www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 03, March 2025, pp : 1160-1167

e-ISSN : 2583-1062
Impact Factor : 7.001

ANALYZING CYBERSECURITY AWARENESS AND PRACTICES ACROSS DEMOGRAPHICS: INSIGHTS FROM A SURVEY STUDY

Dr. Sonam Kaushik[1], Mr. Pramod Kumar Pahal[2], Mr. Dhairya Nidhi[3]

[1]Assistant Professor, BCA, Maharaja Surajmal Institute, Delhi- 110058, India.

[2,3]Student, BCA, Maharaja Surajmal Institute, Delhi- 110058, India.

ABSTRACT

In today's digital age, cyber threats are evolving unprecedentedly, turning awareness into a frontline defence against attacks. Our study explores how college students perceive and handle these risks by exploring their everyday digital habits, knowledge gaps, and potential weak spots. Through a survey spanning multiple academic fields, we examined not only how students recognize online dangers but also whether they consistently apply safeguards like strong passwords or phishing detection. What emerged was a clear picture: many lack crucial knowledge about basic security practices, leaving them exposed. These insights highlight an urgent need for universities to rethink their approach—integrating hands-on cybersecurity training and updating policies to bridge the gap between theoretical knowledge and real-world safety.

1. INTRODUCTION

In today's digital world, where nearly every aspect of life relies on technology, cybersecurity is more important than ever. From online banking and social media to educational platforms and remote work, individuals constantly interact with digital systems that store personal and sensitive information. However, as technology evolves, so do cyber threats. Phishing scams, ransomware attacks, identity theft, and data breaches have become increasingly common, affecting millions of users worldwide. Despite these risks, many individuals still lack proper knowledge of cybersecurity best practices, making them vulnerable to attacks.

One of the biggest challenges in improving cybersecurity awareness is the fact that knowledge and practices vary widely across different groups of people. Factors such as **age, education, field of study, and internet usage habits** play a crucial role in shaping an individual's cybersecurity behavior.

For example, younger individuals who grew up with technology may be more comfortable navigating online security settings, while older users might struggle with identifying phishing scams. Similarly, students in technical fields such as computer science may have better cybersecurity habits compared to those in non-technical disciplines. Understanding these differences is essential to developing targeted awareness programs that effectively address gaps in cybersecurity knowledge.

This study, titled **"Analyzing Cybersecurity Awareness and Practices Across Demographics: Insights from a Survey Study,"** seeks to explore how different groups of individuals perceive and practice cybersecurity. Using survey data, we examine key factors such as **password management, two-factor authentication (2FA) usage, awareness of cyber threats, experiences with online scams, and social media privacy habits.** By analyzing responses from participants across various demographics, we aim to identify common trends, risky behaviors, and areas where cybersecurity education is most needed.

1.1 Research Objectives

The primary objectives of this research are to:

- Evaluate the overall level of cybersecurity awareness among different demographic groups.
- Analyze common security practices such as password habits, 2FA adoption, and social media privacy settings.
- Understand the impact of demographics (age, education, field of study) on cybersecurity behaviors.
- Identify areas where cybersecurity training and awareness programs need improvement.

The insights from this study will be useful for educators, policymakers, and cybersecurity professionals working to improve online safety. By understanding how cybersecurity awareness differs among various groups, we can create more effective educational programs and policies that help individuals protect themselves in an increasingly digital world. The goal is not just to highlight existing issues but to encourage a culture of **proactive cybersecurity practices** that safeguard personal and professional digital environments.

2. METHODOLOGY

To analyze cybersecurity awareness and practices across different demographics, a structured research methodology was adopted. This section outlines the research design, data collection methods, participant demographics, and data analysis techniques used in the study.

2.1 Research Design

This study follows a quantitative research approach using a survey-based method to collect data from participants. The survey was designed to assess cybersecurity knowledge, security practices, awareness of cyber threats, and personal experiences with cybersecurity incidents. The primary goal was to identify patterns and variations in cybersecurity awareness across different demographic groups.

