FYP

Behaviorance-I

Farwah Butt (1101-2021)
Emaan Nadeem (2438-2021)
Hafsa khalid (2625-2021)

Supervisor
Umer Farooq

Department of Computing, FEST
Hamdard University

Summary

- Problem Statement
- Objective
- FYP Scope
- Our methodology
- Our Project Plan (Time lines)
- Budget / Costing (if any)
- FYP Deliverables
- Literature Review
- Demo of 100% of Work
- Experimental Evaluations & Results
- Test Plan & Test Cases
- References

Problem Statement

"Transforming the Weakest Link into the Strongest Defense"

- Organizations struggle with ensuring that employees adhere to security protocols, leading to vulnerabilities that can be exploited by malicious actors. The lack of a comprehensive platform that combines behavioral compliance with cybersecurity measures exacerbates this issue. There is an urgent need for an innovative solution that not only enhances cybersecurity posture but also fosters a culture of security compliance and awareness among employees.

Objective

- The project objective is to develop the smart human behavioral analysis based web application platform "**Behaviorance-I**", with the predictive assessment to forecast human behavior and potential vulnerable actions

FYP Scope

- The scope of project is limited to development of the **Behaviorance-I** web application platform with advanced integrated predictive cybersecurity and psychological assessment, build a comprehensive questionnaire bank, integration of cybersecurity and psychology principles into a unified framework.

Our Methodology

- **Evolutionary Prototyping** Development Methodology
- **WHY?**
- The evolutionary prototyping model combines incremental and extreme models. This model involves a series of prototyping refinements. The first assignment is to design and split the system into several independent modules. This model is used when the customers do not know the exact project requirements beforehand. The evolutionary model is suitable if trying to build a new product or technology that is not clearly understood at the moment.
-

Our Project Plan

Task	Start Date	End Date	Assigned To	Status
Project Planning	01 July 2024	15 July 2024	Farwah, Emaan, Hafsa	Planned
Literature Review/Competitive Analysis	15 July 2024	12 Aug 2024	Farwah, Emaan, Hafsa	Planned
Identifying Factors	12 Aug 2024	26 Aug 2024	Farwah	Planned
Design Platform	26 Aug 2024	21 Oct 2024	Emaan, Hafsa	Planned
Design Questionnaire	21 Oct 2024	02 Dec 2024	Farwah	Planned
Integrate CybPsy Principals	02 Dec 2024	27 Jan 2025	Farwah, Hafsa	Planned
Predicting Human Behavior	27 Jan 2025	24 Feb 2025	Farwah	Planned
Design Assessment Report	24 Feb 2025	07 Apr 2025	Emaan	Planned
Evaluate Performance	07 Apr 2025	07 May 2025	Farwah, Emaan, Hafsa	Planned
Documentation	07 May 2025	1 July 2025	Emaan	Planned

Budget / Costing

- Estimated budget of project major resources
-
- - Developers (3 @ 700 x 4days x 4 week = 33600 x 12 = PKR 403,200 est.)
- - Hard Drive (Rs. 14,000 x 2 = PKR 28,000 est.)
- - Laptop (Rs. 150,000 x 3 = PKR 450,000 est.)
- - Electricity (Rs. 5000 x 12 = PKR 60,000 est.)
- - Internet (3000 x 12 = PKR 36,000 est.)
- - Industry Expert Consultancy (expected 2-4 visits) 8000 x 2 = PKR 16,000 est.
- - LaserJet Printer 16,000
- - Miscellaneous PKR 10,000 est.
-
- Total cost PKR 1,118,200 est.

FYP Deliverables

FYP-I Evaluation

- Project Plan
- S R S
- S D S
- Project Budget
- Database Design
- Platform Prototype
- Project Report – I
- Research Paper (Optional)

FYP-II Evaluation

FYP Demo & Display

Poster

Project Report – II

Research Paper (Optional)

Literature Review

- **Abstract**
- Traditional cybersecurity tools focus mostly on technical defenses, ignoring the human element. This review explores how behavioral compliance can improve organizational security by analyzing user behavior. It highlights the gaps in current systems and discusses how AI and behavioral tools like Behaviorance-I can help build more proactive security strategies.

Literature Review

- **Introduction**
- Most security breaches are caused by human actions, not just technical failures. While tools like firewalls and antivirus are important but they miss the human factor. Behaviorance-I takes a people-first approach, analyzing employee behavior to detect risk and promote awareness. This review looks at existing solutions and how AI can make them more effective.

