Ethical Phishing Simulation Platform

Prepared by: Gagandeep Kurki

Date: October 2025

This report describes an Ethical Phishing Simulation Platform designed for employee awareness and cybersecurity training. It includes both a formal structured version and a descriptive narrative version for clear understanding.

Formal Report Version

1. Executive Summary

The Ethical Phishing Simulation Platform is designed to simulate phishing campaigns ethically within an organization to improve awareness. It helps measure user susceptibility and strengthen defense against phishing attacks.

2. Objectives

• Conduct phishing simulations for employees. • Measure click and report rates. • Provide instant feedback and training. • Generate security awareness reports.

3. Key Features

Campaign Builder, Delivery Engine, Tracking Module, Coaching Pages, Dashboard, Role-Based Access, and Data Safety Controls.

4. Architecture Overview

Frontend (Web UI), Backend (API & Database), Email Relay, Tracking System, and Analytics Dashboard.

5. Data Privacy & Ethics

All data is handled ethically — no real credentials stored, minimal personal data collected, and employees are notified through policy agreements.

6. Metrics & Success

Key metrics include Click Rate, Report Rate, and Repeat Failure Rate. Target goal is a 50% reduction in click rate after three campaigns.

7. Conclusion

The platform helps create a culture of cybersecurity awareness and proactive reporting among employees.

Descriptive Report Version

In this project, the idea was to create a safe and ethical phishing simulation platform that can help employees recognize and handle phishing emails better. The system works by sending out realistic but harmless phishing messages and observing how users react to them. When someone clicks on a fake link, they are redirected to a simple training page that explains how to identify phishing attempts and avoid them in the future. The project was divided into stages. First, a small campaign was tested using simple email templates and tracking links. Next, new features like templates, reporting dashboards, and user groups were added. The final version ensured all data was stored safely, without collecting any real passwords or private information. The platform includes a web dashboard where administrators can create phishing templates, schedule campaigns, and see overall performance. Each campaign provides useful insights such as the percentage of people who clicked a link, who reported it, and who needed more training. The main aim is to lower the number of people falling for phishing emails over time. Ethical and privacy considerations were a top priority throughout the project. No real harm or embarrassment is caused to users. Instead, it focuses on learning and improvement. Regular reports are generated to show progress and help management plan future awareness programs. Overall, this project helped demonstrate how cybersecurity awareness can be improved using simulation and education together. It encourages employees to think before they click and helps build a stronger security culture within any organization.