**Phishing Awareness Dashboard Project Report**

**Date:** January 26, 2016

**Assessor:** Nikhil Babu Jakkam

**1. Executive Summary:**

This report details the design, implementation, and delivery of the Phishing Awareness Dashboard - a crucial tool to evaluate and educate employees on the importance of recognizing and resisting phishing attempts. This initiative is in line with our goal to strengthen our organizational cybersecurity posture by focusing on the most common vulnerability: human behavior.

**2. Project Objective:**

**Primary Objective:** To develop a user-friendly dashboard allowing employees to access educational materials on phishing and view their performance metrics from simulated phishing campaigns.

**3. Project Scope:**

1. Design a simple, intuitive web interface.
2. Incorporate login functionality to personalize user experience.
3. Provide links to educational materials.
4. Display performance metrics from phishing campaigns.

**4. Methodology:**

The project utilized the Flask web framework because of its lightweight nature and ease of use. Flask-Login was chosen for authentication functionality.

**5. Implementation Details:**

**5.1. System Design:**

* **Frontend:** Utilized HTML templates (login.html and dashboard.html).
* **Backend:** Python's Flask framework handled routing and user session management.

**5.2. Directory Structure:**

**Code**: *“/phishing-awareness-dashboard /templates login.html dashboard.html app.py README.md requirements.txt”*

**6. User Authentication:**

Users log in using predefined credentials. Successful authentication grants access to the dashboard, while failed attempts redirect back to the login page.

**7. Results & Metrics Display:**

On successful login, users see a personalized greeting and can access resources detailing phishing risks and preventive methods. (Future implementation will include displaying user-specific performance metrics from phishing campaigns.)

**8. Deployment and Testing:**

The application was tested locally and is ready for deployment on a web server. Continuous integration and deployment tools can be added in future iterations.

**9. Conclusions & Recommendations:**

The Phishing Awareness Dashboard serves as a foundational tool for continuous phishing awareness training. However, continuous improvement is recommended:

1. **User Metrics:** Integrate with the phishing simulation tool to fetch real-time metrics.
2. **Interactive Quizzes:** Incorporate quizzes to test user knowledge and provide instant feedback.
3. **Multi-Factor Authentication:** Enhance security for user logins.

**10. Acknowledgments:**

Gratitude is extended to the IT and legal teams for their collaborative efforts in ensuring this project not only served its educational purpose but also adhered to all ethical guidelines.

**11. Conclusion:**

The Phishing Awareness Dashboard project was initiated in response to the rising threats posed by phishing attacks, recognizing that even the most robust technical defenses can be compromised through human error. By providing an educational platform coupled with real-world simulation metrics, our aim was to empower employees with the knowledge to discern potential threats and act judiciously.

The successful implementation of this dashboard signifies a step forward in our proactive approach to cybersecurity. Its user-friendly design ensures maximum engagement, making cybersecurity education more accessible to all employees, irrespective of their technical acumen.

Moving forward, we understand that cybersecurity threats evolve, and as such, our training methods must adapt. This dashboard will not only serve as a foundation for current training needs but will be pivotal in iterative enhancements, ensuring our workforce remains vigilant against future phishing attempts.

By prioritizing the human element in our cybersecurity strategy, we are not just defending against potential breaches, but fostering a culture of awareness and responsibility. Through initiatives like this dashboard, we are taking holistic strides in ensuring our organization's digital safety, reaffirming our commitment to both our employees and stakeholders.