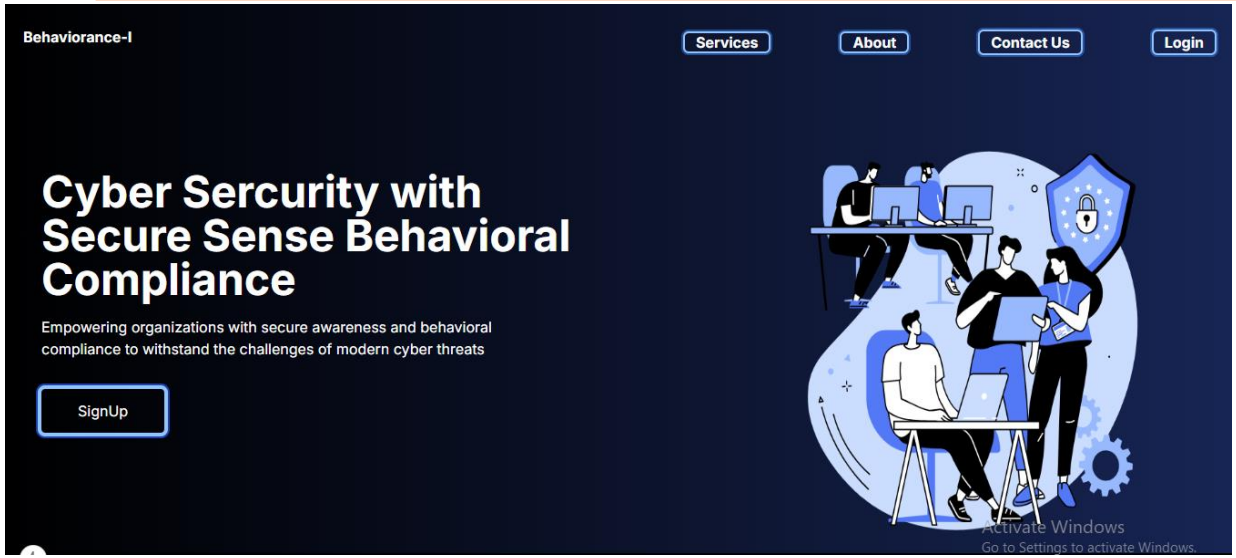
Literature Review

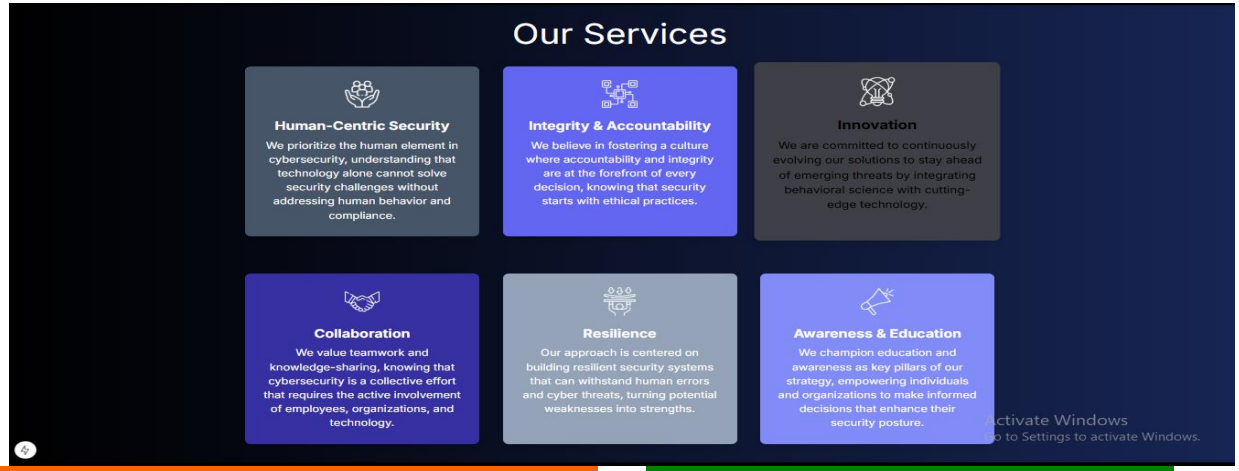
- **Related Work**
- **Qualtrics:**
  A widely used online platform for surveys, analytics, and feedback. Known for real-time analysis, customizable forms, and strong data security. Supports GDPR and HIPAA compliance and integrates with tools like Tableau and Salesforce.
- **SurveyMonkey:**
  Another popular tool for building and analyzing surveys. Offers custom templates, logic-based questions, and app integrations. Commonly used for market research, employee feedback, and academic studies.

Gap Analysis

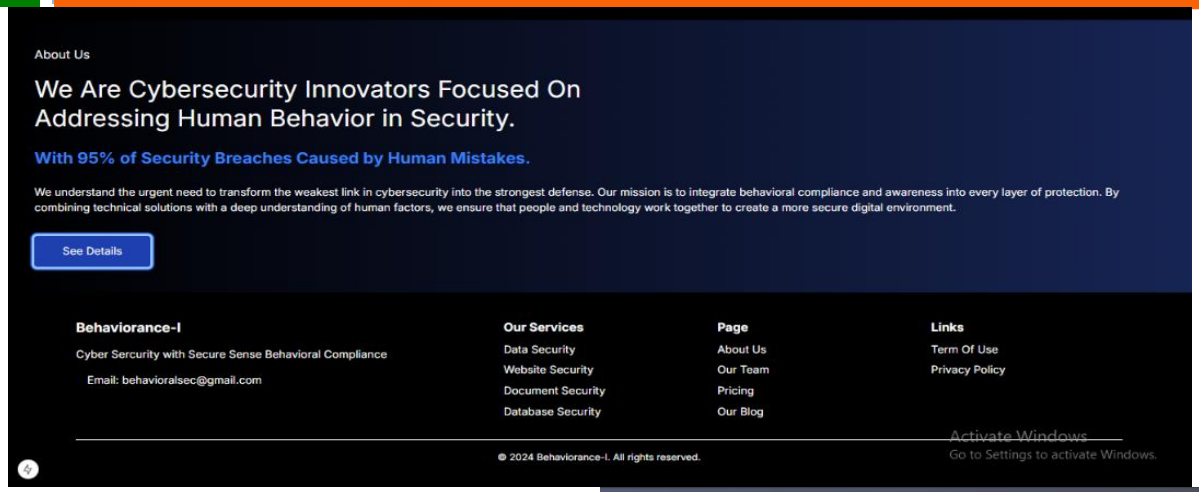
Web Type	Behaviorance-I	Qualtrics	SurveyMonkey
Offerings	Security awareness, analyzing basic knowledge of cyberSecurity and also provide pre-built domains	Advanced surveys, experience management.	Simple surveys, feedback tools, export features.
Features	Customize survey, use ML for suggestions	Advanced tools, AI insights, integrations.	Easy survey builder, templates, basic logic tools.
Target Audience	Individuals, organizations for behavior improvement.	Enterprises, researchers, HR professionals.	Small businesses, non-profits, individuals needing quick surveys.
Usability	User-friendly, quick setup, limited database.	Complex but powerful for professionals.	Beginner-friendly, quick setup.

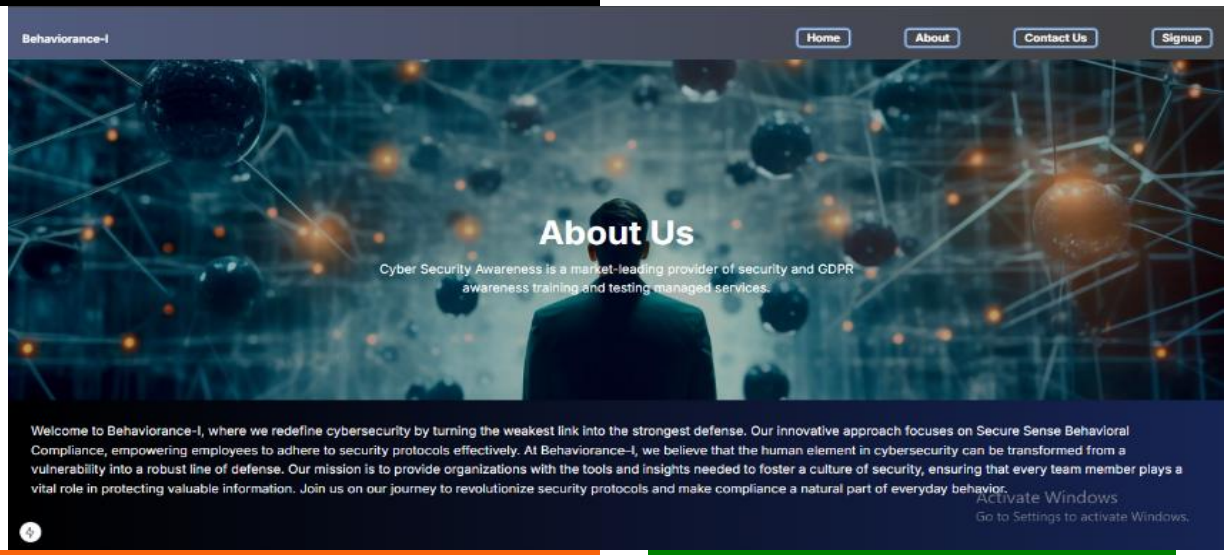
Demo of 100% of Work





Demo of 100% of Work





Demo of 100% of Work

Our mission

Our mission is to empower businesses by providing solutions that make cybersecurity compliance intuitive and engaging for every team member. We believe that when employees understand the 'why' behind security protocols and see them as a part of their daily routine, they become active defenders against cyber threats.

