Research Paper IMPACT FACTOR VALUE : 6.247 | E-ISSN NO : 2455-295X | VOLUME : 12 | ISSUE : 6 | JUNE 2026

A STUDY OF CYBER SECURITY AWARENESS AND PRACTICES AMONG UNIVERSITY STUDENTS

REENA RANI [1]

[1] ASSISTANT PROFESSOR, P.G. DEPARTMENT OF COMPUTER SCIENCE, SHRI JAIN P.G. COLLEGE, BIKANER.

ABSTRACT:

The rapid growth of digital technologies and internet usage has transformed higher education by enabling online learning, digital communication, and cloud-based academic services. However, increased reliance on digital platforms has also exposed university students to various cyber threats, including phishing attacks, malware infections, identity theft, data breaches, and social engineering scams. This study examines the level of cyber security awareness and the cyber security practices adopted by university students. The research highlights students' understanding of cyber threats, password management habits, online privacy concerns, and safe internet usage behaviors. The findings indicate that while students possess basic knowledge of cyber security concepts, significant gaps remain in the practical application of security measures. The study recommends implementing structured cyber security education programs and awareness campaigns within universities to strengthen students' digital safety and resilience against cyber threats.

KEYWORDS:

CYBER SECURITY, AWARENESS, UNIVERSITY STUDENTS, ONLINE SAFETY, DIGITAL LITERACY, INFORMATION SECURITY, CYBER THREATS.

PAPER ACCEPTED DATE:	PAPER PUBLISHED DATE:
13th June 2026	14th June 2026

1. INTRODUCTION

The rapid advancement of information and communication technologies (ICT) has transformed nearly every aspect of modern society, including the education sector. Universities and higher educational institutions have increasingly adopted digital technologies to enhance teaching, learning, research, administration, and communication processes. The widespread availability of the internet, smartphones, cloud computing, online learning platforms, and social networking sites has enabled students to access educational resources anytime and anywhere. Particularly after the global shift toward online and hybrid learning environments, students have become more dependent on digital platforms for academic and personal activities.

While digital transformation has brought numerous benefits such as improved accessibility, efficiency, and collaboration, it has also introduced significant cyber security challenges. As students spend more time online, they become potential targets for various cyber threats, including phishing attacks, malware infections, ransomware, identity theft, online fraud, social engineering attacks, and unauthorized access to personal data. Cybercriminals often exploit users' lack of awareness and poor security practices to gain access to sensitive information, financial accounts, and institutional networks.

Cyber security refers to the collection of technologies, policies, practices, and measures designed to protect computers, networks, software, and data from cyber threats and unauthorized access. In the context of higher education, cyber security is particularly important because universities store vast amounts of sensitive information, including academic records, research data, financial information, and personal details of students and staff. A security breach can result in financial losses, reputational damage, disruption of academic activities, and compromise of confidential information.

University students constitute one of the most active groups of internet users. They regularly engage with email services, online banking, social media platforms, e-commerce websites, learning management systems, and cloud-based applications. Despite their familiarity with technology, many students lack adequate cyber security knowledge and often underestimate the risks associated with their online behavior. Common unsafe practices include using weak passwords, reusing passwords across multiple accounts, sharing personal information on social media, connecting to unsecured public Wi-Fi networks, ignoring software updates, and failing to recognize phishing attempts. Such behaviors increase their vulnerability to cyberattacks.

In recent years, governments, educational institutions, and cyber security organizations have emphasized the

importance of developing cyber security awareness programs to strengthen digital resilience. Universities are increasingly expected to educate students not only in their academic disciplines but also in responsible and secure technology usage. Understanding students' current levels of awareness and their actual cyber security practices is necessary for designing effective educational interventions and training programs.