2.2 Data Collection

- Survey Instrument: A structured questionnaire was developed to gather responses from participants. The survey included multiple-choice questions, Likert scale-based questions, and open-ended responses to capture a comprehensive understanding of cybersecurity awareness and practices.
- Survey Distribution: The survey was distributed online through digital platforms such as Google Forms, email, and social media to reach a diverse group of respondents.
- Survey Duration: The data collection phase lasted a month, ensuring a sufficient number of responses for meaningful analysis

2.3 Participant Demographics

- Target Population: The study focused on college students from various academic backgrounds, as they represent a key demographic that is highly active in the digital space.
- Size: A total of 1000 responses were collected, ensuring a diverse representation of age groups, educational backgrounds, and technology usage habits.
- Demographic Factors Considered: The survey collected information on age, gender, field of study, level of education, and frequency of internet use to analyze how these factors influence cybersecurity awareness.

2.4 Data Analysis

- Descriptive Analysis: The collected data was processed using statistical and visualization tools to identify trends and patterns. Bar charts, pie charts, and frequency tables were used to present key findings.
- Comparative Analysis: Responses were grouped based on demographic factors to compare cybersecurity awareness levels across different segments.
- Correlation Analysis: Statistical techniques were used to assess the relationship between cybersecurity knowledge and security behaviors, such as password management and 2FA adoption.

2.5 Ethical Considerations

- Informed Consent: Participants were informed about the purpose of the study, and their participation was voluntary.
- Anonymity and Confidentiality: No personally identifiable information was collected, ensuring data privacy and confidentiality.
- Academic Integrity: The study adhered to ethical research guidelines and ensured that all data was used solely for academic purposes.

This methodology provides a structured approach to understanding cybersecurity awareness across demographics, ensuring that the findings are both reliable and actionable for improving cybersecurity education and practices.

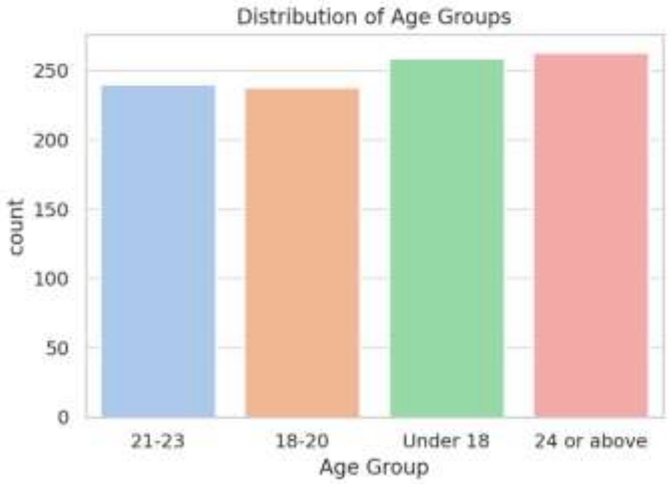
3. FINDINGS AND ANALYSIS

This section presents the key findings from the survey on cybersecurity awareness and practices among different demographic groups. The analysis focuses on various aspects such as cybersecurity knowledge, training, password habits, two-factor authentication (2FA) usage, cyber threat awareness, and experiences with cyber attacks. The results highlight both strengths and areas for improvement in cybersecurity practices.

3.1 Demographic Distribution of Respondents

The survey collected responses from individuals across various age groups, educational backgrounds, and fields of study. The majority of respondents belonged to the 18-24 age group, which is expected as the study primarily focused on college students.

Key Insight: Younger individuals tend to have greater exposure to digital platforms, but this does not necessarily translate to better cybersecurity practices**.**

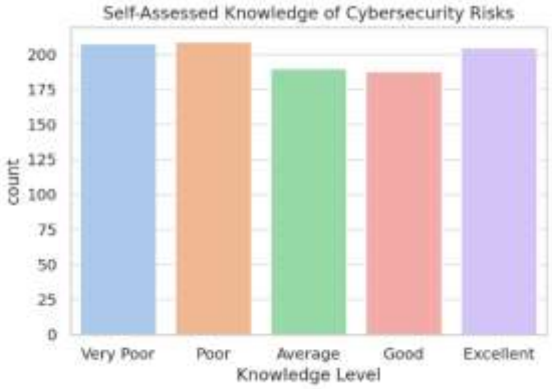


3.2 Cybersecurity Knowledge and Awareness

Participants were asked to rate their knowledge of cybersecurity concepts such as malware, phishing, ransomware, and identity theft.