Our Approach

Our Approach Behavioral Insights: We use advanced analytics to understand employee behavior, identifying areas where compliance may be lacking and providing targeted interventions to address these gaps. Training and Engagement: Our platform offers interactive training modules and gamified experiences that make learning about cybersecurity engaging and memorable. We turn complex security protocols into manageable and actionable habits. Continuous Monitoring and Feedback: Behaviorance-I provides real-time feedback and continuous monitoring to ensure ongoing compliance. Our adaptive approach evolves with the needs of your organization, ensuring that security is never static. Employee-Centric Solutions: We prioritize the user experience by designing solutions that fit seamlessly into daily workflows, reducing friction and increasing adoption rates. Our goal is to make security compliance as effortless as possible.

Behaviorance-I

Cyber Sercurity with Secure Sense Behavioral Compliance

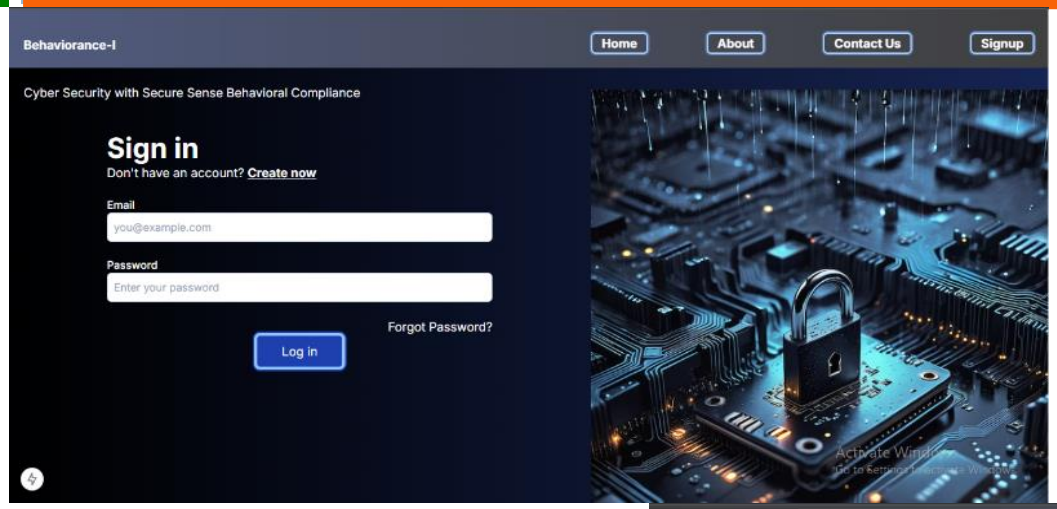
Email: behavioralsec@gmail.com

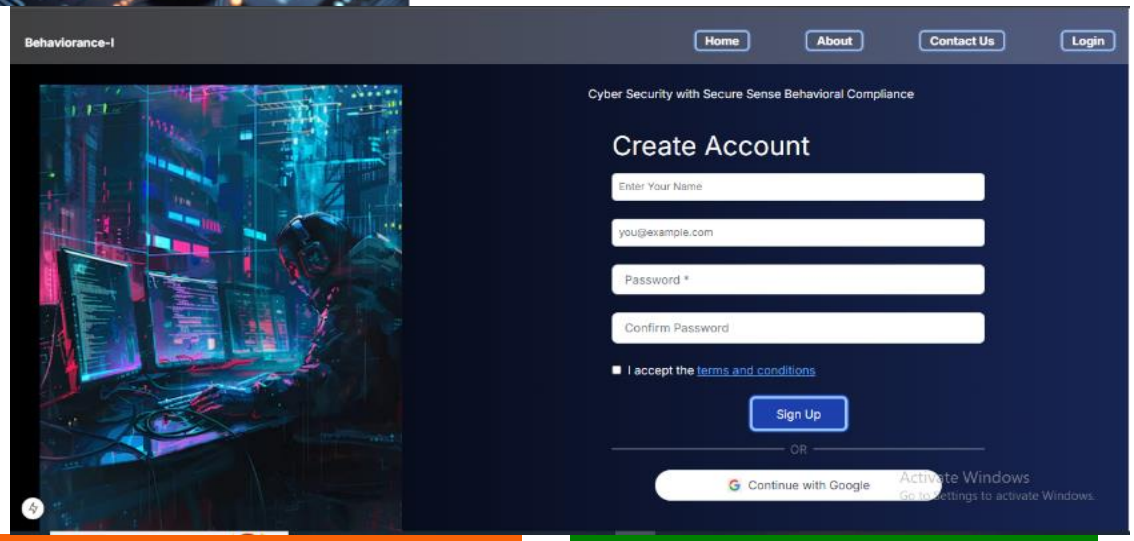
Our Services
- Data Security
- Website Security
- Document Security
- Database Security

