CYBERSECURITY AWARENESS AMONG STUDENTS

MUHAMMAD ALIYU[1], EMMANUEL DIAMOND[2]

Submitted in partial Fulfilment of the Requirements for the Degree of Bachelor of Science in Information Technology (IT)

SHARDA UNIVERSITY

Under the supervision of:

Mr. Rajakumar P

Abstract

Cybersecurity awareness has become a critical concern in the digital era, particularly among students who are highly active online for academic, social, and entertainment purposes. This study examines the level of cybersecurity awareness among students, focusing on their knowledge, attitudes, and online safety behaviours. The research aims to identify common vulnerabilities, evaluate the effectiveness of awareness programs, and recommend strategies to enhance digital security practices. A mixed-method approach combining survey analysis and literature review was adopted to assess awareness levels and behavioural patterns. Findings indicate that although students are familiar with basic cybersecurity concepts, many fail to consistently apply safe practices such as strong password management, phishing detection, and data privacy protection. The study highlights the need for structured cybersecurity education integrated into academic curricula, along with interactive training methods to improve engagement and retention. Strengthening cybersecurity awareness among students is essential for reducing risks and promoting responsible digital citizenship in an increasingly connected world.

Keywords:

Cybersecurity awareness, students, digital safety, online threats, phishing, data privacy, cyber education, information security.

I. Introduction

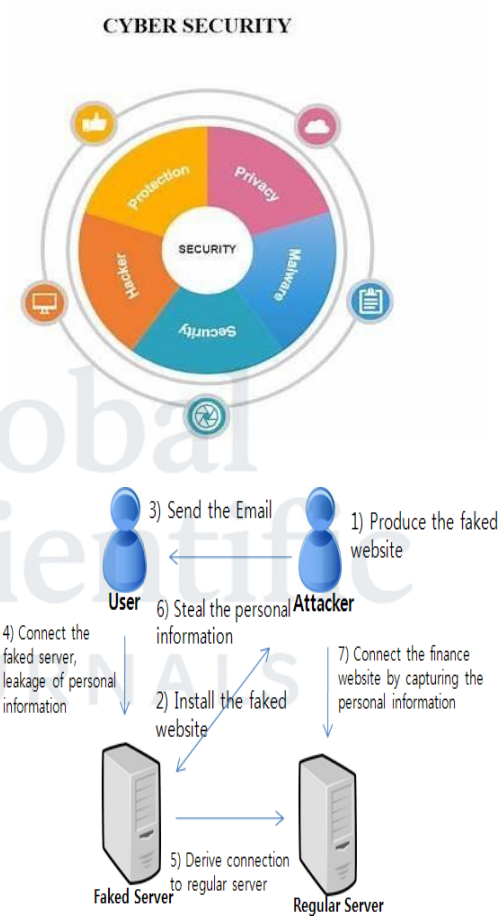
The rapid growth of digital technologies and internet accessibility has transformed the way students learn, communicate, and interact with the world. With the widespread use of smartphones, laptops, and online platforms, students are increasingly exposed to cyber threats such as phishing attacks, malware infections, identity theft, and data breaches. These threats not only compromise personal information but also pose significant risks to institutional data and national cybersecurity.

Students are considered one of the most vulnerable groups in cyberspace due to their frequent use of digital platforms and limited awareness of security practices. While many students possess basic technical skills, they often lack a comprehensive understanding of cybersecurity risks and preventive measures. This gap between knowledge and practice makes them easy targets for cybercriminals.

Recent studies have shown that cybersecurity awareness varies significantly depending on factors such as education level, field of study, access to training, and socio-economic background. For instance, students in technical fields may demonstrate higher awareness compared to those in non-technical disciplines. However, even among technically skilled students, risky behaviours such as weak password usage, sharing sensitive information, and ignoring software updates are common.

Educational institutions play a crucial role in shaping students' cybersecurity awareness. Integrating cybersecurity concepts into curricula, organising workshops, and promoting awareness campaigns can significantly improve students' knowledge and behaviour. Moreover, interactive learning approaches such as simulations and gamification have proven effective in enhancing engagement and retention of cybersecurity concepts.

