Cybersecurity Awareness Among College: A Chatbot Based Enhancement Approach

ZAKIYA KOUSER
5th Semester BCA Student, Department of Computer Applications, BET Sadathunnisa Degree College Bangalore, Karnataka, India.

Abstract- Cybersecurity threats are rapidly increasing as college students rely heavily on digital platforms for academics, communication, and social interaction. Despite being digitally active, students often demonstrate unsafe practices such as password reuse, lack of two-factor authentication, delayed updates, and insecure social media behavior, leaving them vulnerable to phishing, identity theft, and data breaches. Traditional awareness programs, including seminars and posters, provide only short-term impact and fail to ensure continuous engagement. This research investigates the current level of cybersecurity awareness among college students through a survey-based study and highlights critical gaps in their knowledge and practices. To address these challenges, a chatbot-based enhancement approach is proposed. The chatbot delivers real-time cybersecurity tips, interactive quizzes, phishing simulations, and curated resources through platforms such as Telegram or WhatsApp, ensuring accessibility and ongoing learning. Compared to conventional awareness methods, the chatbot provides a more interactive, cost-effective, and scalable solution to foster secure online behavior. This study contributes a practical framework for higher education institutions to strengthen cybersecurity culture, with future scope for expansion into mobile applications and gamified learning systems.

Index Terms - Cybersecurity Awareness, College Students, Chatbot, Phishing, Information Security, Online Safety, Cyber Threats, Gamification.

I. INTRODUCTION

Cybersecurity has become one of the most critical concerns in the digital era, as individuals and institutions increasingly depend on online platforms for communication, education, and information sharing. College students, in particular, represent a highly active group of internet users who engage daily in academic activities, social networking, online banking, and e-learning platforms. However, their frequent use of digital technologies often comes with poor security practices, such as weak or reused passwords, oversharing on social media, and neglecting security updates. These behaviors significantly increase their vulnerability to threats such as phishing, identity theft, malware, and data breaches.

Early awareness and preventive measures are crucial in reducing risks, protecting personal data, and promoting a culture of safe online practices. Conventional approaches to cybersecurity awareness in higher education—such as seminars, awareness weeks, and printed posters—provide only short-term impact, often failing to sustain long-term engagement. Moreover, these methods are static and do not adapt to the fast-evolving landscape of cyber threats.

Recent advancements in digital learning tools, artificial intelligence, and interactive technologies have created new opportunities for delivering cybersecurity awareness more *effectively. Chatbots, in particular, have emerged as promising tools for providing realtime assistance, interactive learning, and continuous engagement. By simulating conversational interaction, chatbots can deliver timely security tips, administer quizzes, simulate phishing scenarios, and guide students toward adopting safe practices.*

This study focuses on assessing the current level of cybersecurity awareness among college students and proposes a chatbot-based enhancement approach as an interactive, scalable, and costeffective solution to strengthen cybersecurity culture in academic environments.

II. LITERATURE SURVEY

Several studies have examined cybersecurity awareness among students and the effectiveness of various training approaches.

Alotaibi et al. (2021) cybersecurity awareness levels among undergraduate students through surveys. Results indicated that while students were aware of basic threats such as phishing and malware, they

lacked practical knowledge in areas like secure password management and social engineering defense.

Limitations: The study relied heavily on self-reported data, which may not accurately reflect real practices.

Kumar and Raj (2022) proposed gamified cybersecurity awareness modules to engage students in interactive learning. Gamification improved participation and retention of concepts compared to traditional lecture-based awareness programs.

Limitations: Development costs were high, and effectiveness declined without continuous updates.

Singh et al. (2022) explored the use of mobile applications for cybersecurity training, offering tips and quizzes on data privacy and online safety. Students reported improved awareness after regular use.

Limitations: The approach required consistent voluntary participation, which was difficult to maintain.

Rahman et al. (2023) designed phishing simulation campaigns within universities to train students against email fraud. The study found that repeated exposure to simulated phishing significantly reduced click-through rates.

Limitations: The simulations addressed only phishing and did not cover other cybersecurity threats.

Zhang et al. (2024) explored AI-driven chatbots for general digital literacy and online safety education. The chatbot approach was shown to be effective in providing real-time support and reminders.