Page
- About Us
- Our Team
- Pricing
- Our Blog

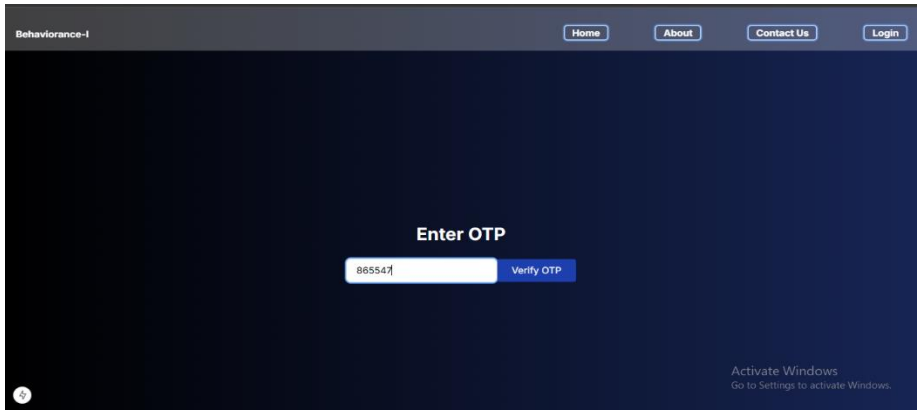
Links
- Term Of Use
- Privacy Policy

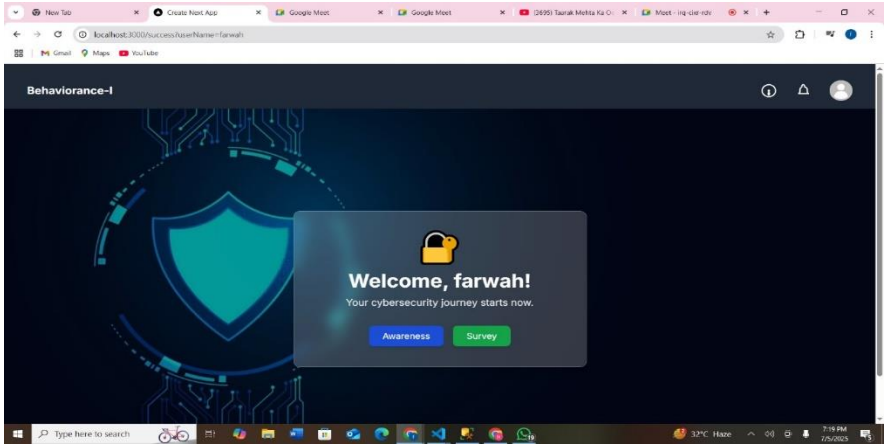
Demo of 100% of Work

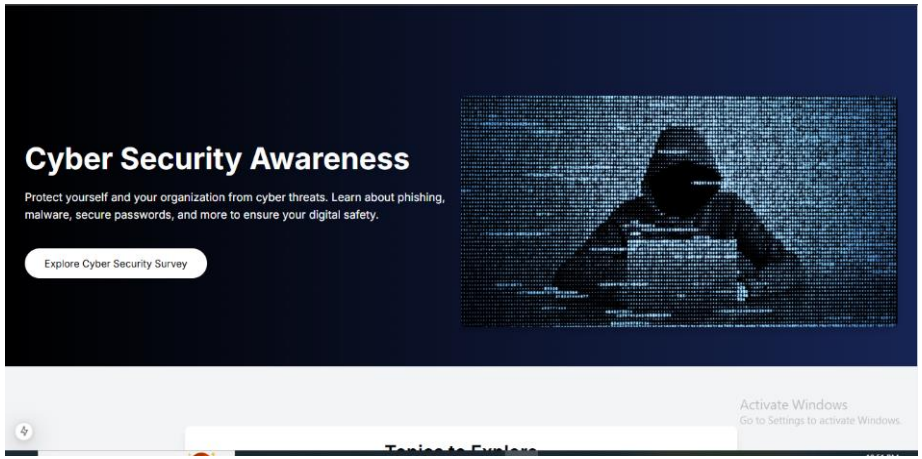


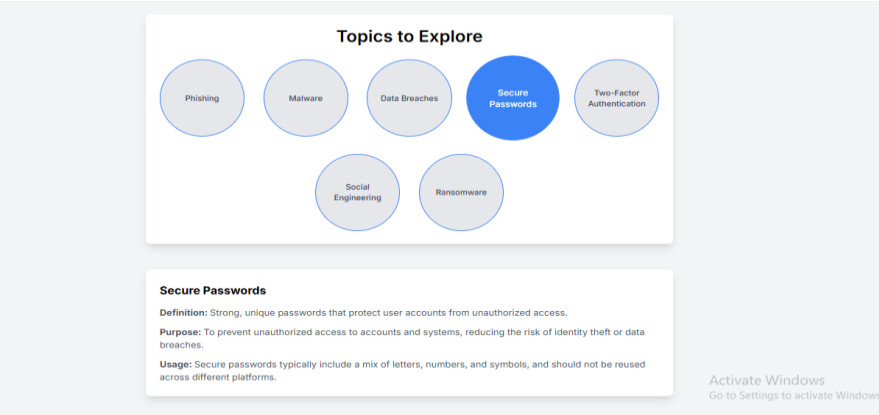


Demo of 100% of Work

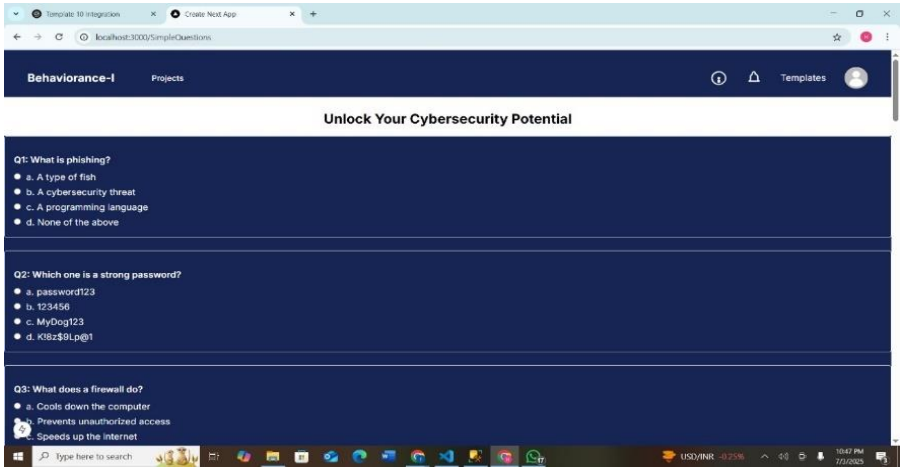


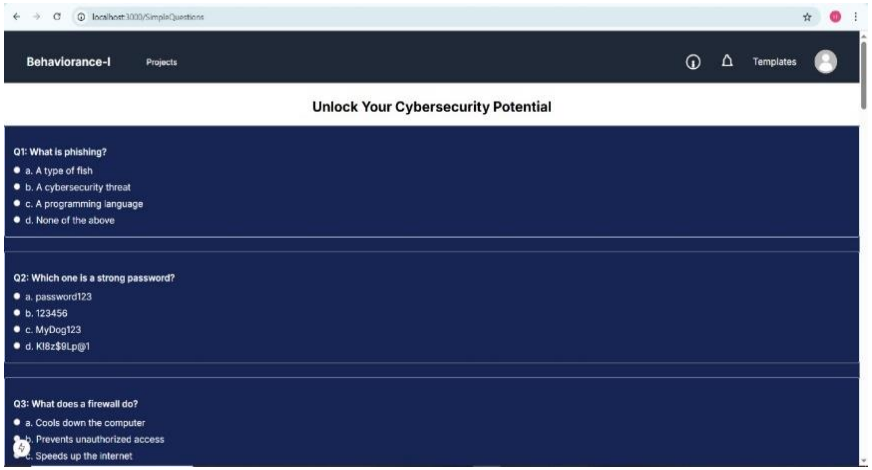


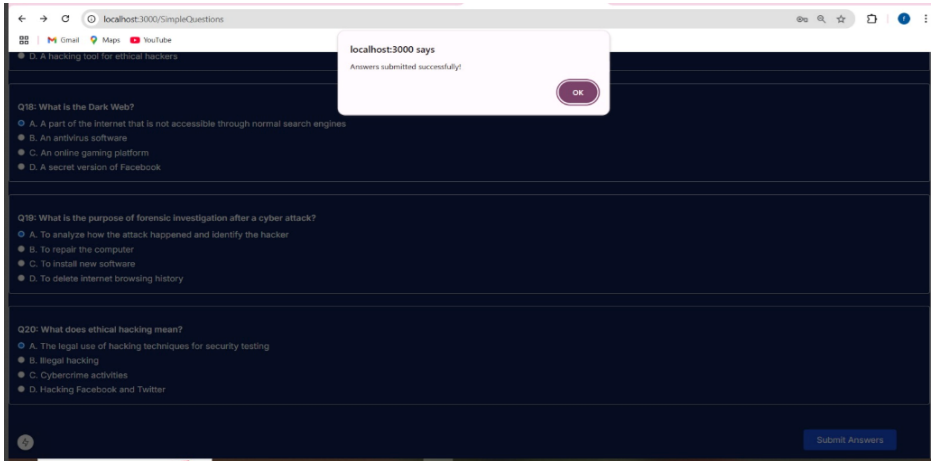


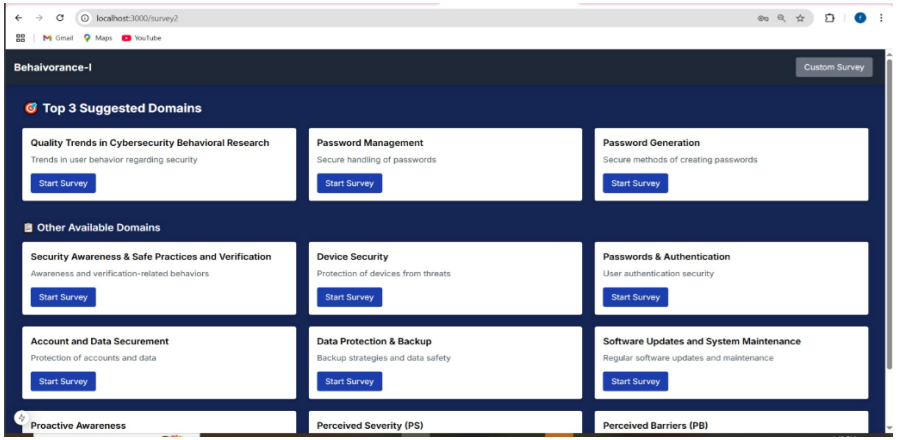


Demo of 100% of Work

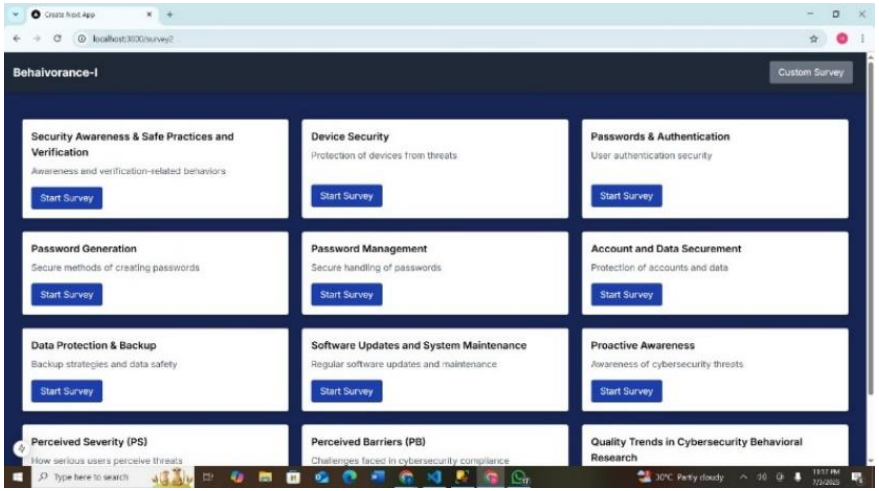


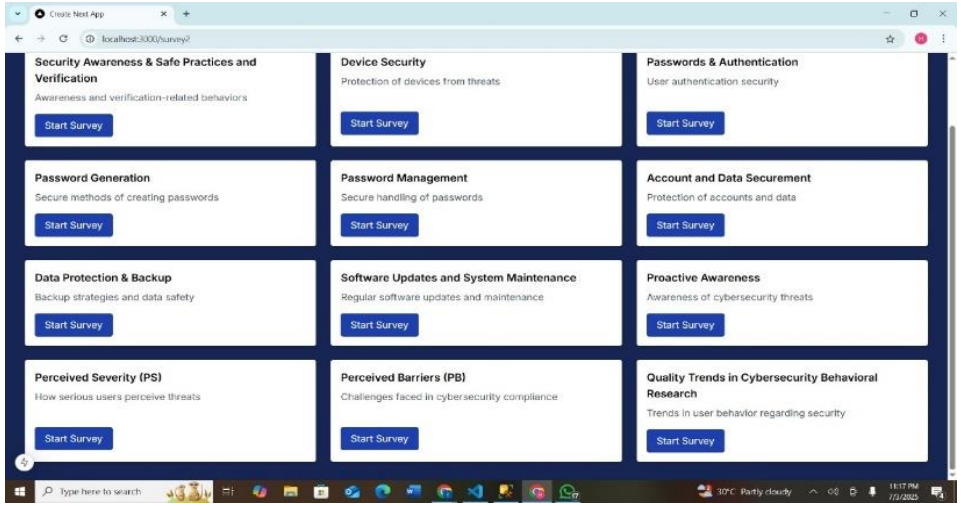


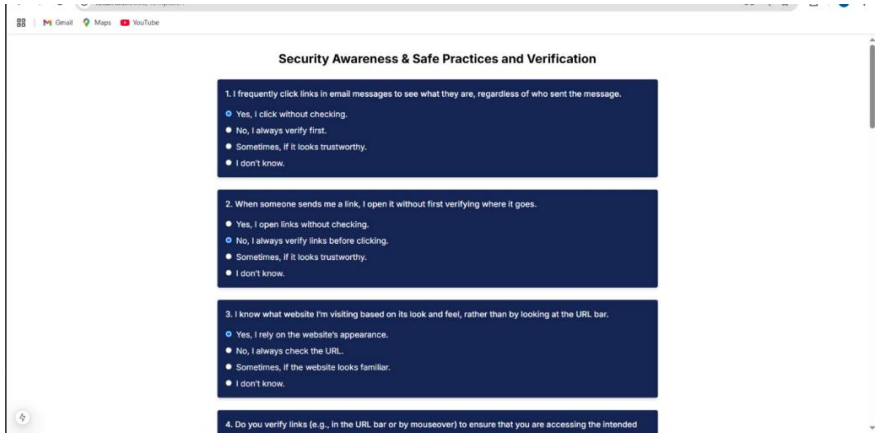


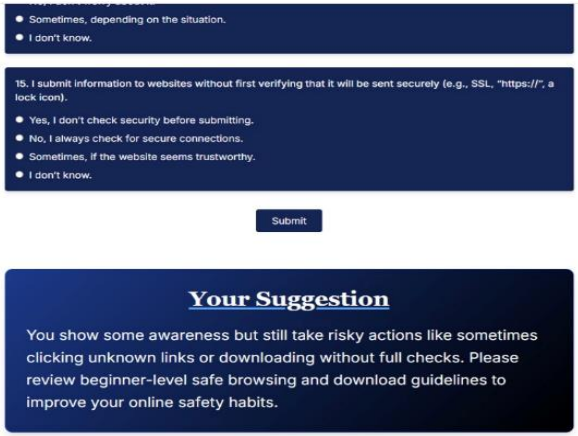


Demo of 100% of Work

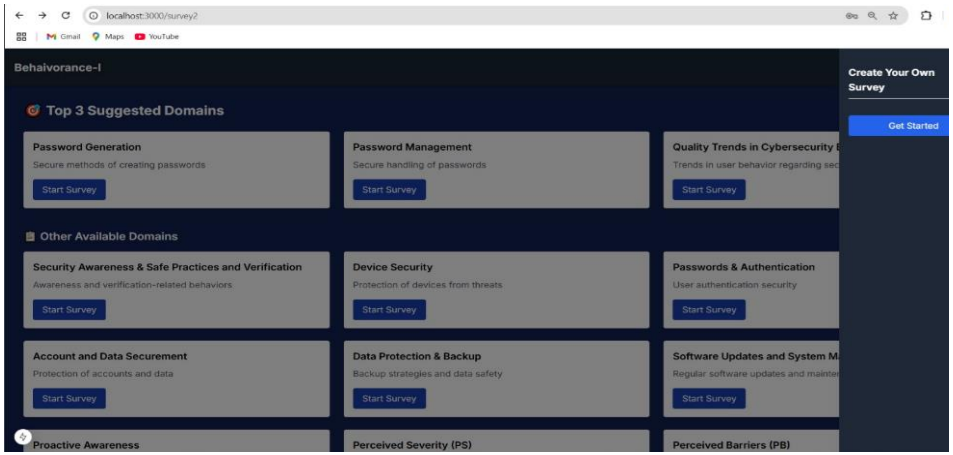


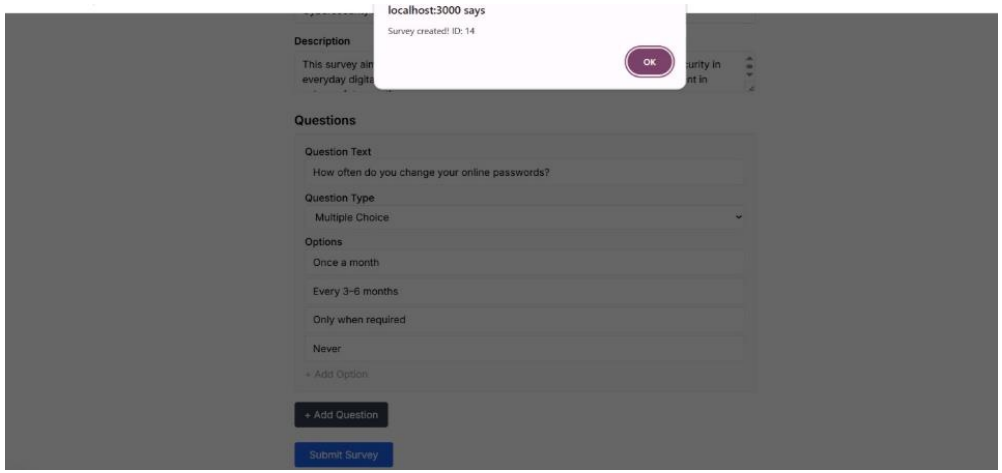


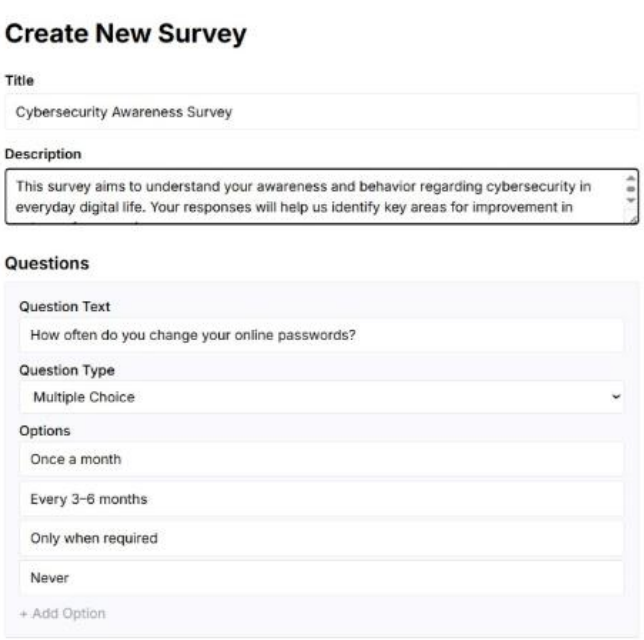




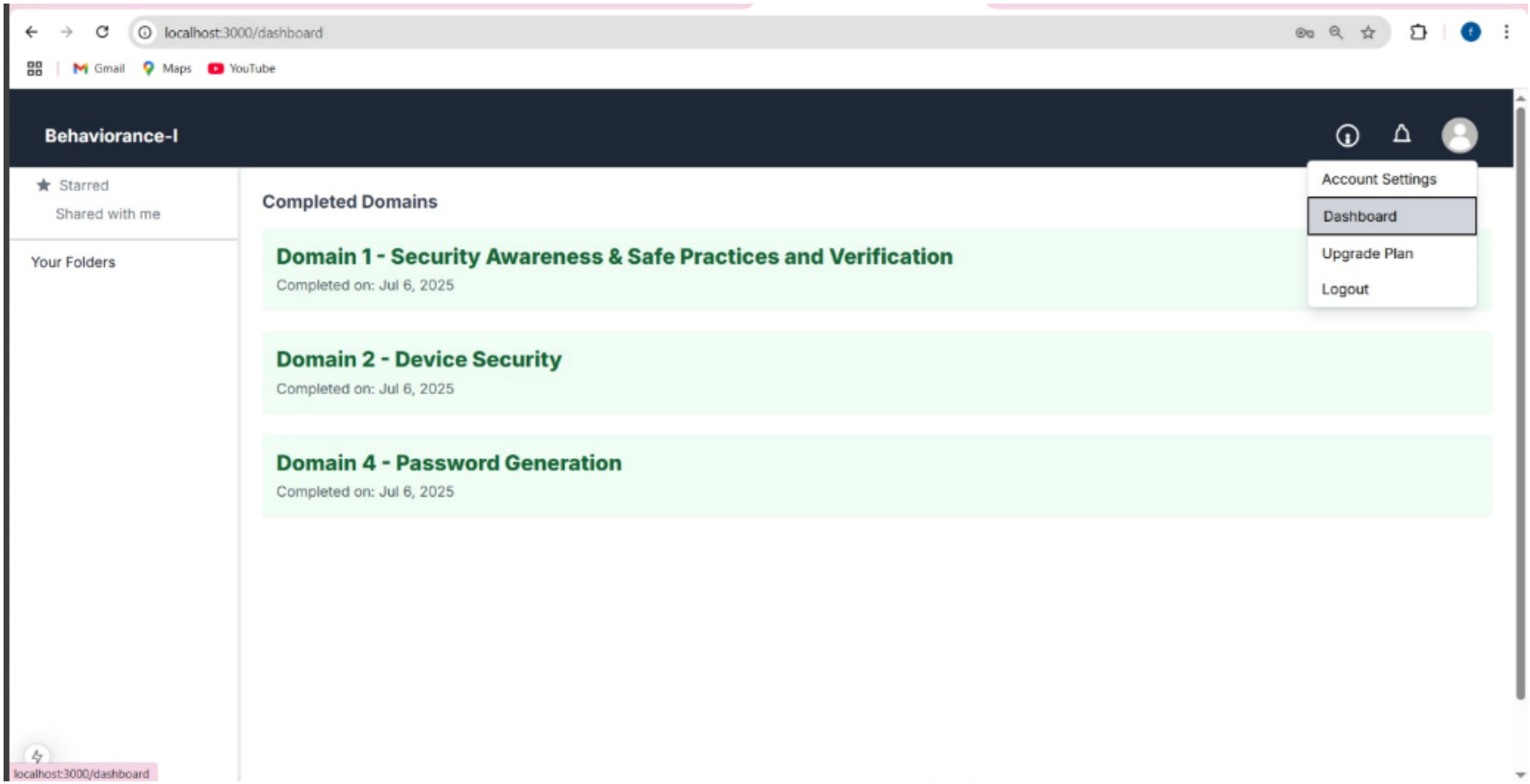
Demo of 100% of Work



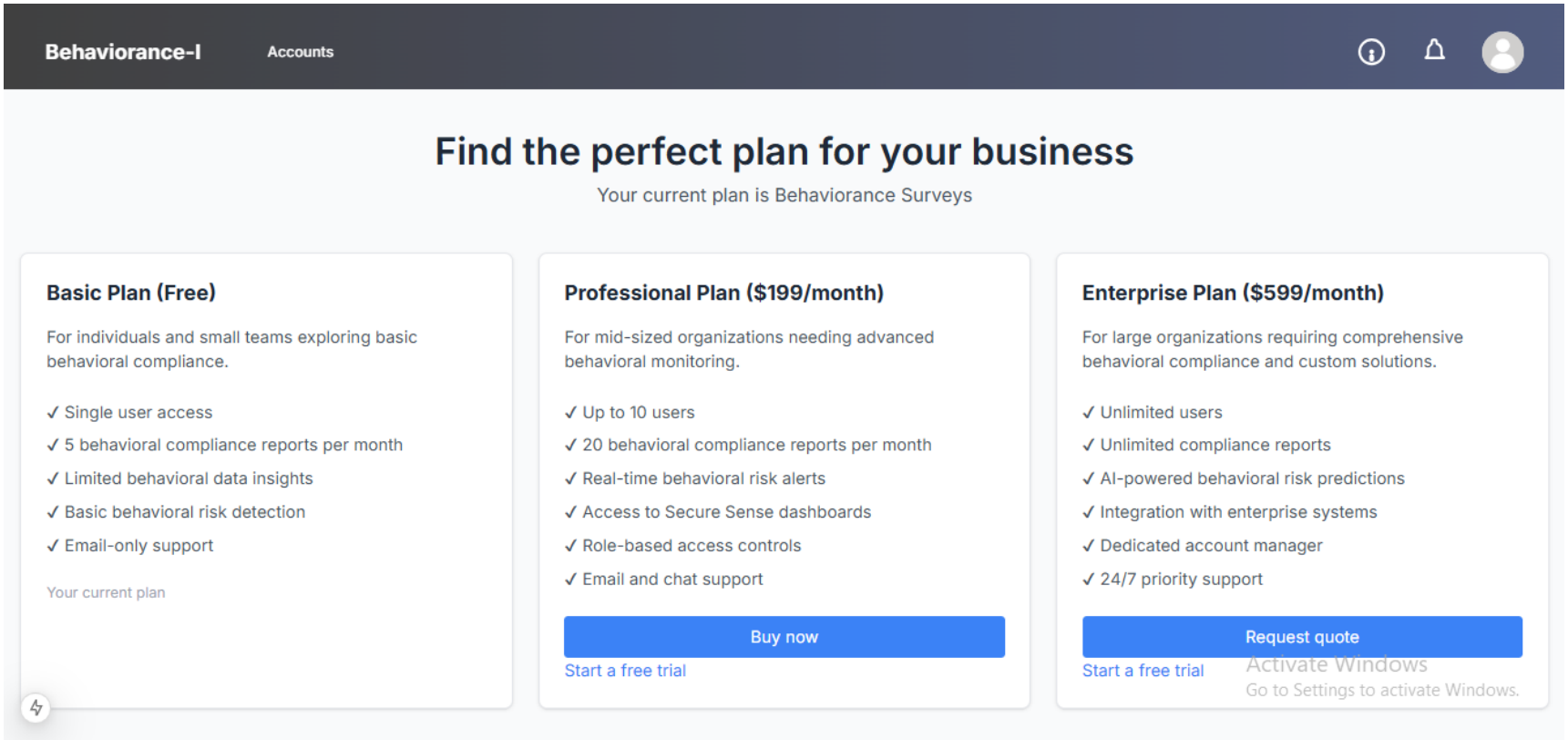




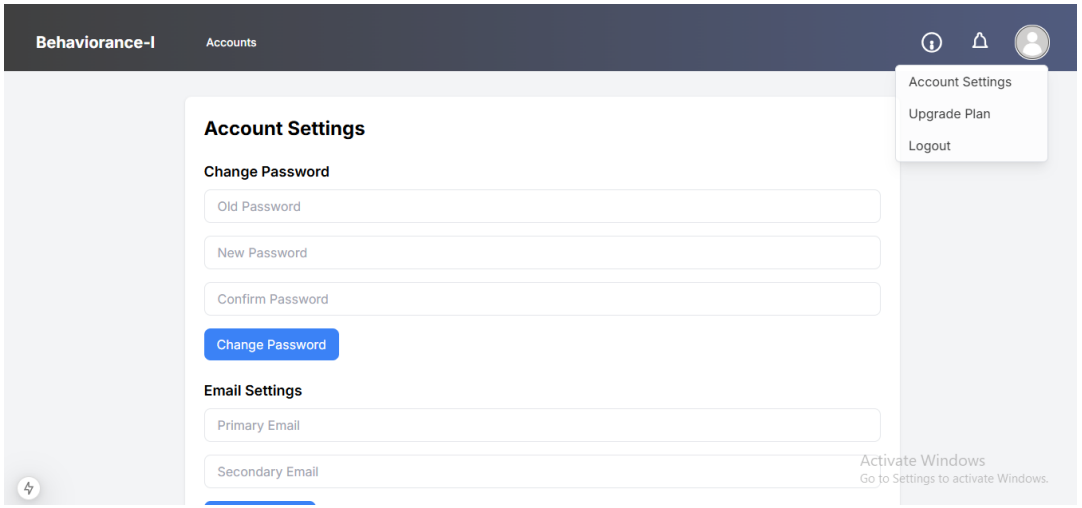
Demo of 100% of Work

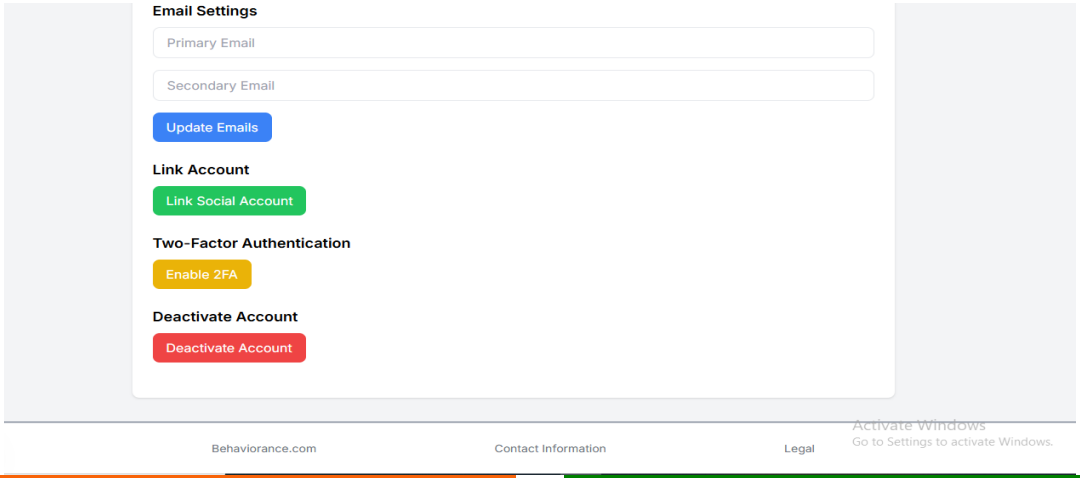


Demo of 100% of Work



Demo of 100% of Work





Experimental Evaluations & Results

- **Evaluation Testbed**
- The Behaviorance-I platform was tested in a simulated work environment to check its performance and accuracy.
- **Hardware Used:**
  3 laptops (Core i7, 16 GB RAM), external drives, printer, stable internet
- **Software Stack:**
