2], Prof. A. J. Pimprikar[3]
[1,2,3]*MCA II yr Sem IV P.G. Dept of Computer Applications, PRMITR Badnera City-Amravati country-India*

***Abstract*--In today's digital era, college students heavily depend on the internet for academic, social, and personal activities. However, increasing cyber threats such as phishing, hacking, identity theft, and malware attacks have made cybersecurity awareness very important. This research paper presents an analytical study on the level of cybersecurity awareness among college students. The study focuses on students' knowledge about online threats, password security practices, social media privacy, and safe internet usage. The findings highlight that while students are active internet users, many lack proper awareness about cybersecurity measures. The paper also suggests strategies to improve awareness through training programs, workshops, and curriculum integration.**

***Keyword*-- Cybersecurity, Awareness, Phishing, Data Privacy, Online Safety, College Students**

I. Introduction

Nowadays, digital technology has become an important part of students' lives. College students use the internet for online classes, research, social media, banking, shopping, and communication. While technology makes life easier, it also increases the risk of cyber threats such as hacking, phishing, malware attacks, identity theft, and online fraud.

Cybersecurity means protecting computers, networks, and personal data from unauthorized access or cyber attacks. As the number of cybercrimes is increasing rapidly, students are becoming easy targets because they spend more time online and often lack proper awareness about digital safety.

Many college students use weak passwords, share personal information on social media, click on unknown links, and ignore software updates.

These unsafe practices can lead to serious consequences such as financial loss, data theft, and misuse of personal information.

Therefore, it is important to study and analyze the level of cybersecurity awareness among college students. Understanding their knowledge, behavior, and practices will help in identifying gaps and suggesting effective measures to improve digital safety.

Key Elements:

1. Knowledge of Cyber Threats:

Understanding phishing, hacking, ransomware, and malware.

2. Password Security:

Using strong passwords and enabling two-factor authentication.

3. Social Media Privacy:

Managing privacy settings and avoiding oversharing.

4. Safe Browsing Habits:

Avoiding suspicious links and unsafe downloads.

5. Reporting Mechanism:

Knowing how to report cybercrime.

II. Literature Review

- Artificial intelligence has been understood since 1956 [2] through different hypothetical understandings that are affected by various fields such as chemistry, biology, linguistics, mathematics, and advancements in AI solutions.
- Industrial Engineering Journal ISSN: 0970-2555 Volume: 52, Issue 5, May: (2023) Research has shown that AI has the potential to transform education in several ways.
  For example, AI can be used to create personalized learning experiences that cater to the individual needs of each student.
- Kristina Ishmael Deputy Director, Office of Educational Technology May 2023, AI can be defined as "automation based on associations." When computers automate reasoning based on associations in data (or associations deduced from expert knowledge), two shifts fundamental to AI occur and shift computing beyond conventional edtech: (1) from capturing data to detecting patterns in data and (2) from providing access to instructional resources to automating decisions about instruction and other educational processes.
- Miguel A. Cardona, Ed.D. Secretary, U.S. Department of Education Roberto J. Rodríguez Assistant Secretary, Office of Planning, Evaluation, and Policy Development may 2023 AI may enable achieving educational priorities in better ways, at scale, and with lower costs.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

Addressing varied unfinished learning of students due to the pandemic is a policy priority, and AI may improve the adaptivity of learning resources to students' strengths and needs. Improving teaching jobs is a priority, and via automated assistants or other tools

III. Research Methodology

This research uses a survey-based method to collect data from college students. A structured questionnaire was designed including questions about:

- Password usage habits
- Awareness of phishing attacks
- Knowledge of two-factor authentication
- Use of antivirus software
- Social media privacy settings

The data was collected through Google Forms and analyzed using percentage and graphical representation methods. The study used simple statistical tools to interpret awareness levels.

Fig.3.1 Data Collection and Analysis Process

IV. Data Analysis And Interpretation

The collected data revealed the following key findings:

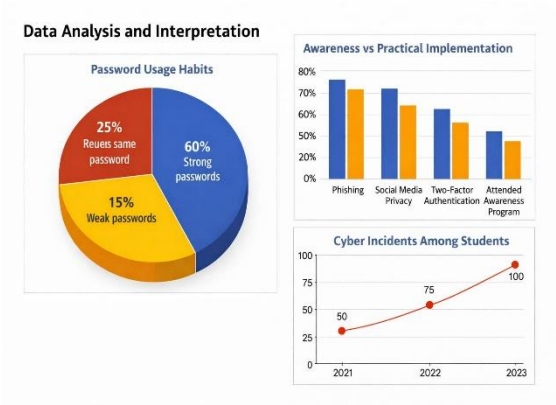
75% of students are aware of phishing but only 40% can correctly identify fake emails.

60% use strong passwords, while 25% reuse the same password across multiple platforms.

70% students use social media privacy settings, but many are unaware of advanced privacy controls.

Only 35% have attended any cybersecurity awareness program.

The analysis shows moderate awareness but a lack of practical knowledge. Many students know about threats but do not follow secure practices consistently.



V. Problem Statement

The major findings of this study are:

- Students have basic knowledge of cybersecurity.
- Practical application of security measures is low.
- Awareness programs are not regularly conducted in colleges.
- Students are vulnerable to phishing and social engineering attacks.