- Majority of respondents rated their cybersecurity knowledge as "Very Poor" or "Poor."
- A fine percentage considered themselves highly knowledgeable, while some admitted to having good or average of cybersecurity threats.

Key Insight: Despite living in a technology-driven era, many students lack comprehensive cybersecurity awareness, suggesting a need for better education in this domain.

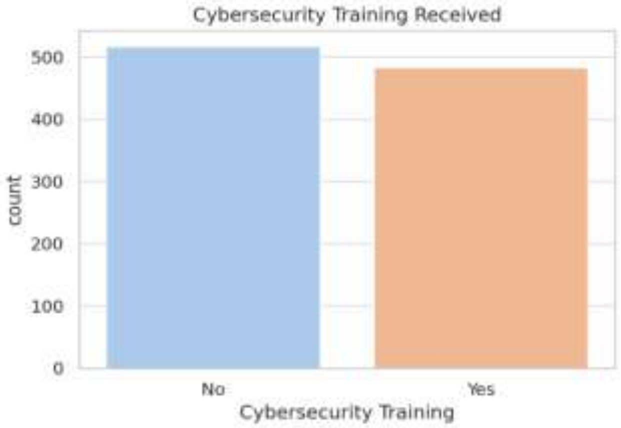


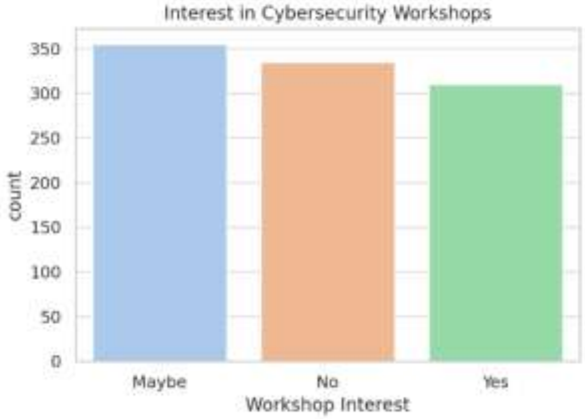
3.3 Cybersecurity Training and Education

The survey also examined whether respondents had received formal cybersecurity training.

- A significant portion of respondents (over 50%) reported that they had never received any formal cybersecurity training.
- Those who had undergone training demonstrated higher awareness and better security habits.

Key Insight: There is a clear gap in cybersecurity education that institutions need to address through awareness programs and workshops.



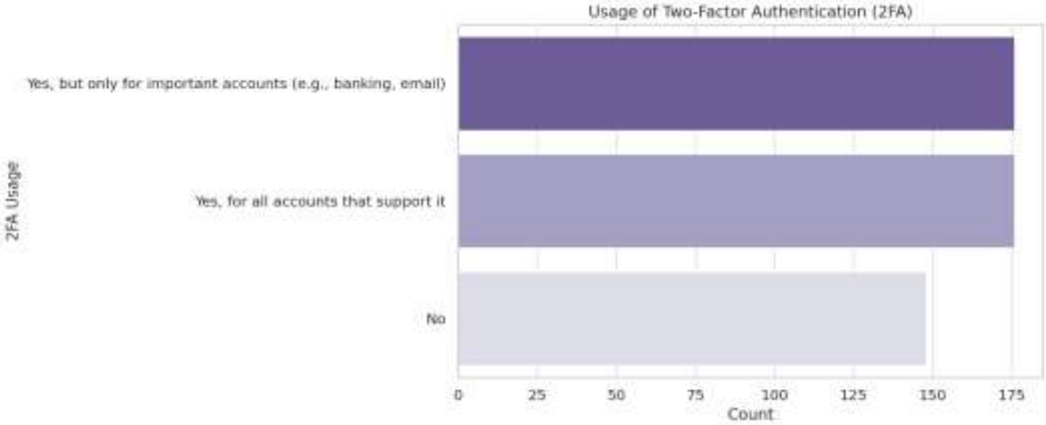


3.4 Use of Two-Factor Authentication (2FA)

The adoption of **two-factor authentication (2FA)** is considered a crucial security practice. The survey results show:

- **Only a moderate percentage of respondents use 2FA across all their online accounts.**
- Some respondents reported enabling 2FA only for financial or sensitive accounts, while others admitted they never use it.