  Frontend & backend: Next.js, Database: MS SQL, Custom survey, ML: K-mean
- **User Roles Simulated:**
  Admin, Employee, and System Analyst
- **Testing:**
  Real user inputs were used. Surveys, dashboards

Experimental Evaluations & Results

- **Results and Discussion**
- The system worked well in login, form submission, risk prediction and custom survey.
- Provide domains based on checking the user knowledge.
- Risk levels were calculated correctly using questionnaire responses.
- User's dashboard was easy to use and showed the user history.
- Minor issues (layout, slow loading) were fixed during testing.
- No data loss or system failures occurred.
- Overall, the system improved cybersecurity awareness by focusing on human behavior.

Experimental Evaluations & Results

- **Conclusion of Evaluation**
- Behaviorance-I met all its key goals.
  It performed reliably, gave accurate risk predictions, and was well-received by users.
  The platform is ready for real organizational use and has strong potential for future upgrades like better analytics and security tool integration.

Test Plan & Test Cases

- **1. Purpose**
- The purpose of this test plan is to verify the functional behavior of the **Behaviorance-I** platform. It outlines the key components tested to ensure the platform is stable, secure, and functions as intended across different user roles and scenarios.
- **2. Scope**
- This test plan covers the following key modules:
- User authentication (Login with OTP)
- Provide Awareness
- Check user basic knowledge
- Questionnaire submission
- Suggestions
- Admin functionality
- Error handling
- Machine learning risk prediction

Test Plan & Test Cases

- **3. Test Objectives**
- Confirm that users can log in securely using valid credentials.
- Ensure that the suggested domains are correctly shown based on user knowledge.
- Ensure the questionnaire can be submitted, stored, and acknowledged.
- Verify that the system calculates and displays the correct suggestions.
- Validate admin capabilities, including adding new questionnaires.
- Test system handling of incomplete inputs and incorrect OTPs.
- Check that ML logic correctly identifies risk and provides suggestions.

4. Testing Approach

- The testing approach includes:
- **Manual Testing:** Step-by-step execution of test cases
- **Black Box Testing:** Focusing on input/output without internal code access
- **Positive and Negative Testing:** Testing both valid and invalid user actions

Test Plan & Test Cases

6. Environment Setup

- **Frontend/Backend:** Next.js and Next.js API Routes
- **Database:** MSSQL, ML: K-mean
- **Devices Used:** Windows laptops with latest browsers
- **Browser Compatibility:** Chrome, Edge, Firefox tested