2. OBJECTIVES OF THE STUDY

- **To Assess the level of Cyber Security Awareness:**The foremost objective of this study is to assess the level of cyber security awareness among university students. As digital technologies have become an integral part of academic and personal life, it is important to understand how well students comprehend cyber security concepts, online risks, and protective measures. This objective focuses on evaluating students' knowledge of cyber security fundamentals and their awareness of the importance of maintaining digital safety.
- **To Examine Awareness of Common Cyber Threats:**Another key objective is to evaluate students' understanding of common cyber threats such as phishing attacks, malware, ransomware, identity theft, social engineering, and data breaches. The study seeks to determine whether students can recognize these threats and understand their potential consequences on personal, academic, and financial information.
- **To Analyze Cyber Security Practices:**The study aims to examine the cyber security practices adopted by university students in their daily digital activities. This includes investigating how students manage passwords, protect their devices, update software, use antivirus programs, and secure their online accounts. Understanding these practices will help identify whether students apply safe behaviors while using digital technologies.
- **To Evaluate Online Privacy and Data Protection Awareness:**With the increasing use of social media and online platforms, protecting personal information has become a significant concern. This objective focuses on assessing students' awareness of privacy settings, data protection measures, and responsible sharing of personal information online. The study seeks to determine the extent to which students prioritize privacy and take precautions to safeguard their digital identities.
- **To Identify the Relationship Between Awareness and Behavior:**The study also aims to examine the relationship between cyber security awareness and actual online behavior. While students may possess theoretical knowledge about cyber security, they may not always translate this knowledge into practice. This objective seeks to identify gaps between awareness and behavior and understand how knowledge influences security-related decision-making.
- **To Assess the Effectiveness of Cyber Security Education:**This study seeks to evaluate the effectiveness of cyber security education, training programs, workshops, and awareness campaigns conducted by educational institutions. It aims to determine whether such initiatives contribute to improving students' understanding of cyber security risks and encourage safer online practices.

3. LITERATURE REVIEW

Cyber security awareness has become a critical component of digital literacy. Previous studies suggest that awareness significantly influences individuals' online behavior and their ability to protect themselves from cyber threats.

- **Concept of Cyber Security Awareness:**Cyber security awareness refers to an individual's understanding of cyber threats, vulnerabilities, and the protective measures required to ensure safe online behavior. According to information security researchers, awareness is a critical factor in reducing cyber risks because human error remains one of the leading causes of security breaches. Awareness encompasses knowledge of cyber threats, understanding of security policies, and the ability to apply safe practices while using digital technologies. In the context of higher education, cyber security awareness enables students to recognize potential threats and make informed decisions regarding their online activities.
- **Growing Importance of Cyber Security in Higher Education:**The increasing integration of digital technologies in higher education has significantly expanded the cyber threat landscape. Universities now rely heavily on online learning platforms, cloud-based services, digital libraries, electronic communication systems, and online examination portals. While these technologies improve accessibility and efficiency, they also expose institutions and students to various cyber risks. Researchers have highlighted that universities are attractive targets for cybercriminals because they store large volumes of sensitive personal, academic, and research data. Consequently, cyber security awareness among students has become a crucial component of institutional security strategies.
- **Cyber Threats Affecting University Students:**Several studies have identified university students as one of the most vulnerable groups to cyber threats due to their extensive internet usage and dependence on digital devices.

Common threats include phishing attacks, malware infections, ransomware, identity theft, account hacking, and social engineering attacks. Students frequently use social media, online banking, e-commerce websites, and cloud services, increasing their exposure to cyber risks. Researchers have found that many cyber incidents occur because students fail to recognize suspicious activities or underestimate the potential consequences of unsafe online behavior.

- **Password Security and Authentication Practices:**Password management remains one of the most important aspects of cyber security. Previous studies indicate that many students continue to use weak passwords, reuse passwords across multiple accounts, and rarely change their credentials. Such practices significantly increase the likelihood of unauthorized access and account compromise. Researchers have emphasized the importance of strong passwords and multi-factor authentication (MFA) as effective security measures. Studies suggest that students who receive cyber security training are more likely to adopt secure password practices and use additional authentication methods to protect their accounts.
- **Social Media Usage and Privacy Concerns:** Social media platforms have become an integral part of students' lives, providing opportunities for communication, networking, and information sharing. However, excessive sharing of personal information can expose users to privacy and security risks. Research has shown that many students are unaware of privacy settings available on social networking platforms and often disclose sensitive information without considering potential consequences. Cybercriminals frequently exploit publicly available information to conduct phishing attacks, identity theft, and social engineering schemes. Therefore, awareness of social media privacy and responsible online behavior is essential for cyber security.
- **Phishing Awareness Among Students:** Phishing is one of the most common cyber threats targeting students and educational institutions. Phishing attacks typically involve fraudulent emails, messages, or websites designed to trick users into revealing confidential information such as usernames, passwords, and financial details. Several studies have found that although students are generally familiar with the concept of phishing, many struggle to identify sophisticated phishing attempts. Research suggests that practical awareness training and simulated phishing exercises can significantly improve students' ability to detect and avoid such attacks.
- **Role of Cyber Security Education and Training:**Cyber security education plays a vital role in developing secure online behaviors among students. Researchers have consistently emphasized the need for educational institutions to integrate cyber security topics into academic curricula and co-curricular activities. Workshops, seminars, awareness campaigns, and online training modules have been found to improve students' understanding of cyber risks and encourage the adoption of protective measures. Studies indicate that students who participate in cyber security training programs demonstrate higher levels of awareness and better security practices compared to those who have not received such training.

