INFORMATION SECURITY

PROJECT PROPOSAL

PHISHING EMAIL DETECTION

Team Member

21F – 9104 – Saad Nadeem

21F – 9079 – Saad Habib

21F – 9127 – Abdul Basit

21F – 9134 – Talha Rauf

20F - 0337 – Sultan-ul-Arfeen

Submitted to

Dr. Umer Aftab

Table of Contents

1. Introduction

Phishing attacks pose a significant threat to individuals and organizations alike. By tricking users into divulging sensitive information, these attacks can lead to financial losses, data breaches, and compromised security. This project aims to tackle this growing issue by developing an intelligent phishing email detection system. Leveraging advanced machine learning algorithms, this system will provide users with a reliable tool to safeguard their email communications.

2. Objectives

The primary objectives of this project are:

- Detect phishing emails with high accuracy.
- Provide an intuitive and user-friendly interface for email analysis.
- Ensure the system is scalable, reliable, and secure.

3. Prepared Solutions

The solution involves the development of a machine learning-based phishing detection system. The system will analyze the content of emails to classify them as phishing or safe. Key components of the solution include:

- Backend powered by machine learning models for email classification.
- A responsive and visually appealing frontend interface.
- Real-time predictions and detailed feedback for users.

4. Tools and Technology

The following tools and technologies will be used:

- Programming Languages: Python, JavaScript
- Frameworks: FastAPI for backend, HTML/CSS/JavaScript for frontend
- Libraries: Scikit-learn, TfidfVectorizer for model development
- Deployment: Uvicorn, Nginx for hosting the application
- Additional Tools: GitHub for version control and collaboration

5. Project Scope

This project focuses on detecting phishing emails based on their textual content. The scope is limited to analyzing the email body and subject line for indicators of phishing. Attachments, images, and links within emails are outside the scope of this project.

6. Expected Outcomes

The anticipated outcomes of this project include:

- A fully operational phishing email detection system.
- An intuitive and responsive user interface for seamless user interaction.
- Enhanced email security and reduced risk of falling victim to phishing attacks.

7. Conclusion

Phishing remains a persistent and evolving threat in the digital age. By developing a robust phishing email detector, this project aims to provide a significant contribution to email security. The combination of machine learning and user-focused design will ensure the solution is both effective and accessible. This project underscores the importance of proactive measures in combating cyber threats.