**Ethical Phishing Simulation Platform**

**1. Executive Summary**

An Ethical Phishing Simulation Platform is a controlled system that sends realistic, simulated phishing emails to employees to measure susceptibility and improve security awareness. This project builds a platform to design campaigns, deliver simulated phishing messages, capture user interactions (clicks, credential entry, attachments opened), provide immediate feedback to users, and report organization-wide metrics. The goal is to reduce successful phishing incidents by educating employees through measured, repeatable training.

**2. Objectives**

* Run periodic simulated phishing campaigns with varying difficulty and themes.
* Measure user behavior (click rate, credential submission rate, report-to-IT rate).
* Provide immediate, friendly coaching to users who fall for simulations.
* Produce dashboards and reports for managers and security teams.

**3. Key Features**

* Campaign Builder — create templates, choose target groups, schedule campaigns.
* Delivery Engine — send email simulations using safe sender infrastructure and tracking tokens.
* Interaction Tracking — record clicks, form submissions, attachment opens, and report actions.
* User Feedback Module — show instant coaching page to users who click or submit data.
* Reporting & Dashboard — campaign-level metrics, user risk scores, trend graphs.
* Role-Based Access Control (RBAC) — admins, campaign managers, HR, and auditors.
* Safety Controls — opt-outs, blacklisted users, and simulated payloads that never execute harmful code.

**4. Architecture (High Level)**

* Frontend: Web UI for campaign creation, dashboards, and user coaching pages.
* Backend: API service to manage campaigns, templates, targets, and logging.
* Mail Delivery: Dedicated SMTP relay or ESP (with proper consent) to deliver simulation emails.
* Tracking: Short, unique URLs and server-side logging to capture user actions.
* Database: Store campaign configs, hashed user results, and audit logs (encrypt sensitive fields).
* Analytics: Job to aggregate metrics and generate reports.

**5. Implementation Plan (Phases)**

Phase 1 – MVP (4 weeks)

* Basic campaign builder, send plain simulated emails to small groups.
* Simple tracking for clicks and opens.
* Basic coaching page after click.

Phase 2 – Enhanced Features (4 weeks)

* Add templates, scheduling, user groups, and reporting dashboard.
* Add RBAC and opt-out lists.

Phase 3 – Hardening & Privacy (2 weeks)

* Add encryption for sensitive data, audit logs, and data retention policies.
* Legal/HR review and consent flow.

Phase 4 – Scale & Automation (ongoing)

* Integration with HR/ID systems, automated training assignments, and trend analytics.

**6. Data, Privacy & Ethics**

* Consent & Policy: Ensure organizational policy permits simulation campaigns; notify employees via acceptable channels (policy, onboarding). Consider explicit consent where required.
* Minimization: Store only necessary data (timestamp, action, campaign id). Avoid capturing real credentials — any entered text should be hashed and immediately discarded after coaching.
* Safety: Do not include executable attachments or links to malware. Use static coaching pages hosted on a secure domain.
* Transparency & Remediation: Provide clear remediation materials and allow users to ask questions or flag campaigns.

**7. Metrics & Success Criteria**

* Click Rate: % of users who clicked a simulated phishing link.
* Credential Submission Rate: % who submitted information (should be zero if credentials are not captured; otherwise measured as attempted submissions).
* Report Rate: % of users who reported email to IT/security.
* Repeat Failure Rate: Users who fail multiple campaigns (used for targeted training).
* Time to Remediation: Average time from click to completed training.

**10. Conclusion**

An Ethical Phishing Simulation Platform is a practical and measurable way to improve an organization’s security posture. By combining realistic simulations, immediate coaching, and clear reporting — while respecting privacy and ethics — organizations can reduce phishing risk and build a security-aware culture.