RESEARCH GAP

Although numerous studies have examined cyber security awareness in different contexts, there remains a need for continuous research focusing on university students due to the evolving nature of cyber threats and technological advancements Therefore, the present study seeks to bridge this gap by providing a comprehensive analysis of cyber security awareness and practices among university students and identifying areas for improvement in higher education institutions.

4. RESEARCH METHODOLOGY

Research methodology refers to the systematic process adopted to collect, analyze, and interpret data in order to achieve the objectives of the study. It provides a framework for conducting research in a scientific and organized manner. The present study employs a quantitative research approach to examine the level of cyber security awareness and practices among university students.

- **Research Design:**The study adopts a descriptive research design, which is appropriate for understanding the current status of cyber security awareness and online security practices among university students. Descriptive research helps in collecting detailed information about existing conditions, behaviors, attitudes, and perceptions without manipulating any variables. The design enables the researcher to analyze students' awareness levels, identify common security practices, and evaluate their preparedness against cyber threats.
- **Nature of the Study:**The study is both exploratory and descriptive in nature. It explores students' understanding of cyber security concepts and describes their online behavior, security practices, and responses to cyber threats. The research aims to provide a comprehensive picture of cyber security awareness within the university environment.
- **Population of the Study:**The population of the study consists of undergraduate and postgraduate students enrolled in universities and higher

education institutions. These students represent a diverse group of internet users who regularly interact with digital technologies for academic, social, and personal purposes. Since university students are among the most active users of digital platforms, they form an appropriate population for examining cyber security awareness and practices.

- **Sample and Sampling Technique:**A representative sample of students is selected from the target population to ensure reliable and meaningful results. The study may include a sample size of 150 to 300 students drawn from different academic disciplines such as Arts, Commerce, Science, Computer Applications, and Management.
- **Sources of Data:**The study utilizes both primary and secondary sources of data.

Primary Data: Primary data are collected directly from university students through a structured questionnaire. The questionnaire is designed to gather information regarding students' cyber security awareness, knowledge of cyber threats, password management practices, online privacy concerns, and security behaviors.

Secondary Data: Secondary data are collected from various published sources, including:

- Research journals and scholarly articles
- Books related to cyber security and information security
- Government reports and policy documents
- Conference proceedings
- University publications
- Reports from cyber security organizations
- Online databases and academic websites

Secondary data provide theoretical support and background information for the study.

- **Data Collection Procedure:**Data are collected through online and offline survey methods. The questionnaire is distributed to selected students through institutional email, online survey platforms, and classroom interactions. Respondents are informed about the purpose of the study and assured that their responses will remain confidential and used solely for academic purposes.

  Participation in the survey is voluntary, and respondents are encouraged to provide accurate and honest information to ensure the reliability of the research findings.
- **Limitations of the Study:**The study may be subject to certain limitations. The findings are based on self-reported responses, which may be influenced by personal bias or inaccurate reporting. The study is limited to selected university students and may not fully represent all higher education institutions. Additionally, cyber security awareness and practices may change over time due to technological advancements and emerging cyber threats.

