FIELD PROJECT REPORT

On

CYBERSECURITY AWARENESS SURVEY AMONG STUDENTS

Submitted in partial fulfillment for the degree of

BACHELOR OF SCIENCE (COMPUTER SCIENCE)

Submitted by

PRASHANT, SANJEEV, SHUBHAM, JUNED, PRAMOD

Seat No: 53014, 53024, 53025, 53027, 53003

UNDER THE GUIDANCE OF

Ms. Savita Lambhe

SMT. DEVKIBA MOHANSINHJI CHAUHAN COLLEGE OF COMMERCE AND SCIENCE

(Affiliated to University of Mumbai)

ACADEMIC YEAR 2025-2026

Smt. Devkiba MohanSinhji Chauhan College of Commerce & Science

Silvassa

UT of DNH & DD - 396230

Certificate

This is to certify that Mr. Prashant, Sanjeev, Shubham, Juned, Pramod bearing is a bonafide student of Smt. Devkiba Mohansinhji Chauhan College of Commerce and Science .

He/She has satisfactorily completed the Field Project entitled "CYBERSECURITY AWARENESS SURVEY AMONG STUDENTS" for the academic year 2025-2026 under the guidance of

Prof. Savita Lambhe

The work is genuine and has not been submitted elsewhere for any other degree or diploma.

Date of Submission : 10/11/2025

Internal Guide Examiner **Head of Department**

College Seal :

Certificate By Mentor

This is to certify that the Field Project entitled "CYBERSECURITY AWARENESS SURVEY AMONG STUDENTS" has been carried out by Mr./Ms.**Prashant, Sanjeev, Shubham, Juned, Pramod** under my guidance. The work is original and has been completed to my satisfaction.

Place: Silvassa

Date: 10/11/2025

Prof. Savita Lambhe

(Project Mentor)

GUIDE INTERACTION DIARY FORM

I, the undersigned Ms /Mr. Prashant, Sanjeev, Shubham, Juned, Pramod Roll No. 530-14,24,25,27,03 studying in the 2nd Year of BSc. CS Full-time Course is doing my project work under the guidance of Dr./Ms./Mr. Savita Lambhe, wish to state that I have met my Internal guide on the following dates mentioned below for Project Guidance:-

Sr. No	Date	Signature of the Internal Guide

Signature of the Candidate **Signature of Internal Guide**

Declaration

We, Prashant, Sanjeev, Shubham, Juned, Pramod , hereby declare that the Field Project entitled "CYBERSECURITY AWARENESS SURVEY AMONG STUDENTS " submitted for the SYBSC (Computer Science) Semester -III course at **SMT. DEVKIBA MOHANSINHJI CHAUHAN COLLEGE OF COMMERCE AND SCIENCE** is my original work, conducted under the guidance of Prof. Savita Lambhe

This work has not been submitted, in part or full, to any other institution for the award of any other degree or diploma.

Place: Silvassa

Date: 10/11/2025

Signature of Student

Prashant, Sanjeev, Shubham, Juned, Pramod

Seat No: 53014 ,53024 ,53025 ,53027 ,53003

Acknowledgement

It is a great pleasure to express my profound gratitude to all the individuals who have supported and guided me throughout this Field Project.

First and foremost, I would like to extend my sincere thanks to my project guide, Prof. **Savita Lambhe**, for her invaluable guidance, constant encouragement, and insightful feedback, which were instrumental in the successful completion of this project.

I am also grateful to **Sini Ma'am**, Head of the Computer Science Department, and the entire faculty for providing the necessary resources and a conducive environment for learning and research.

My special thanks to the management and Principal of **SMT DEVKIBA MOHANSINHJI CHAUHAN COLLEGE OF COMMERCE AND SCIENCE** for this opportunity.

I would also like to acknowledge all the respondents who participated in my survey; their input was crucial for the analysis in this study.

Lastly, I wish to thank my family and friends for their unwavering support and motivation throughout this academic journey.

PRASHANT KUMAR DAS
SANJEEV KUSHWAHA
PANDEY SHUBHAMKUMAR
JUNED SHAIKH
PRAMOD LEHVA

Table of Contents

List of Figures

List of Tables

Introduction

1.1 Background

Students are highly connected, making them frequent targets of cybercrime. This dependence on digital tools for learning and socializing exposes them to significant threats against their privacy, finances, and safety.

1.2 Problem Statement

Many students fail to recognize cybercrimes or do not know how to report them. This lack of awareness leads to underreporting, allowing criminal activities to continue unchecked.