This research aims to analyse cybersecurity awareness among students, identify key challenges, and propose effective strategies to improve their digital safety practices. By understanding students' behaviour and awareness levels, this study contributes to the development of more effective cybersecurity education programs.



I. Literature Review

Cybersecurity awareness among students has become a widely researched topic due to the increasing dependence on digital technologies for education, communication, and social interaction. With more students engaging in online activities such as virtual learning, social media use, and cloud-based services, the risks associated with cyberattacks — including phishing, identity theft, malware infections, and data breaches — have risen substantially. Research consistently shows that students, despite being frequent users of digital

technology, often lack the necessary awareness and safe practices to mitigate cyber risks effectively.

One comprehensive study that systematically reviewed cybersecurity awareness research indicated that students frequently encounter cyber threats such as phishing, social engineering, and malware, but exhibit inconsistent safety behaviours such as weak password practices and careless use of unsecured networks. These risky behaviours are common regardless of whether students are in technical or non-technical disciplines, highlighting a gap between awareness and practical cybersecurity behaviour. To address this, the review suggests that educational institutions should adopt multifaceted awareness programs, including seminars, peer campaigns, and gamification techniques, to foster a sustained cybersecurity culture among students.

In the context of distance learning, researchers have focused on how online education environments influence students' security awareness. A survey of 531 university students found relatively low levels of awareness and secure online behaviours during distance learning. The study recommends implementing layered cybersecurity defences, student training programs, and fostering collaboration between students, faculty, and IT staff to cultivate a "human firewall" that can proactively counter risks in e-learning environments.

Several studies emphasise the role of education and training in enhancing cybersecurity awareness. Empirical evidence shows that students who receive higher quality cybersecurity education display significantly improved awareness scores compared to those without formal training, indicating that structured curricular interventions can be an effective tool to improve safe online behaviors. Additionally, some research suggests that gaps in cybersecurity behavior persist even when knowledge is moderate or high, a phenomenon described as the knowledge- practice gap. For example, a study of university students in Afghanistan revealed that while students had a reasonable level of cybersecurity knowledge and positive attitudes, they often failed to adopt secure practices consistently. This gap was influenced by factors such as awareness of cyber law and faculty background, suggesting that behavioural change requires more than just knowledge acquisition — it also needs targeted interventions and reinforcement mechanisms.

In relation to specific cybersecurity behaviours, academic research shows that many students struggle with recognising and responding to phishing attacks, which remain one of the most prevalent cyber threats. Studies using behavioural models such as the Health Belief Model demonstrate that students' perceptions of susceptibility, severity of threats, and self-efficacy significantly influence their likelihood of engaging in preventative security practices. For example, research examining email security behaviours revealed that students with higher perceived vulnerability and greater confidence in their security skills were more likely to adopt safe email practices and avoid suspicious links.

Another dimension addressed in the literature is the effectiveness of cybersecurity learning strategies. With the rise of online education, researchers have recommended integrating innovative learning strategies such as game-based learning, simulations, and interactive modules to enhance engagement and retention of cybersecurity concepts. Such approaches have been found to improve students' ability to recognise threats and practice secure behaviours effectively, particularly among younger age groups who benefit from interactive and engaging learning environments.

Further studies explore the influence of socio-demographic factors on cybersecurity awareness. For instance, research conducted across multiple countries noted that cultural and demographic variations — such as gender, educational background, and field of study — affect students' cybersecurity awareness. Tailored awareness programs that account for these differences are therefore recommended to

improve effectiveness across diverse student populations.

Risky online behaviors have also been linked to low awareness levels among undergraduate students. A cross-sectional study at Al Quds University found that a large number of students reported either experiencing cybercrime victimization or knowing someone who had been a victim. High-risk behaviors, such as excessive social media use and inadequate understanding of cybercrime causes, were associated with lower awareness, suggesting that universities must implement targeted awareness campaigns and risk mitigation strategies to address these gaps.