The findings suggest a gap between theoretical knowledge and practical implementation.

VI. Suggestion and Recommendation

Based on the study, the following recommendations are suggested:

- Colleges should conduct regular cybersecurity workshops.
- Awareness sessions should include live demonstrations of cyber attacks.
- Students should be trained to use two-factor authentication.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435 (Online) Volume 15, Issue 04, April 2026)

- Cybersecurity topics should be included in academic curriculum.
- Institutions should collaborate with cybersecurity experts for training sessions.

These measures can significantly improve cybersecurity awareness among students.

Fig.6.1

VII. Challenges In Personalized And Online Learning

- *Technological Barriers:* Not all students have equal access to the internet or devices.
- The digital divide can widen inequalities in education.
- *Teacher Training:* Educators must be trained to effectively use digital tools and platforms.
- *Self-Discipline:* Online learning requires a high level of motivation and self-regulation, which can be challenging for some students.

VIII. The Future Of Education

Hybrid Models:

- We will likely see a blend of traditional in-person and online education, offering the best of both worlds.
- Schools may incorporate more personalized learning techniques through online platforms, allowing teachers to focus on higher-order skills like critical thinking.

Artificial Intelligence:

- AI can help create highly customized learning experiences, providing personalized recommendations and insights.

Global Collaboration:

- Online platforms allow learners from around the world to connect and collaborate, breaking down geographic barriers.

Continuous Learning:

- The future will emphasize lifelong learning, with online platforms providing continuous education opportunities beyond traditional school years.

IX. Future Scope Online Learning

- There may come a time decade in the future where AI will be advanced enough to provide a personalized learning experience, but we are nowhere near that yet.
- The younger the student the more crucial the traditional learning set up is necessary with a teacher present to facilitate learning.
- The pre-K "student", the Kindergartner, and all of the elementary school aged kids plus all but a handful of middle schoolers need that communal approach to learning with a human teacher present.
- Thousands of years of evolution have baked in this need to socialize while learning and screen time is a terribly poor way for most people (including adults) to learn.

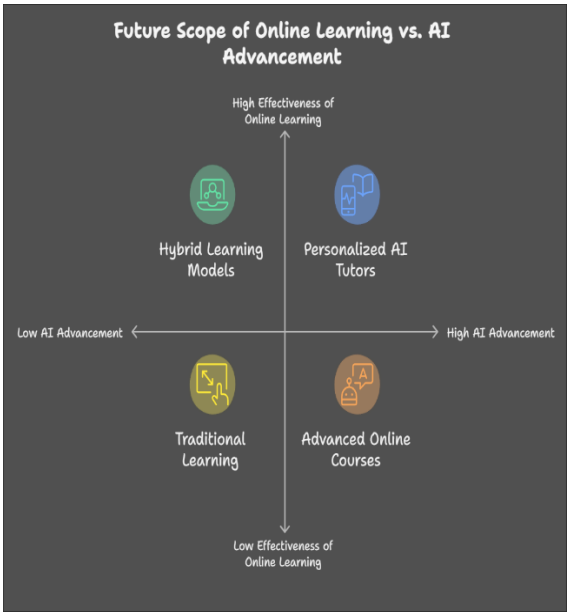


Fig.9.1 Future scope of online vs. AI advancement

- "Pandemic learning" via Zoom has proven that online learning for a great percentage of students (all the way up through most of high schoolers) was vastly inferior to classroom learning. There was no one on the students' side of the screen to 'make' them learn. The vast majority of kids have no innate drive to focus and learn. The older the student, the greater possibility (not probability) that learning online can be as effective as learning in a classroom.

X. Conclusion

Summary: Personalized learning and online education are reshaping the future of education. These innovations promise more engaging, accessible, and efficient learning experiences.

Looking Ahead: The future of education will likely be hybrid, combining the flexibility of online learning with the personal touch of in-person guidance.

REFERENCES

[1] Kumaraguru, P., Rhee, Y., Sheng, S., et al. (2010). Teaching Johnny Not to Fall for Phish: A Phishing Awareness Study. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

[2] Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. Computers & Security, 66, 40–51.

[3] Bada, M., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour? International Conference on Cyber Security for Sustainable Society.

[4] Furnell, S., & Clarke, N. (2012). Power to the People? The Evolving Recognition of Human Aspects of Security. Computers & Security, 31(8), 983–988.

[5] Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Environment. Journal of Information Security.

[6] Hadlington, L. (2017). Human Factors in Cybersecurity; Examining the Link Between Internet Addiction, Impulsivity, Attitudes Towards Cybersecurity, and Risky Cybersecurity Behaviours. Heliyon.

[7] Manohar, S. S., Garg, A., & Havaldar, A. (2023). Study of Awareness of Cyber Security in Educational Organizations. International Journal of Advance Research, Ideas and Innovations in Technology.

[8] Mittal, C. (2024). An Empirical Study on Cybersecurity Awareness and Vulnerability to Cyber Attacks. International Journal of Scientific Research and Management

[9] Putri, A. A. (2024). Cybersecurity Awareness: A Literature Review on Internet Users' Awareness and Safe Behavior. Journal of Artificial Intelligence and Engineering Applications.

[10] Kshetri, N. (2023). Cybersecurity Awareness and Education Among University Students. International Journal of Information Management.