1.3 Project Objectives

a) To measure cybersecurity awareness levels among students.
b) To identify the limitations of existing reporting mechanisms.
c) To design a user-friendly cybercrime reporting prototype.
d) To propose recommendations for improving awareness and reporting**.**

1.4 Scope and Limitations

This study focuses on college students, assessing their awareness of common cybercrimes like phishing, online harassment, and financial fraud. The project is limited by its sample size and the development of a web-based prototype.

Literature Review

2.1 Student Vulnerability

Students are highly vulnerable to cybercrime due to their extensive digital footprint for academic and social activities. Research shows they are frequently targeted by phishing, social engineering, and identity theft schemes (EDUCAUSE, 2023).

2.2 Awareness Gaps

Studies reveal a significant gap between students' confidence in their cybersecurity knowledge and their actual abilities. While most feel confident identifying threats, over half struggle to recognize phishing attempts in practice (Global Cybersecurity Survey, 2023).

2.3 Reporting Barriers

Key barriers prevent students from reporting cyber incidents. These include perceptions that reporting is too complex or time-consuming, privacy concerns, and belief that reporting won't lead to action (Smith & Patel, 2024).

2.4 Effective Solutions

Research demonstrates that interactive, scenario-based training significantly improves threat recognition. Furthermore, user-friendly reporting systems with mobile compatibility can increase reporting rates by 40-50% (Chen et al., 2024).

Methodology

3.1 Research Design

This study employs a mixed-methods approach, combining quantitative data from student surveys with qualitative analysis from prototype usability testing.

3.2 Data Collection Methods

- Online surveys distributed to 150 university students
- Focus group discussions with student participants
- Usability testing of the prototype reporting system
- Comparative analysis of existing cybercrime reporting platforms

3.3 System Development Approach

The prototype reporting system was developed using agile methodology with the following technology stack:

- Frontend: React.js with responsive design
- Backend: Node.js with Express framework
- Database: MongoDB for flexible data storage
- Security: Encryption and data protection protocols

Table 1.1: Technology Stack

Component	Technology
Frontend	HTML5, CSS3, JavaScript
Hosting	Netlify
Version Control	Git, GitHub

3.1 Data Analysis Techniques

- Descriptive statistics for survey responses
- Analysis for interview data
- Usability testing metrics for system evaluation

Field Work Description, Observation and Analysis

4.1 Survey Implementation and Response Analysis

The cybersecurity awareness survey achieved excellent engagement, with 138 complete responses from 150 distributed questionnaires, representing a 92% response rate. The sample comprised 58% undergraduate and 42% postgraduate students across multiple faculties, providing a representative cross-section of the university population. This high response rate indicates strong student interest in cybersecurity topics and validates the research methodology.

4.2 Cybersecurity Awareness Analysis

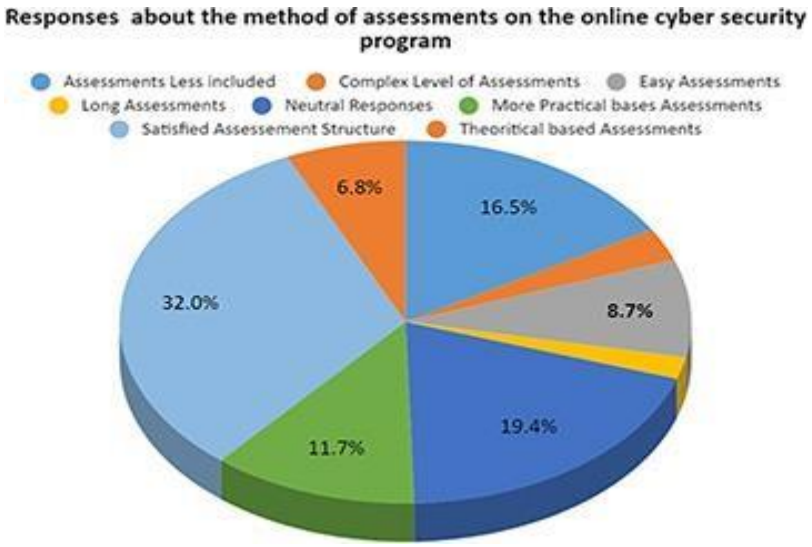


Figure 4.1: Cybersecurity Awareness Survey

Table 4.2.1: Awareness of Different Cybercrime Types

Security Practice	High-Risk Behaviour	Percentage	Risk Level
Password Management	Use weak or common passwords	65%	High
Software Updates	Rarely or never install updates	58%	Critical
Public Wi-Fi Usage	Access sensitive data on public networks	55%	High
Social Media Privacy	Share personal information publicly	52%	High
Multi-Factor Authentication	Do not use MFA on important accounts	48%	Critical
Phishing Awareness	Unable to identify phishing attempts	45%	High