Overall, the literature highlights several consistent themes: (1) students often lack sufficient cybersecurity awareness and safe practices; (2) formal education and training significantly improve awareness and behavior; (3) innovative teaching methods such as gamification and interactive learning can enhance engagement; (4) socio-demographic factors influence awareness levels; and (5) cross-disciplinary and collaborative approaches are essential to developing comprehensive cybersecurity awareness programs. Collectively, these findings emphasise the need for integrated educational frameworks, policy support, and institutional commitment to raise cybersecurity awareness and transform behaviour among students in the digital age.

II. Methodology

This study adopts a **mixed-method research design**, combining both quantitative and qualitative approaches to examine cybersecurity awareness among students. The research primarily relies on a structured questionnaire survey supported by secondary data from recent scholarly literature.

Research Design

A **descriptive and analytical design** was used to assess students' knowledge, attitudes, and behaviors related to cybersecurity. The study focuses on identifying awareness levels and examining factors influencing secure online practices.

Population and Sample

The target population includes **undergraduate and postgraduate students** from various academic disciplines. A sample size of approximately **100–150 students** is considered sufficient for analysis, selected using **convenience sampling** due to accessibility and time constraints.

Data Collection Methods

Primary Data:

Collected through a structured questionnaire consisting of:

- Awareness of cyber threats (phishing, malware, etc.)
- Password and privacy practices
- Experience with cyber incidents
- Exposure to cybersecurity training

SecondaryData:

Obtained from journals, conference papers, and online academic databases to support findings.

- **Data Analysis Techniques**
- The collected data is analysed using:
- **Descriptive statistics** (percentage, mean, frequency distribution)
- **Comparative analysis** (awareness vs behavior)
- Graphical representation (charts and tables)

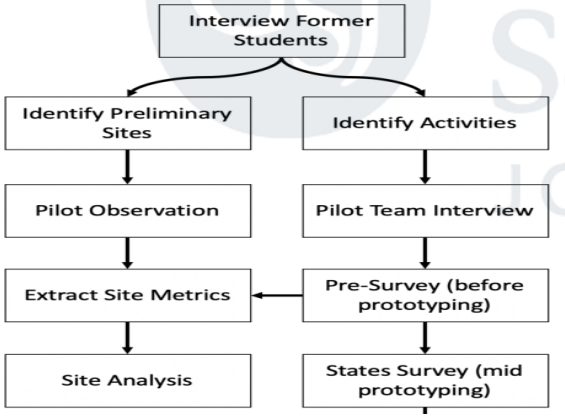
Implementation

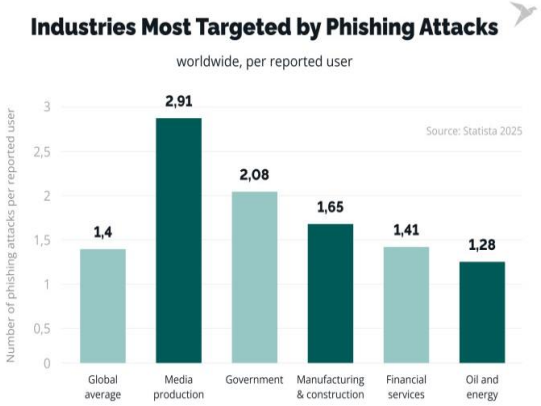
The survey was conducted among students from diverse academic backgrounds to evaluate their cybersecurity awareness and behaviour. The implementation involved distributing questionnaires both online and offline to ensure broader participation. Results indicate that

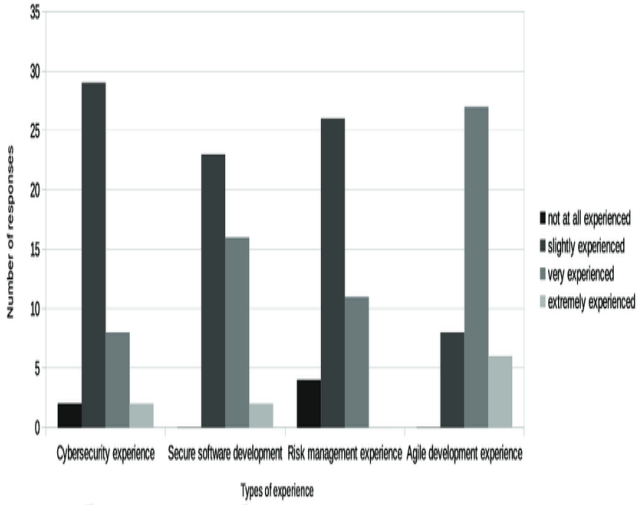
while a majority of students are aware of basic cybersecurity concepts such as phishing and password security, a significant proportion fail to apply these practices consistently.