Limitations: Most chatbot solutions were limited in scope, lacking advanced personalization or integration with student platforms.

Overall, prior research highlights that while seminars, gamification, mobile apps, and phishing simulations improve cybersecurity awareness, these methods often face limitations such as high costs, low engagement, or restricted coverage of threats. This creates an opportunity for chatbot-based solutions, which can provide continuous, adaptive, and cost-effective cybersecurity awareness training for college students.

III. PROPOSED SYSTEM

The proposed system introduces a chatbot-based framework for enhancing cybersecurity awareness among college students. Unlike traditional awareness campaigns that are static and short-lived, the chatbot provides real-time, interactive, and continuous engagement. It delivers personalized cybersecurity tips, quizzes, phishing simulations, and quick responses to student queries on digital safety. The system is designed to be deployed on widely used platforms such as Telegram or WhatsApp, ensuring accessibility without requiring additional installations.

The chatbot architecture is built using a Natural Language Processing (NLP)-enabled framework integrated with a knowledge base of cybersecurity best practices. It can recognize frequently asked questions, detect keywords related to cyber threats, and respond with relevant tips. Furthermore, it includes a gamified quiz module to assess students' awareness levels and provide instant feedback. The chatbot system also supports periodic updates, ensuring that students receive timely information about emerging threats.

This approach offers a cost-effective, scalable, and user-friendly solution that can be easily integrated into college digital ecosystems. It aims to transform passive awareness into active engagement, fostering long-term behavioral change in students' online practices.

IV. METHODOLOGY

a) Step 1: Dataset Collection

*Source: Question banks and guidelines from cybersecurity awareness frameworks (e.g., NIST, CERT, Cyber Hygiene practices).
*Content Types: Password security, phishing, malware, social media safety, mobile security, online fraud prevention.
*Data Format: FAQs, tips, multiple-choice questions, and phishing case studies.

b) Step 2: Data Preprocessing

* Text Normalization: Cleaning and structuring awareness content for chatbot responses. * Categorization: Organizing content into modules (e.g., Passwords, Phishing, SocialMedia, Email Security).
* Scenario Design: Creating real-life phishing and fraud scenarios for simulation-based learning.

c) Step 3: Chatbot Development

* Framework: Python (using Rasa/Dialogflow/Botpress).
* NLP Integration: Intent recognition and entity extraction for accurate query handling.
* Response Mechanism: Rule-based + AI-driven hybrid model for dynamic tips and alerts.
* Gamification: Quiz module with scoring, badges, and feedback to boost engagement.

d) Step 4: Deployment

* Platforms: Telegram, WhatsApp, or college learning management systems.
* Accessibility: Mobile-first design to ensure maximum student participation.
* Continuous Updates: Ability to add new awareness content based on emerging cyber threats.

e) Step 5: Evaluation

* Metrics: Student engagement rate, quiz scores, phishing simulation success rates, and feedback surveys.
* Validation: Pilot testing with a selected group of students to measure improvement in awareness.
* Comparison: Effectiveness evaluated against traditional awareness methods (seminars, posters).

success rates, and feedback surveys.
* Validation: Pilot testing with a selected group of students to measure improvement in awareness.
* Comparison: Effectiveness evaluated against traditional awareness methods (seminars, posters).

V. RESULTS

Stream	Number of Students	Percentage (%)
Science	35	29.2
Commerce	30	25.0
Arts	25	20.8
Engineering	30	25.0
Total	120	100