5. CYBER SECURITY THREATS FACED BY UNIVERSITY STUDENTS

The increasing dependence on digital technologies for academic, social, and personal activities has made university students highly vulnerable to a wide range of cyber security threats. Students regularly use laptops, smartphones, cloud-based applications, social media platforms, online banking services, and learning management systems, which expose them to numerous cyber risks. Cybercriminals often target students because they may lack adequate cyber security awareness and frequently share personal information online. Understanding these threats is essential for developing effective security practices and reducing vulnerabilities.

- **Phishing Attacks:** Phishing is one of the most common cyber threats faced by university students. In a phishing attack, cybercriminals send fraudulent emails, text messages, or social media messages that appear to come from legitimate organizations such as universities, banks, or technology companies. The objective is to trick users into revealing sensitive information, including usernames, passwords, credit card details, or personal data. Students who are unfamiliar with identifying suspicious emails are particularly vulnerable to such attacks. Successful phishing attacks can lead to account compromise, financial loss, and identity theft.
- **Malware Attacks:** Malware refers to malicious software designed to damage, disrupt, or gain unauthorized access to computer systems. Common forms of malware include viruses, worms, spyware, adware, trojans, and ransomware. University students often download files, applications, and educational resources from various online sources, increasing the risk of malware infections. Once installed, malware can steal sensitive information, monitor user activities, corrupt files, or provide attackers with remote access to devices.
- **Social Engineering Attacks:** Social engineering involves manipulating individuals into disclosing confidential information or performing actions that compromise security. Unlike technical attacks, social engineering exploits human psychology and trust. Cybercriminals may impersonate university staff, classmates, technical support personnel, or trusted organizations to obtain passwords, personal information, or access credentials. Students who are unaware of these tactics may inadvertently become victims of such attacks.

- **Public Wi-Fi Security Risks:** University students frequently connect to public Wi-Fi networks in campuses, libraries, cafes, airports, and other public places. While convenient, public Wi-Fi networks often lack adequate security measures, making them attractive targets for cybercriminals. Attackers can intercept communications, steal login credentials, and monitor online activities through unsecured networks. Students who access sensitive information on public Wi-Fi without using secure connections may face significant security risks.
- **Fake Websites and Online Scams:** Cybercriminals often create fake websites that closely resemble legitimate websites to deceive users into providing sensitive information. Students may encounter fraudulent scholarship websites, fake job portals, counterfeit e-commerce stores, and deceptive educational platforms. These scams are designed to steal personal information, financial details, or login credentials.

6. FINDINGS AND DISCUSSION

The findings of the study provide valuable insights into the level of cyber security awareness and the online security practices of university students. Based on the analysis of the collected data, several important observations were made regarding students' knowledge of cyber threats, digital security behavior, and attitudes toward online safety. The discussion of these findings helps in understanding the strengths and weaknesses of students' cyber security preparedness and highlights areas requiring improvement.

- **General Awareness of Cyber Security:** The study revealed that a majority of university students are familiar with the concept of cyber security and understand its importance in protecting personal and institutional information. Most respondents indicated that they had heard about cyber security through academic courses, social media, news platforms, and online resources. However, while general awareness was relatively high, the depth of understanding varied significantly among students from different academic disciplines. Students enrolled in technology-related programs demonstrated higher awareness levels compared to those from non-technical backgrounds.
- **Use of Multi-Factor Authentication:** The study found that awareness of multi-factor authentication (MFA) was moderate among university students. While some students actively used MFA for email, banking, and social media accounts, many respondents either lacked knowledge about the feature or had not enabled it on their accounts. This indicates that students may not be fully utilizing available security measures that could significantly enhance account protection.
- **Social Media Security and Privacy Awareness:** The analysis revealed that social media platforms are among the most frequently used digital services by university students. While most respondents expressed concern about online privacy, many admitted to sharing personal information such as photographs, location details, contact information, and personal opinions on social networking sites. A substantial number of students were unaware of advanced privacy settings or rarely reviewed their account security configurations. This behavior increases the risk of identity theft, cyber stalking, and social engineering attacks.
- **Awareness of Phishing Attacks:** The findings indicate that most students have heard about phishing attacks; however, their ability to identify fraudulent emails and fake websites varies considerably. Many respondents could recognize obvious phishing attempts, but a significant number struggled to detect sophisticated phishing messages that closely resembled legitimate communications. This highlights the need for practical training and awareness programs that focus on real-world phishing scenarios.
- **Challenges Identified Among Students:** Several challenges were identified during the study. These included limited practical knowledge of cyber security, overconfidence in personal security practices, lack of participation in cyber security training programs, and inadequate understanding of emerging cyber threats. Many students also reported difficulty keeping up with rapidly evolving cyber risks and technological developments. These challenges highlight the need for continuous education and awareness initiatives.
- **Role of Universities in Enhancing Cyber Security Awareness:** The findings suggest that universities play a crucial role in promoting cyber security awareness among students. Respondents expressed interest in attending workshops, seminars, awareness campaigns, and training programs related to digital safety. Many students believed that cyber security education should be integrated into university curricula regardless of academic discipline. This indicates a growing recognition of the importance of cyber security skills in academic and professional environments.