Key Insight: While 2FA is widely recommended, many users still do not enable it across all accounts, leaving them vulnerable to cyber threats.

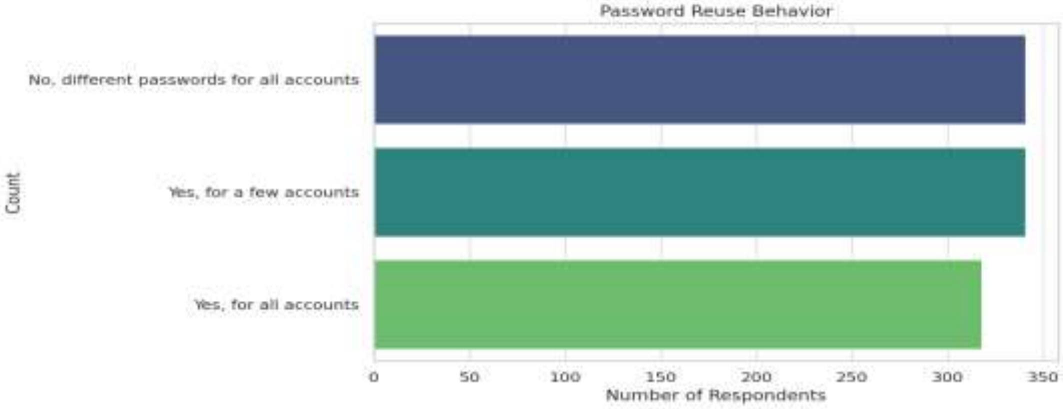


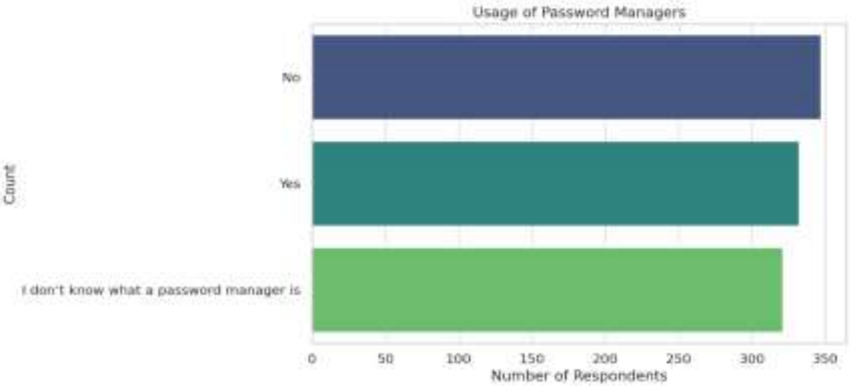
3.5 Password Management Practices

Strong password habits are essential for cybersecurity, yet the survey revealed concerning trends:

- **A large number of respondents reuse passwords across multiple accounts, increasing their risk of cyber-attacks.**
- Many respondents admitted they only change passwords when forced to do so.
- Some students use weak passwords, such as birthdays or simple word combinations, making them easy targets for attackers.

Key Insight: Poor password management remains a common issue, highlighting the need for stronger security measures like password mangers and regular password updates.



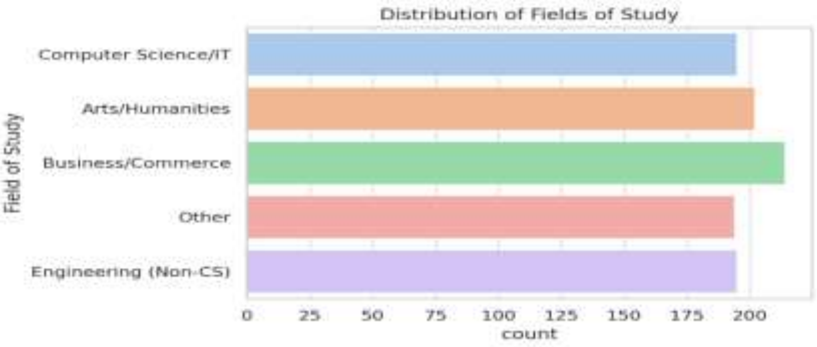


3.6 Familiarity with Cyber Threats

Respondents were asked to identify cyber threats they were familiar with. The most recognized threats included:

- Phishing, Ransomware, and Identity Theft were among the most well-known threats.
- Less awareness was observed for threats like Social Engineering, Man-in-the-Middle attacks, and Keylogging.