7. Entry & Exit Criteria

- **Entry:** All modules must be integrated, and test data prepared.
- **Exit:** All test cases must be executed and pass successfully, with bugs (if any) resolved.

8. Conclusion

- All major test cases were executed successfully, and the system performed reliably. The platform is ready for deployment and can be enhanced further with real-user feedback and extended test coverage.

Test Plan & Test Cases

Test Case ID	Description	Input	Expected Output	Status
TC01	User Login with valid credentials and incorrect OTP	Valid email + password + OTP / Valid email/password but wrong OTP	Redirect to Home Page / Show error message “Invalid OTP”	Pass
TC02	User Login with invalid credentials	Invalid email or password	Show error message “Incorrect email or password”	Pass
TC03	Questionnaire submission	Answers to 15 questions	Store responses + display acknowledgment	Pass
TC04	Admin adds new questionnaire	Questionnaire title + questions	Updated bank appears in user module	Pass
TC05	Data not saved with incomplete survey	Partial questionnaire responses	Prompt error + prevent submission	Pass
TC06	ML model gives accurate prediction	High-risk behavior pattern	Analyze risk behavior and give suggestion	Pass
TC07	Domains are correctly suggested based on user knowledge	User anwers the basic knowledge questions	Show relevant domains tailored to user’s knowledge	Pass

