PHISHGUARD

TODO LIST

BY RANCORP

TABLE OF CONTENTS

GENERAL TASKS

- Set up a CI/CD pipeline to automate testing and deployment: Implement a system to automatically test and deploy code changes, ensuring quick and reliable software delivery.
- Improve the overall documentation, including installation instructions and usage examples: Enhance the documentation to make it more comprehensive and user-friendly, including detailed installation instructions and usage examples.
- Create a user-friendly graphical interface for non-technical users: Develop a graphical user interface (GUI) that is easy to use for people who may not be comfortable with command-line tools.
- Optimize performance for handling large volumes of emails: Improve the software's performance to efficiently process large amounts of email data without slowing down or crashing.

DOMAIN REPUTATION CHECKS (functions start here)

i. Integrate additional domain reputation services.
ii. Implement caching for domain reputation results to reduce redundant checks.
iii. Add support for custom domain reputation lists maintained by users.

Content Analysis

i. Enhance the machine learning model for detecting phishing keywords.
ii. Integrate a more comprehensive spell checker.
iii. Add natural language processing (NLP) capabilities to better understand email context.
iv. Implement a more robust URL extraction and analysis mechanism.

URL Scanning

i. Integrate more URL scanning services.
ii. Add functionality to scan shortened URLs.
iii. Implement real-time URL scanning and analysis.

Attachment Analysis(functions ends here)

i. Integrate with more antivirus scanning services.
ii. Add support for analyzing different types of file attachments.
iii. Implement sandboxing techniques to safely open and analyze attachments.
iv. Enhance the detection of ransomware and other sophisticated malware.

Threat Intelligence Integration

i. Integrate additional threat intelligence feeds.
ii. Implement a system for users to report and share phishing threats.
iii. Develop a dashboard to visualize threat intelligence data and trends.

Testing and Quality Assurance

i. Write unit tests for all functions.
ii. Create integration tests to ensure components work together seamlessly.
iii. Implement fuzz testing to identify potential security vulnerabilities.
iv. Conduct user acceptance testing (UAT) to gather feedback and improve usability.

User Interface and Experience

i. Design and implement a web-based user interface.
ii. Add email alert notifications for detected phishing attempts.
iii. Create detailed logs and reports for administrators.
iv. Implement user authentication and role-based access control.

Documentation

i. Write comprehensive installation and setup guides.
ii. Provide detailed usage instructions and examples.
iii. Create a developer guide for contributing to the project.
iv. Document the API endpoints and data formats used.

Community and Support

i. Set up a discussion forum or mailing list for user support.
ii. Create a contribution guide to help new contributors get started.
iii. Organize community events like bug bounties and hackathons.
iv. Establish a code of conduct to foster a positive community environment.

Future Enhancements

i. Explore the integration of AI and machine learning for advanced threat detection.
ii. Develop plugins for popular email clients to extend PhishGuard's capabilities.
iii. Investigate the feasibility of real-time email scanning.
iv. Expand support to additional communication platforms (e.g., chat applications).

Conclusion

PhishGuard aims to provide comprehensive protection against phishing threats. Your contributions can help make the internet a safer place. Feel free to pick any of the tasks above and start contributing!

Note: This TODO report is a living document and will be updated regularly to reflect the project's progress and new ideas.