Key Insight: While students are familiar with common cyber threats, awareness of more sophisticated attacks remains low, making them potential targets.



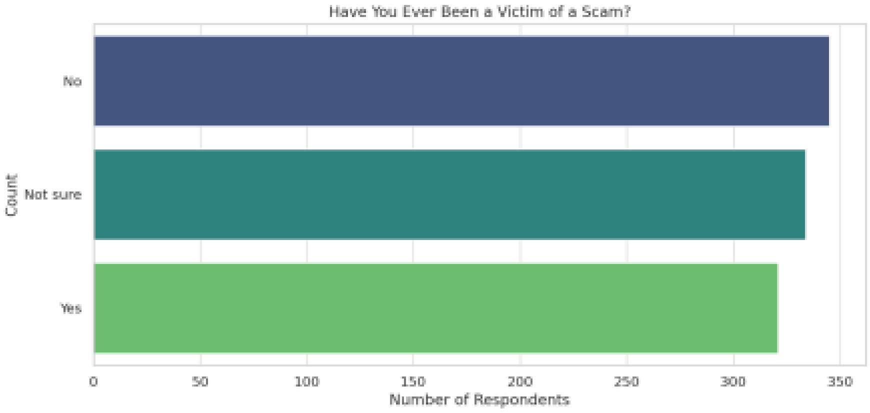
3.7 Experiences with Cyber Attacks and Biggest Challenges

The survey also examined how many respondents had personally experienced cyber threats and faced challenges.

- **A noticeable percentage reported being victims of cyber-attacks such as phishing attempts and social media hacks.**
- Those who had experienced cyber threats were more likely to adopt better security practices afterward.
- Lack of awareness or education on cybersecurity best practices.
- Difficulties in remembering multiple strong passwords.
- Overconfidence in their ability to identify and avoid cyber threats.
- Neglecting security measures due to convenience or time constraints.

Key Insight: Experiencing a cyber-attack serves as a wake-up call, reinforcing the importance of cybersecurity measures. However, proactive education is needed to prevent such incidents before they occur.

Many users struggle with cybersecurity due to a mix of knowledge gaps, convenience-based choices, and overconfidence in their digital skills.



4. DISCUSSION

The findings from this study reveal a significant gap between cybersecurity awareness and actual security practices among college students. While many respondents recognize the importance of cybersecurity, their behaviors suggest a lack of consistent protective measures. One of the most concerning trends is the **absence of formal cybersecurity education**, leaving students to rely on self-learned or trial-and-error approaches to online security. Without structured guidance, many develop habits that expose them to risks, such as weak passwords, password reuse, and neglecting essential security measures like two-factor authentication (2FA).

Another key issue is **poor password management**, with many students admitting they only change passwords when forced to do so or reuse the same passwords across multiple accounts. This makes them vulnerable to credential-stuffing attacks, where a compromised password from one account can lead to breaches in others. Additionally, while students frequently use online platforms for academic and personal activities, **many are unaware of advanced cyber threats** such as social engineering attacks and man-in-the-middle attacks, further increasing their risk of being targeted.

To address these challenges, universities should take an active role in promoting cybersecurity awareness. Integrating **cybersecurity training into the academic curriculum** or conducting regular workshops can help students develop better security habits. Hands-on learning experiences, such as simulated phishing exercises or password security demonstrations, can make cybersecurity education more engaging and effective.

Ultimately, improving cybersecurity practices among college students requires more than just awareness—it demands a proactive approach that encourages responsible digital behavior. By fostering a culture of cybersecurity consciousness, institutions can help students protect themselves against online threats and develop habits that will benefit them in the long run.

