AIML Tool for Phishing Domain Detection Capstone Project Scope Document

1. Project Overview

1.1 Project Title:

• AIML Tool for Phishing Domain Detection

1.2 Project Objectives:

• Develop an AI/ML-based tool capable of accurately detecting phishing domains in real-time.

• Achieve a high level of precision and recall in identifying malicious domains.

• Enhance user awareness of potential phishing threats through an intuitive user interface.

1.3 Project Background:

• Phishing attacks continue to pose a significant threat to cybersecurity. This project aims to leverage artificial intelligence and machine learning to create an advanced tool capable of identifying and mitigating phishing domains effectively.

2. Project Scope

2.1 In-Scope:

• Machine learning model development for phishing domain detection.

• Integration with a user-friendly web-based interface for real-time scanning.

• Regular updates of the model to adapt to evolving phishing tactics.

• Testing and validation of the tool's accuracy against known phishing domains.

2.2 Out-of-Scope:

• Addressing other types of cyber threats beyond phishing domains.

• Implementation of physical security measures.

3. Deliverables

3.1 Major Deliverables:

• Trained and validated machine learning model for phishing domain detection.

• Web-based interface for users to input and scan domains.

• Documentation outlining the tool's functionality and integration guidelines.

• Regular updates to the model based on new threat intelligence.

3.2 Acceptance Criteria:

• The machine learning model achieves a precision and recall rate of at least 90%.

• The web interface allows users to submit domains for scanning and provides clear results.

• Documentation is comprehensive and accessible for both end-users and developers.

4. Project Timeline

4.1 Project Milestones:

• Model development and initial testing - Months 1-2

• Web interface development - Months 3-4

• Integration and testing - Months 5-6

• Documentation and deployment - Months 7-8

Technical Constraints:

• The tool must be compatible with common web browsers and platforms.

7. Assumptions

7.1 Project Assumptions:

• The availability of a sufficient dataset for training the machine learning model.

8. Risks

8.1 Project Risks:

• Availability of labeled training data.

• Integration challenges with existing cybersecurity infrastructure.

???????????????????????????????????????????????????????????????????????????

Conducting a thorough risk analysis is essential for any project, especially for complex initiatives like developing an AIML (Artificial Intelligence and Machine Learning) tool for phishing domain detection. Identifying and managing risks early in the project can significantly increase the likelihood of successful completion. Here's a risk analysis specific to your AIML tool project:

Risk Analysis for AIML Tool for Phishing Domain Detection

1. Data Availability and Quality:

Risk: Insufficient or poor-quality training data may impact the accuracy of the machine learning model.

Mitigation: Conduct a comprehensive data collection and preprocessing phase. Use a diverse dataset that includes a variety of phishing scenarios.

2. Model Performance:

Risk: The AI/ML model may not achieve the desired precision and recall rates.

Mitigation: Implement rigorous model validation techniques, including cross-validation. Regularly fine-tune the model based on new data and feedback.

3. Integration Challenges:

Risk: Difficulty integrating the AI/ML model with the user interface or other components of the system.

Mitigation: Plan for incremental integration and conduct thorough testing at each integration point. Collaborate closely between the development teams responsible for the model and the user interface.

4. User Acceptance:

Risk: End-users may find the tool difficult to use or not trust its results.

Mitigation: Involve end-users in the development process through user testing and feedback sessions. Implement a user-friendly interface and provide clear documentation.

5. Ethical Considerations:

Risk: Violation of ethical guidelines, such as privacy concerns or biased model predictions.

Mitigation: Adhere to strict ethical guidelines, obtain proper consent for data usage, and regularly evaluate the model for biases. Transparently communicate ethical practices to stakeholders.

6. Deployment Issues:

Risk: Problems may arise during the deployment phase, leading to downtime or functionality issues.

Mitigation: Conduct thorough testing in a staging environment before deployment. Implement a rollback plan in case of unexpected issues. Provide user training and support during the initial deployment phase.

7. Resource Constraints:

Risk: Limited budget or resources may impact the project's progress.

Mitigation: Develop a detailed budget plan, allocate resources efficiently, and consider alternative solutions or open-source tools where appropriate.

8. Changing Phishing Tactics:

Risk: Phishing tactics may evolve during the project, rendering the model less effective.

Mitigation: Implement regular updates to the model based on new threat intelligence. Keep the model adaptive to changing patterns in phishing attacks.

9. Legal and Compliance Issues:

Risk: Legal and compliance issues may arise due to the use of certain datasets or the nature of the tool.

Mitigation: Ensure compliance with data protection regulations, and obtain legal advice to address any potential issues. Document the tool's usage within legal and regulatory frameworks.

10. Team Collaboration Issues:

Risk: Poor collaboration or communication among team members may lead to delays or misunderstandings.

Mitigation: Foster a collaborative team culture, conduct regular team meetings, and use project management tools for effective communication and tracking.

Risk Management Approach

Develop a risk register to document and regularly review identified risks.

Assign responsibilities for monitoring and mitigating specific risks.