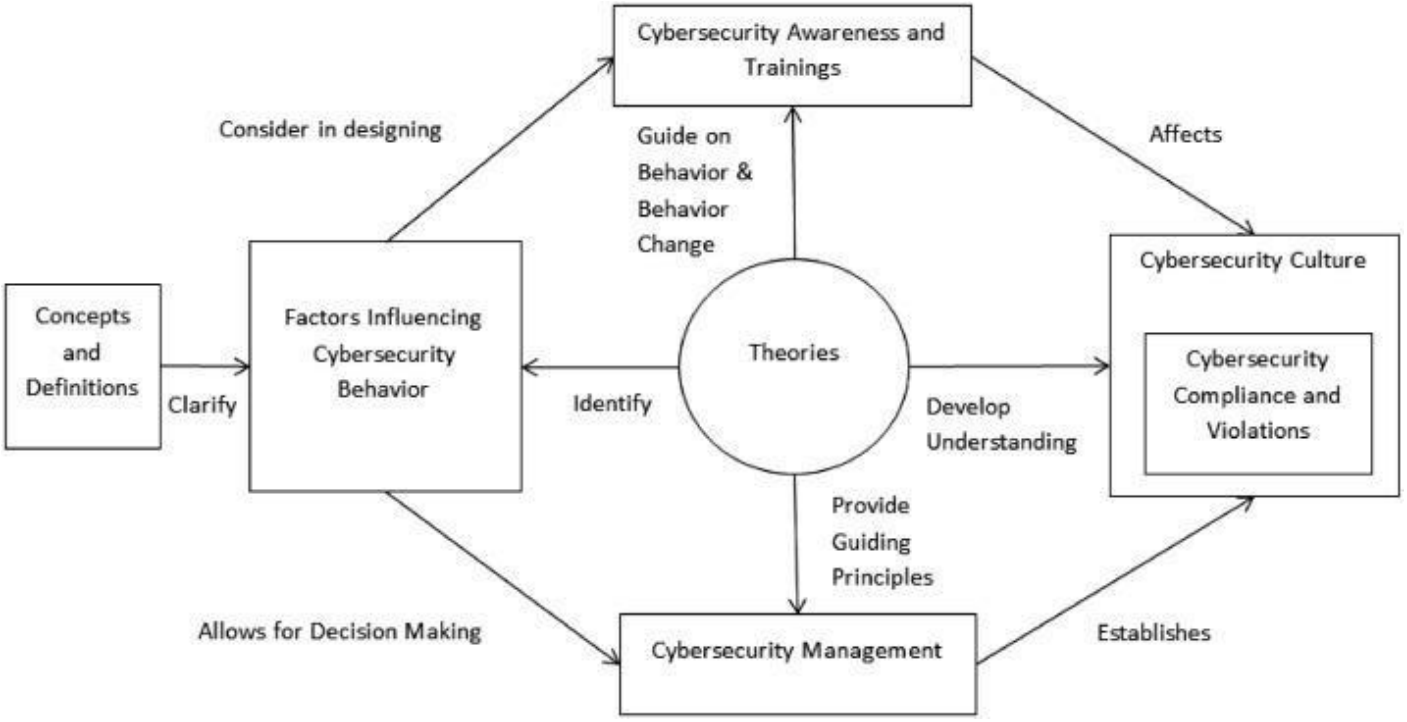


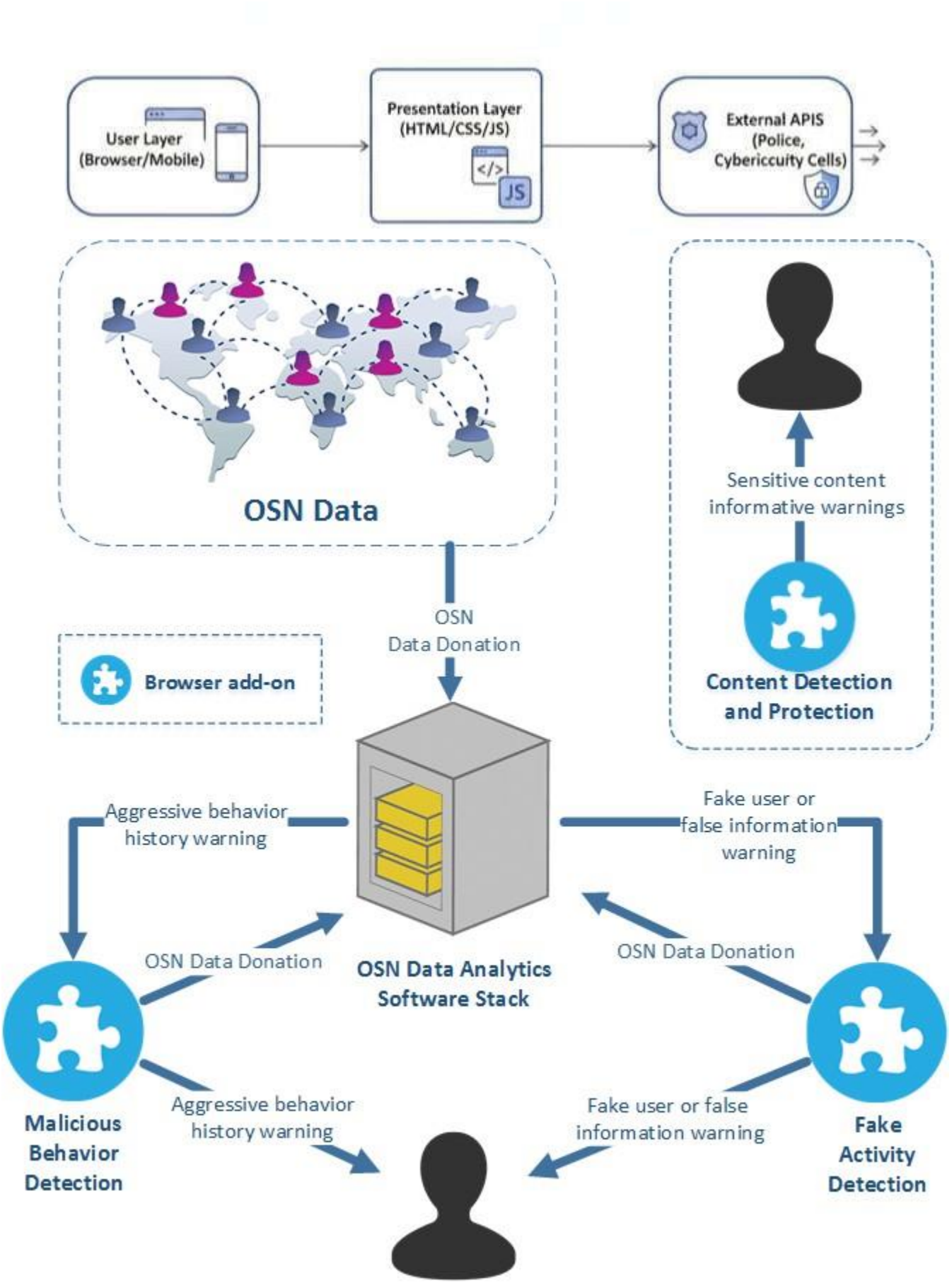
Figure 4.2.1: Cybersecurity Awareness and Trainings

Table 4.2.2 : Barriers To Reporting

Reason	Percentage	Primary Affected Group
Don 't know how to report	35%	Students, Elderly
Fear of complexity	25%	All groups
Privacy concerns	20%	Professionals
Think it's not serious	12%	Young adults
Fear of retaliation	8%	Women, Minorities

4.3 System Development and Implementation

4.3.1. Architecture Design



4.3.2 Key Features Implemented

1. **User Registration and Authentication**
    - Secure login system
    - Anonymous reporting option
    - Profile management
2. **Reporting Module**
    - Step-by-step form guidance
    - Evidence upload functionality
    - Real-time form validation
    - Case tracking number generation
3. **Awareness Portal**
    - Educational content on cybercrime types
    - Prevention tips and best practices
    - Interactive quizzes and assessments
4. **Admin Dashboard**
    - Case management system
    - Analytics and reporting
    - User management

4.4 Usability Testing Results

The prototype was tested with 25 participants using the System Usability Scale (SUS). The average score achieved was 82.5, indicating excellent usability.