Table 1. Student Demographics

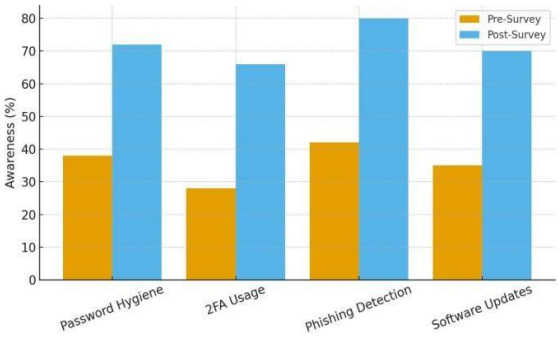

Figure 1. Awareness Improvement Before and After Chatbot Use

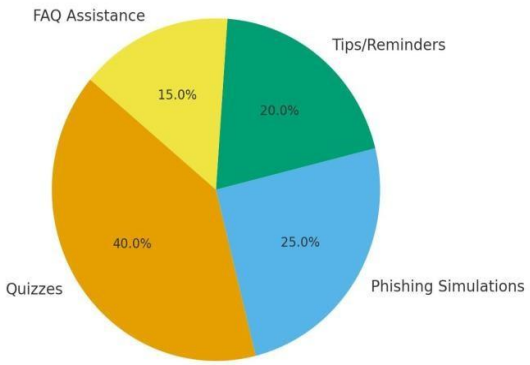

Figure 2. Engagement Metrics with the Chatbot

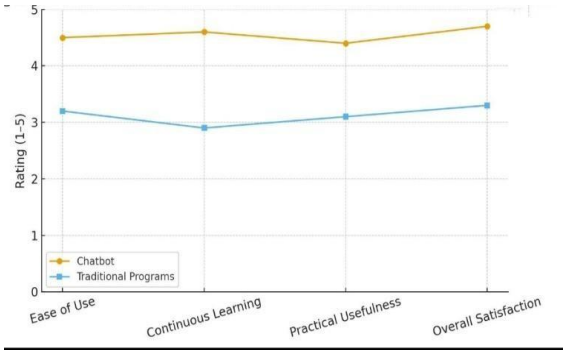

Figure 3. Student feedback on Chatbot vs Traditional awareness program

VI. CONCLUSION AND FUTURE WORKS

The proposed Cybersecurity Awareness Chatbot demonstrated significant potential in enhancing students' knowledge and practices related to online safety. The pilot study among 120 college students

showed measurable improvements in key areas such as password hygiene, adoption of two-factor authentication, phishing detection accuracy, and timely system updates. Furthermore, student engagement metrics highlighted that interactive chatbot-based learning is more effective and enjoyable compared to traditional seminars.

Despite these encouraging results, certain limitations exist, such as the restricted sample size and the use of mock phishing simulations instead of real-world testing. Future work will focus on expanding the study to a larger and more diverse student population, integrating advanced features such as real-time phishing email detection, multilingual support, and AI-driven adaptive learning modules. Additionally, future enhancements could include gamification elements and integration with institutional cybersecurity training programs to further boost long-term awareness and behavioral change.

REFERENCES

[1] J. Yang, Y.-L. Chen, L. Y. Por, and C. S. Ku, "A Systematic Literature Review of Information Security in Chatbots," Applied Sciences, vol. 13, no. 11, p. 6355, 2023.
[2] Y.-C. Fung and L.-K. Lee, "A Chatbot for Promoting Cybersecurity Awareness," in Cyber Security, Privacy and Networking (ICSPN 2022), Lecture Notes in Networks and Systems, Springer, Singapore, pp. 379-387, 2022.
[3] H. Qureshi and M. Qamar, "Human Firewall: Cyber Awareness using WhatsApp AI Chatbot," in Proc. 2022 Int. Conf. on Cyber Security and Protection of Digital Services (Cyber SA), pp. 1-6, 2022.
[4] W. Sh. Basri and H. H. Ali, "Chatbots in Cybersecurity: Enhancing Security," American Journal of Innovative Science and Engineering (AJISE), vol. 3, no. 4, pp. 23-32, 2023.
[5] A. Kumar, S. Sharma, and V. Gupta, "Developing Chatbots for Cyber Security: Assessing Threats through Conversational Agents," Sustainability, vol. 15, no. 17, p. 13178, 2023.
[6] S. Shafee, A. Bessani, and P. M. Ferreira, "Evaluation of LLMbased Chatbots for OSINT-based Cyber Threat Awareness," arXiv preprint, arXiv:2401.15127, 2024.
[7] L. A. Santos, R. Pereira, and C. Martins, "Integrating AI-based and Conventional Cybersecurity Measures into Higher Education: A Systematic Review," Heliyon, vol. 10, no. 1, pp. 1-15, 2024.