5. RECOMMENDATION

Based on the findings of this study, several steps can be taken to improve cybersecurity awareness and practices among college students. Addressing these issues requires a collaborative effort from universities, educators, students, and policymakers to ensure a safer digital environment. The following recommendations outline key actions that can help bridge the gap between cybersecurity awareness and effective security practices:

1. **Integrate Cybersecurity Education into the Curriculum**

- Universities should introduce mandatory cybersecurity courses or workshops to educate students on digital safety.
- Including hands-on activities such as simulated phishing attacks, secure password management techniques, and data privacy exercises will enhance practical learning.
- Cybersecurity literacy should be incorporated into general IT courses to ensure that students from all disciplines gain essential knowledge.

2. **Promote the Use of Strong Authentication Methods**

- Institutions should encourage students to enable two-factor authentication (2FA) across all online accounts, especially for academic and financial platforms.
- Campaigns highlighting the risks of weak passwords and providing password management best practices should be conducted regularly.
- Universities can collaborate with cybersecurity organizations to offer students access to free or discounted password managers to enhance security.

3. **Conduct Regular Cybersecurity Awareness**

- Hosting seminars, webinars, and workshops on topics such as phishing detection, social engineering threats, and safe online practices can improve student awareness.
- Engaging students through interactive awareness drives, competitions, and gamified cybersecurity challenges can make learning more effective.
- Institutions should send monthly cybersecurity tips via email or student portals to reinforce best practices.

4. **Establish a Cybersecurity Help Desk or Support Team**

- Universities should create a dedicated cybersecurity support center where students can report security concerns and receive expert guidance.
- Offering real-time assistance for issues such as phishing attempts, account breaches, or malware infections can help students take immediate action.
- Cybersecurity clubs or student-led initiatives can be formed to spread awareness and assist peers in adopting secure practices.

5. Encourage Proactive Cybersecurity Habits Among Students

- Students should be trained to regularly update their software and applications to protect against vulnerabilities.
- Educational institutions should promote the principle of least privilege, teaching students to limit personal information shared online and adjust privacy settings on social media.
- Encouraging ethical hacking and responsible disclosure programs can help students develop an interest in cybersecurity and contribute to digital safety.

6. Strengthen Collaboration with Cybersecurity Experts and Organizations

- Universities should partner with cybersecurity firms, government agencies, and tech companies to provide students with up-to-date security insights and resources.
- Internship programs and mentorship opportunities with cybersecurity professionals can help students gain real-world experience and develop industry-relevant skills.
- Joint initiatives between educational institutions and cybersecurity organizations can lead to the development of comprehensive training modules tailored for students.

6. FUTURE RESEARCH DIRECTION

While this study provides valuable insights into cybersecurity awareness and practices among college students, there is still much to explore in this rapidly evolving field. As cyber threats become more sophisticated, future research should focus on identifying emerging risks, evaluating the effectiveness of cybersecurity education, and exploring innovative solutions to enhance digital security. The following directions can help expand the scope of cybersecurity research:

1. Longitudinal Studies on Cybersecurity Awareness

- Future research could conduct long-term studies to track how cybersecurity awareness and behaviors change over time.
- Examining how students' cybersecurity habits evolve as they transition from college to professional environments could provide insights into lifelong digital security practices.

2. Assessing the Impact of Cybersecurity Training Programs

- Evaluating the effectiveness of different cybersecurity training methods, such as gamified learning, interactive simulations, and traditional lectures, can help determine the most impactful approaches.
- Studies should analyze whether formal cybersecurity training leads to sustained behavioral changes in students' online security

3. Exploring the Role of Artificial Intelligence (AI) in Cybersecurity Awareness

- Investigating how AI-powered cybersecurity tools can assist students in identifying and preventing cyber threats.
- Exploring chatbots, AI-driven phishing detectors, and automated security alerts as potential solutions for improving cybersecurity education.

4. Cybersecurity Challenges in Remote Learning and Hybrid Education

- With the rise of online learning platforms and remote education, research should focus on the new cybersecurity risks associated with virtual classrooms.
- Identifying security vulnerabilities in e-learning platforms and developing best practices for students and educators can strengthen cybersecurity in academic settings.