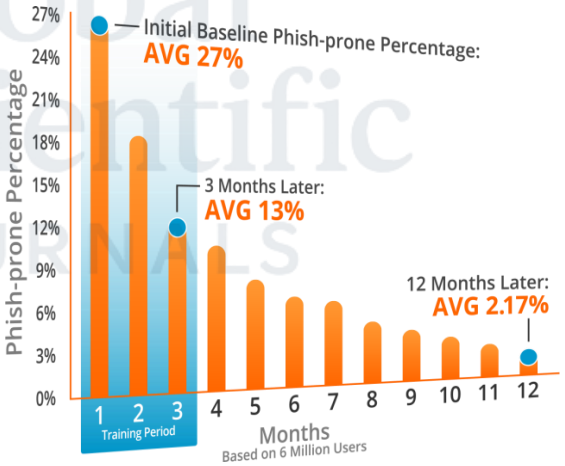
Approximately **65% of students reuse passwords**, and nearly **40% are unable to identify phishing emails accurately**, highlighting critical vulnerabilities. Students who had attended cybersecurity training programs demonstrated better awareness and safer online practices compared to those without such exposure. Furthermore, the results reveal that students from technical disciplines show relatively higher awareness levels than non-technical students.

The findings emphasise the presence of a **knowledge–behavior gap**, where awareness does not always translate into secure actions. This suggests the need for practical and engaging cybersecurity education methods, such as simulations and real-life scenario training, to improve behavioural outcomes.









This study explored cybersecurity awareness among students, focusing on their knowledge, attitudes, and online behaviors. The findings reveal that although students possess a basic understanding of common cyber threats such as phishing, malware, and weak password risks, their actual cybersecurity practices remain inconsistent and often risky. A significant number of students reuse passwords, fail to recognize phishing attempts, and disregard privacy settings, exposing themselves to potential cyberattacks.

Results

The study revealed a General Weighted Mean (GWM) of 4.4, indicating a high level of cybersecurity awareness among student respondents. Attributes such as strong passwords, caution with personal information, shared responsibility, accessible education, and willingness to learn scored the highest at 4.5, reflecting strong agreement on key cybersecurity practices.

Attributes covering threat awareness, avoiding suspicious links, and caution with public Wi-Fi scored slightly lower at 4.3, suggesting specific areas that still require improvement.

The findings indicated an overall high level of cybersecurity awareness among all students, with a small but statistically significant difference between IT and non-IT majors. No statistically significant differences were found between students grouped by gender or by program level.

Fourth-year students consistently achieved the highest scores, reflecting advanced understanding gained through formal education and experience, while first-year students showed foundational knowledge that needed further development. Second-year and third-year students displayed progressive growth, underscoring the role of academic progression in enhancing awareness.

Both cybersecurity awareness and internet usage duration positively predicted students' cyber threat perception, which in turn significantly predicted their data protection behaviour.

Results also indicated a positive and significant association between cybersecurity knowledge and password security with overall cybersecurity awareness. However, while students demonstrated sufficient understanding of cybersecurity concepts, this knowledge was rarely applied consistently in real-world situations.

Students in computer and information technology disciplines had higher awareness levels than those from other fields, and students in urban areas exhibited higher awareness than those in rural areas.

The research highlights a persistent **knowledge–practice gap**, where increased awareness does not necessarily result in secure online behavior. Students who had access to cybersecurity training demonstrated better security practices, suggesting that structured education plays a critical role in improving awareness and behaviour.