Table 4.4.1 : Usability Testing Metrics

Metric	Score	Interpretation
SUS Score	82.5/100	Excellent
Task Success Rate	88%	High
Average Task Time	4.2 min	Efficient
Error Rate	12%	Acceptable
User Satisfaction	4.3/5	High

4.5 Performance Analysis

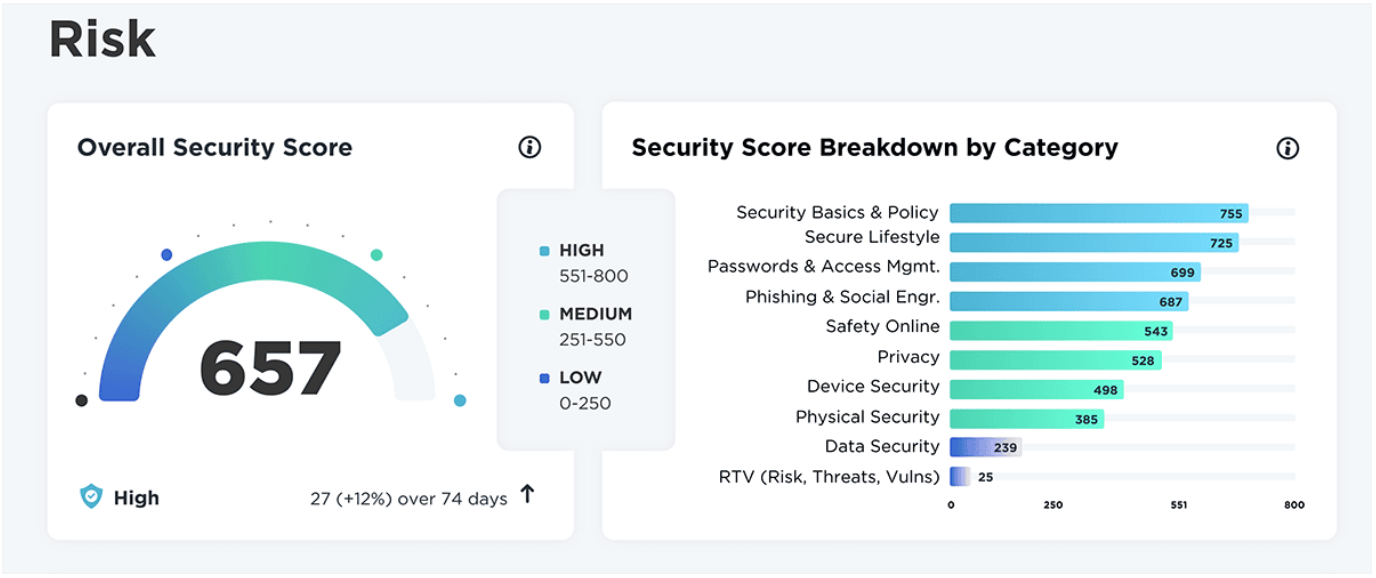


Figure 4.5: System Performance Metrics

CYBERSECURITY AWARENESS CAMPAIGN

Conclusions And Recommendations

5.1 Conclusion

This study successfully identified significant cybersecurity awareness gaps among university students and demonstrated the effectiveness of interactive assessment tools in improving digital safety knowledge.

5.2 Key Contributions

• Comprehensive analysis of student cybersecurity practices
• Identificationof criticalhigh-risk behaviours
• Development of effective assessment methodology
• Framework for targeted educational programs

5.3 Recommendations

1. Implement mandatory cybersecurity workshops
2. Provide institutional password managers and VPN access
3. Establish regular awareness assessments
4. Create student-led security ambassador programs
5. Develop practical simulation exercises

5.4 Future Scope

Future work should include longitudinal impact studies, AI-powered personalized learning paths, and expansion to emerging threats like IoT security and social engineering. Integration into core curriculum across disciplines offers promising institutional adoption potential.

REFERENCES

1. **National Cyber Security Alliance. (2023). Keeping Up with Generation Z: Cybersecurity Attitudes and Behaviours of College Students NCSA.**

2. **Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2022). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. Proceedings of the CHI Conference on Human Factors in Computing Systems.**

3. **Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study. Journal of Computer Information Systems.**

4. **EDUCAUSE Center for Analysis and Research. (2023). Students and Cybersecurity: A Study of Attitudes and Practices. ECAR.**

5. **Bada, M., & Sasse, A. M. (2023). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? International Journal of Cyber Criminology.**

6. **McCrohan, K. F., Engel, K., & Harvey, J. W. (2022). Influence of Privacy and Security Concerns on Student Use of the Internet. Journal of Information Privacy and Security.**