Reference

- 1. Kannelønning, K. and Katsikas, S.K. (2023) 'A systematic literature review of how cybersecurity-related behavior has been assessed', Information & Computer Security, 31(4), pp. 463–477. Available at: https://doi.org/10.1108/ICS-08-2022-0139.
- 2. Almansoori, A., Al-Emran, M. and Shaalan, K. (2023) 'Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories', Applied Sciences, 13(9), p. 5700. Available at: https://doi.org/10.3390/app13095700.
- 3. Rohan, R. et al. (2023) 'A systematic literature review of cybersecurity scales assessing information security awareness', Heliyon, 9(3). Available at: https://doi.org/10.1016/j.heliyon.2023.e14234.
- 4. Khan, N.F. et al. (2022) 'The cybersecurity behavioral research: A tertiary study', Computers & Security, 120, p. 102826. Available at: https://doi.org/10.1016/j.cose.2022.102826.
- 5. Rohan, R. et al. (2021) 'Understanding of Human Factors in Cybersecurity: A Systematic Literature Review', in 2021 International Conference on Computational Performance Evaluation (ComPE). IEEE, pp. 133–140. Available at: https://doi.org/10.1109/ComPE53109.2021.9752358
- 6. Rahman, T. et al. (2021) 'Human Factors in Cybersecurity: A Scoping Review', ACM International Conference Proceeding Series [Preprint]. Available at: https://doi.org/10.1145/3468784.3468789.

THANK YOU