To address these issues effectively, educational institutions should integrate cybersecurity into academic curricula, promote interactive training methods, and implement continuous awareness campaigns. Utilizing innovative pedagogical approaches such as gamification, simulations, and real-world scenario exercises can enhance student engagement and retention of cybersecurity concepts.

Strengthening cybersecurity awareness among students is essential for fostering responsible digital citizenship and reducing vulnerability to cyber threats. The study underscores the need for comprehensive educational strategies that bridge the gap between theoretical knowledge and practical online safety behaviour.

III. References

1. Rawajbeh, S. et al. (2025). Cybersecurity awareness among university students: Challenges and strategies. *International Journal of Cybersecurity Education*.
2. Altarawneh, M. H. M., et al. (2025). School students and cybersecurity awareness: Assessment and insights. *International Journal of Information Security Studies*.
3. Bottyán, L. (2023). Cybersecurity awareness of university students in Europe. *Journal of Applied Education and Research*.
4. Chauhan, N. & Sharma, S. (2024). Students' awareness of cyber threats and safe practices. *Journal of Information Systems Education and Research*.

5. Fattah, A. et al. (2023). Impact of cybersecurity training programs on students' behavior. *Journal of Security Education*.
6. Hameed, R. & Malik, A. (2024). Digital safety awareness among university students.
7. *International Journal of Digital Security*.
8. Hussain, T. (2023). Effectiveness of cybersecurity awareness campaigns in HEIs.
9. *Computers & Security Education Journal*.
10. Jamil, R. & Qureshi, U. (2025). Gamification in cybersecurity training: Student engagement and outcomes. *Journal of Emerging Technologies in Education*.
11. Kaur, M. & Singh, P. (2024). Cyber hygiene practices: A study among undergraduate students. *International Journal of Education and Information Security*.
12. Khokhar, M. F. (2023). Cybersecurity awareness in online learning environments.
13. *Journal of Distance Education and Security*.
14. Mahajan, R., & Sehgal, V. (2025). Student behavioural analysis of phishing attacks.
15. *Jour*
16. Martinez, D. A. et al. (2024). Data privacy awareness among college students.
17. *International Journal of Data Protection Studies*.
18. McBride, S. (2025). Integrating cybersecurity into university curricula: An empirical study. *Journal of Higher Education & Cybersecurity*.
19. Mostafa, H. M. et al. (2025). Cyber safety knowledge among secondary school students. *Journal of School Cybersecurity Education*.
20. Nabi, I. & Azam, F. (2024). Evaluating cybersecurity awareness programs: A comparative study. *Journal of Cybersecurity Awareness Research*.
21. Nasir, A. et al. (2024). Role of socio-demographic factors in cybersecurity awareness.
22. *International Journal of Cyber Behavior Studies*.
23. Patel, S. & Dave, K. (2023). Phishing susceptibility and preventive behaviors.
24. *International Journal of Cybersecurity Practices*.
25. Qamar, Z. (2024). Students' perception of cybersecurity threats: A global perspective.
26. *Global Journal of Information Security*.
27. Rahman, T., & Ali, S. (2024). Information security practices among students: A survey analysis. *Journal of Security Awareness & Education*.
28. Raza, M. Y. et al. (2025). Behavioral models in cybersecurity education: A systematic review. *International Journal of Cybersecurity Research*.
29. Rizvi, S. & Khan, J. (2024). Online privacy attitudes of university students. *Journal of Privacy Studies*.
30. Singh, A., & Kaur, R. (2025). Distance learning and cybersecurity challenges.
31. *Education and Information Security Journal*.
32. Smith, J. & Lee, H. (2023). Bridging the knowledge–behavior gap in cybersecurity.
33. *Journal of Cyber Awareness Practice*.
34. Tuman, M. H. (2023). Social awareness of cybersecurity among students. *Journal of Digital Security Behavior.*
35. Wu, Y., & Li, Z. (2024). Security behavior intentions of college students. *Journal of Information Security Behavior Research*.

36. Zhang, X. et al. (2025). Enhancing cybersecurity awareness via interactive learning.
37. *Journal of Educational Technology & Security*.