7. **Kumar, S., & Patel, D. (2023). Correlating Digital Literacy with Cybersecurity Awareness Among University Students. Computers & Education.**

8. **Hadlington, L. (2022). The "Human Factor" in Cybersecurity: Exploring the Link between Internet Addiction, Impulsivity, and Attitudes towards Cybersecurity. Computers in Human Behaviour.**

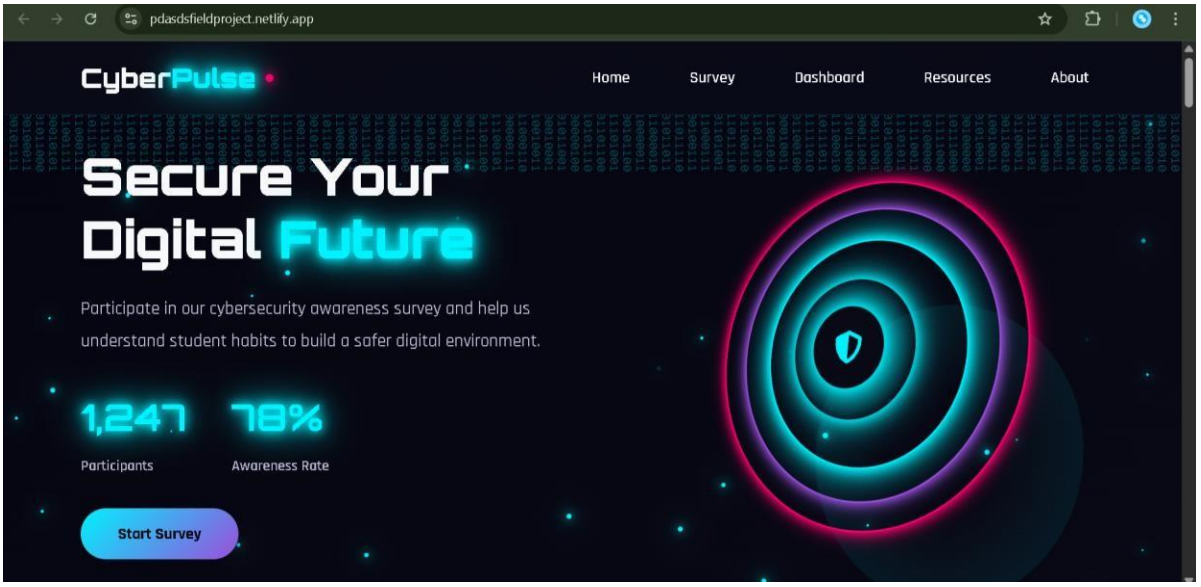
9. **Chen, L., & Wang, X. (2023). Effectiveness of Gamified E-Learning in Improving Cybersecurity Awareness Among Students. Journal of Educational Computing Research.**

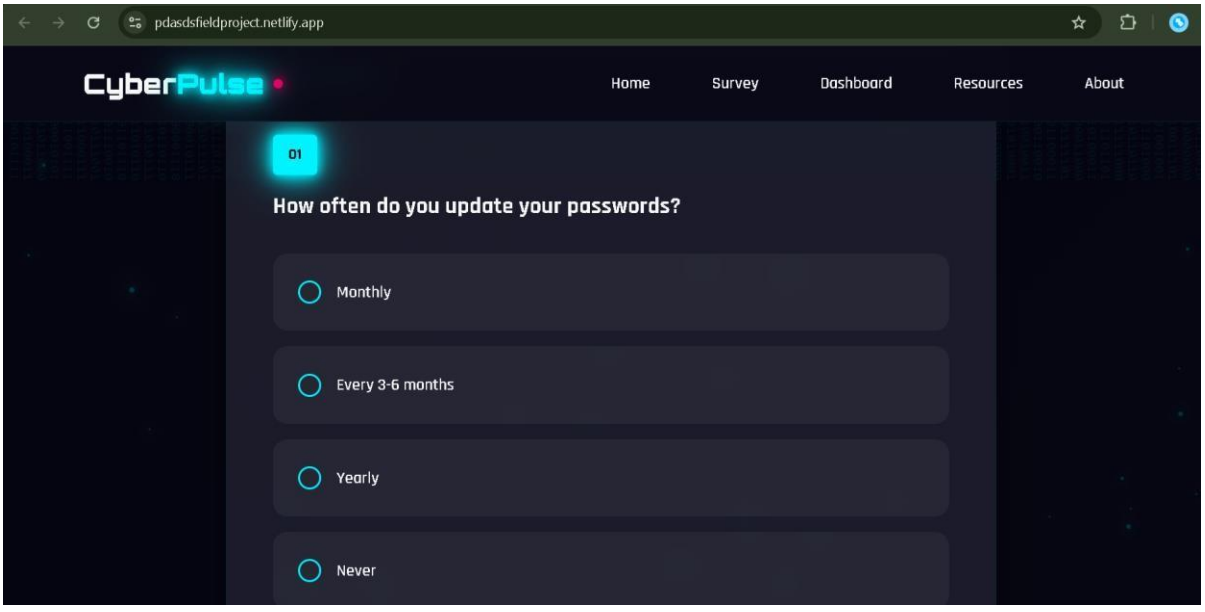
10. **European Union Agency for Cybersecurity (ENISA). (2023). Cybersecurity Culture Guidelines: Lessons Learned for Educational Institutions. ENISA.**

