Project Report

Phishing Simulation Platform

Introduction

Phishing is a major cybersecurity threat that manipulates human behaviour to steal credentials and data. This project aims to build a safe, controlled simulation environment that replicates phishing techniques to train users and assess their awareness levels in recognizing such attacks.

Abstract

The Phishing Simulation Platform is developed using HTML, CSS, and Python (Flask) to simulate real-world phishing attempts within a secure environment. The project provides realistic email and web templates that mimic legitimate sources to help organizations and individuals evaluate susceptibility to phishing attacks. It is designed purely for educational and research purposes.

Tools Used

- HTML & CSS: Designed dynamic phishing templates and interactive web interfaces.
- Python (Flask): Implemented backend for campaign management and data collection.
- Visual Studio Code: Used as the integrated development environment for code editing.

Steps Involved in Building the Project:

The following systematic steps were followed in building the Phishing Simulation Platform.

- Create virtual environment, install Flask and dependencies, and initialize project structure.
- Build responsive HTML/CSS templates to mimic legitimate pages and emails.
- Add Flask routes to serve templates, record interactions, and manage campaigns.
- Store interaction events (clicks, form submissions) locally for analysis.

- Run campaigns in a lab, validate behaviour, and ensure no real-world harm.
- Review captured metrics to refine templates and improve detection/education outcomes.

Conclusion

The phishing simulation platform provides an ethical and practical tool for improving phishing awareness. By combining realistic templates with backend tracking, the platform helps measure user susceptibility and informs targeted training. Future enhancements may include richer analytics, integration with simulated email delivery systems for controlled exercises, and role-based training scenarios. This report is prepared for inclusion in a public repository and is intentionally anonymized for general sharing.