5. Behavioral and Psychological Aspects of Cybersecurity

- Future studies could examine the psychological factors influencing cybersecurity behaviors, such as risk perception, overconfidence in security knowledge, and resistance to adopting best practices.
- Research into how peer influence, social norms, and digital literacy levels impact cybersecurity habits among different demographic groups.

6. Cross-Cultural and Global Comparisons of Cybersecurity Awareness

- Comparing cybersecurity awareness levels across different countries, cultures, and educational systems could offer a broader understanding of global cybersecurity challenges.
- Identifying best practices from institutions that have successfully implemented effective cybersecurity policies and adapting them to other regions.

7. Ethical Hacking and Student Engagement in Cybersecurity Research

- Encouraging research on ethical hacking, penetration testing, and responsible disclosure programs as educational tools for students.

- Exploring the potential of student-led cybersecurity initiatives and their impact on fostering a proactive security culture on college campuses.

7. CONCLUSION

Cybersecurity is an essential aspect of digital life, yet this study highlights **significant gaps in awareness and security practices among college students**. While most students recognize the importance of online safety, many still engage in risky behaviors, such as weak password management, neglecting two-factor authentication (2FA), and lacking awareness of advanced cyber threats. The absence of formal cybersecurity education further contributes to these vulnerabilities, leaving students unprepared to handle potential cyber risks effectively.

One of the most concerning findings is that **many students have never received formal cybersecurity training**, which directly impacts their ability to protect personal and sensitive information. Without structured learning, students are left to navigate online security based on their own experiences, often leading to unsafe practices. Additionally, **password reuse and infrequent updates remain widespread**, making students easy targets for cyber attacks.

To bridge this gap, it is crucial for educational institutions to **prioritize cybersecurity education** by integrating training programs, workshops, and real-world cybersecurity simulations into the curriculum. Providing students with **practical, hands-on learning experiences**—such as phishing awareness exercises and secure password management techniques—can significantly improve their ability to recognize and respond to cyber threats.

Moving forward, raising cybersecurity awareness should be a **shared responsibility** among students, educators, and policymakers. By fostering a culture where cybersecurity is seen as a daily habit rather than an afterthought, students can develop stronger, more proactive security behaviors that will benefit them throughout their academic and professional lives. Strengthening cybersecurity literacy today will create a more resilient digital society in the future.

8. REFERENCE

[1] Al-Janabi, S., & Al-Shourbaji, I. (2016). A study of cybersecurity awareness among college students in the Middle East. Journal of Information Security and Applications, 29, 78–84.

[2] Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 386–408.

[3] Jansen, J., & Van Schaik, P. (2018). Testing a model of precautionary online behavioral intentions. Computers in Human Behavior, 87, 371–383.

[4] Kumar, N., & Singh, A. (2021). Assessing cybersecurity literacy among university students: A survey-based study. International Journal of Cyber Research, 5(2), 112–130.

[5] National Institute of Standards and Technology (NIST). (2020). Framework for improving critical infrastructure cybersecurity. Retrieved from https://www.nist.gov/cyberframework

[6] Ponemon Institute. (2021). The state of cybersecurity in higher education: Challenges and recommendations. Cybersecurity Report 2021.

[7] Renaud, K., & Dupuis, M. (2019). Cybersecurity education and behavior: Understanding barriers to adopting strong passwords. Computers & Security, 83, 105–123.

[8] Sharma, P., & Gupta, R. (2022). Evaluating the effectiveness of cybersecurity training programs for students. Cybersecurity & Privacy Journal, 3(1), 55–70.

[9] Verizon. (2023). Data breach investigations report: Key trends in phishing and password security. Retrieved from https://www.verizon.com/dbir

[10] Yeboah-Boateng, E. O., & Amanor, P. (2014). Phishing, SMiShing & Vishing: Understanding and preventing digital fraud in higher education institutions. International Journal of Cybersecurity, 7(3), 215–231.

[11] On-ground Survey (2025). Analyzing cybersecurity awareness and practices across demographics: Insights from a survey study. Internal research data.