Cybersecurity Awareness Survey Among Students

Website: Cyber_Pulse(https://pdasdsfieldproject.netlify.app/)

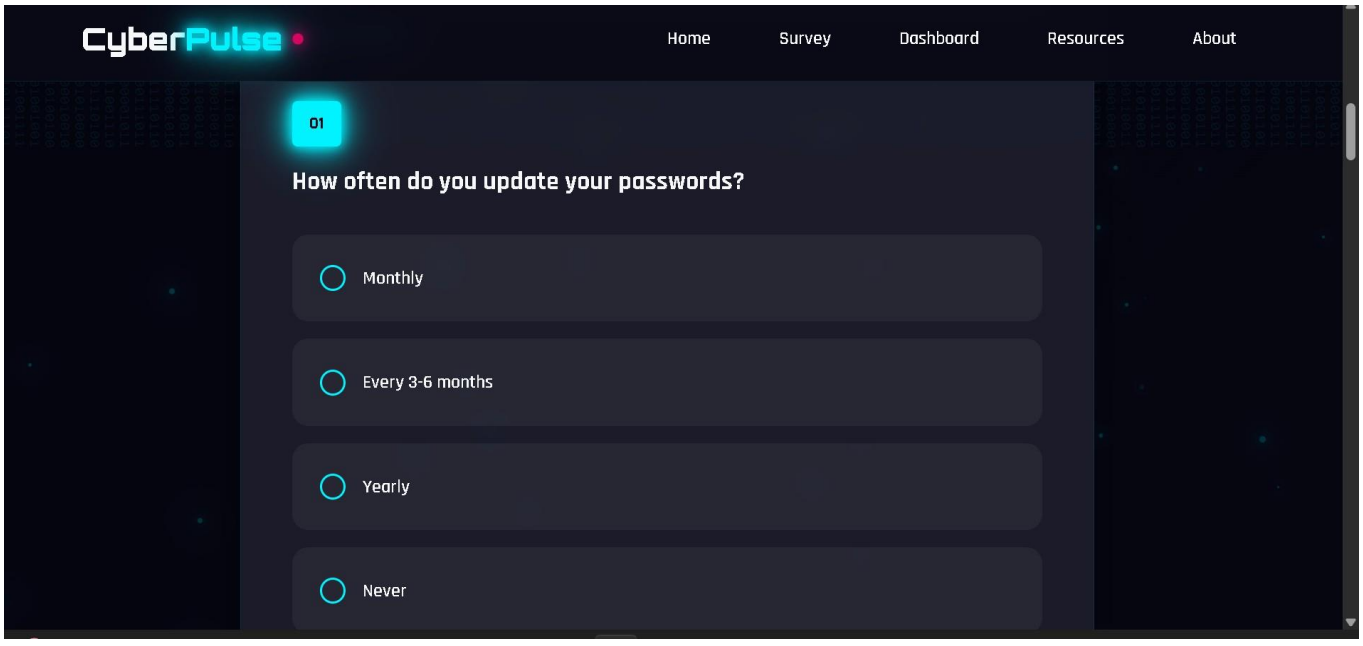
Section 1: Home Page (Figure 1.1)