7. RECOMMENDATIONS

To improve cyber security awareness and practices among university students, the following measures are recommended:

- Introduce cyber security awareness programs as part of university orientation.

- Include basic cyber security education in academic curricula.
- Conduct regular workshops and seminars on digital safety.
- Promote the use of strong and unique passwords.
- Encourage the adoption of multi-factor authentication (MFA).
- Provide training on identifying phishing emails and scams.
- Increase awareness about privacy protection on social media platforms.
- Encourage regular software updates and antivirus usage.
- Establish university cyber security support centers.
- Organize cyber security competitions and awareness campaigns.

8. CONCLUSION

The rapid advancement of digital technologies has transformed the higher education sector, making online platforms an indispensable part of students' academic and personal lives. From virtual classrooms and cloud-based learning systems to social media and digital payment applications, university students are increasingly dependent on technology for communication, learning, research, and entertainment. While these technological developments offer numerous benefits, they also expose students to a wide range of cyber security threats, including phishing attacks, malware infections, identity theft, ransomware, data breaches, and online fraud. Consequently, cyber security awareness has become a critical requirement for ensuring a safe and secure digital learning environment.

The findings of this study indicate that university students generally possess a basic understanding of cyber security concepts and recognize the importance of protecting their digital information. Most students are aware of common cyber threats and acknowledge the risks associated with unsafe online behavior.

The study underscores the vital role of universities and higher education institutions in fostering cyber security awareness and digital responsibility. Educational institutions are uniquely positioned to equip students with the knowledge, skills, and attitudes necessary to navigate the increasingly complex cyber environment. Integrating cyber security education into academic curricula, organizing workshops and awareness campaigns, conducting simulated cyberattack exercises, and promoting best practices for online safety can contribute significantly to improving students' cyber resilience.

Furthermore, universities should establish comprehensive cyber security policies and provide access to resources that help students understand emerging threats and security technologies. Continuous learning and regular awareness initiatives are essential because cyber threats evolve rapidly, and security knowledge must be updated accordingly. Collaboration among educators, information technology departments, policymakers, and cyber security professionals can further strengthen institutional efforts to create a culture of cyber security awareness.

In conclusion, cyber security awareness is no longer an optional skill but a fundamental requirement for students in the digital age. As higher education continues to embrace digital transformation, the responsibility of ensuring cyber safety becomes increasingly important. By promoting awareness, encouraging responsible digital behavior, and providing practical cyber security education, universities can empower students to protect themselves and contribute to a safer digital society. The development of strong cyber security awareness among university students will not only safeguard personal and institutional information but also prepare future professionals to address the cyber challenges of an increasingly interconnected world.

REFERENCES

1. Al-Janabi, S., & Al-Shourbaji, I. (2016). A Study of Cyber Security Awareness in Educational Institutions.

2. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., &Jerram, C. (2017). Determining Employee Awareness Using the Human Aspects of Information Security Questionnaire.

3. Whitman, M. E., &Mattord, H. J. (2022). Principles of Information Security. Cengage Learning.

4. Stallings, W. (2021). Effective Cyber Security: A Guide to Using Best Practices and Standards.

5. National Institute of Standards and Technology (NIST). Cybersecurity Framework.

6. ISO/IEC 27001: Information Security Management Systems Standard.

7. Kumar, R., & Singh, P. (2023). Cyber Security Awareness Among College Students: Challenges and Solutions.