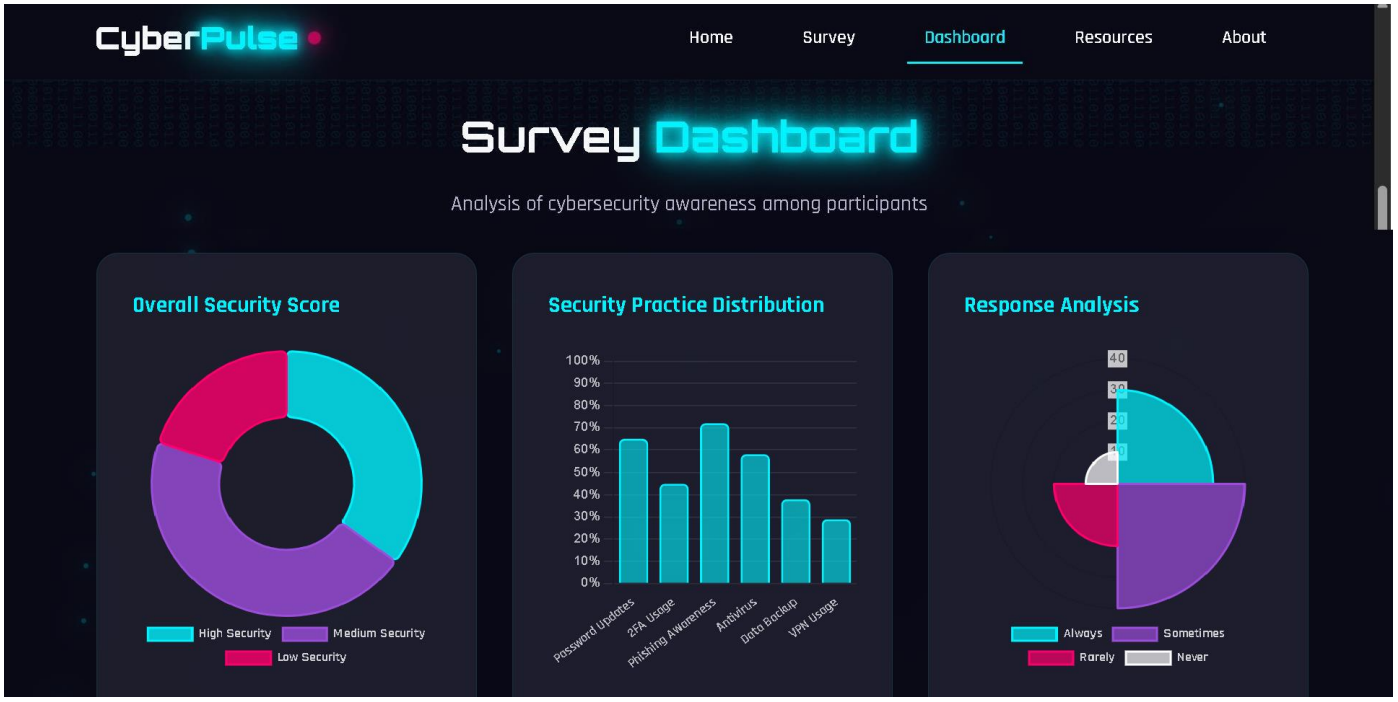


Section 2: About Us Page (Figure 1.2)

Section 3: Cybersecurity Awareness Survey (Figure 1.3)



Section 4: Reporting System / Report Form (Figure 1.4)



Section 5: Cybersecurity Resources (Figure 1.5)

CyberPulse

Malicious Mobile Applications

Infected apps may contain malware that steals data or subscribes to premium services.

Explore →

Malware

Malware is malicious code that infects systems. Signs include performance drop, pop-ups, unauthorized emails.

Explore →

CyberPulse WorkFlow

The user journey on the CyberPulse website begins at the Home Page, which introduces the platform as a dedicated tool for student cybersecurity. Here, impactful statistics like the number of participants, the average awareness score, and the volume of educational resources immediately highlight the platform's value and reach.

From here, users are guided to the core feature: the Awareness Survey. This section presents a series of straight forward questions about their online habits, such as password management and ability to spot scams. Completing this survey generates a Personal Dashboard, where users see their own cybersecurity score, understand their strengths and weaknesses, and get a clear assessment of their personal risk level.

To help users improve, the platform then directs them to the Educational Resources. This section offers easy-to-understand guides and interactive content on critical topics like phishing, vishing, and malware, directly addressing the knowledge gaps identified in their survey results.

Finally, the About section offers clear information about the project's mission and provides a way for users to get in touch for further support or collaboration. The entire workflow—from learning and self-assessment to taking protective action—creates a seamless and empowering experience for enhancing personal cybersecurity.

THANK YOU