Task 11: Phishing Attack Simulation & Detection

Objective

To simulate a phishing attack in a controlled environment and understand how phishing works, how it is detected, and how it can be prevented to improve social engineering awareness.

Tools Used

- GoPhish
- Manual phishing email templates (alternative)

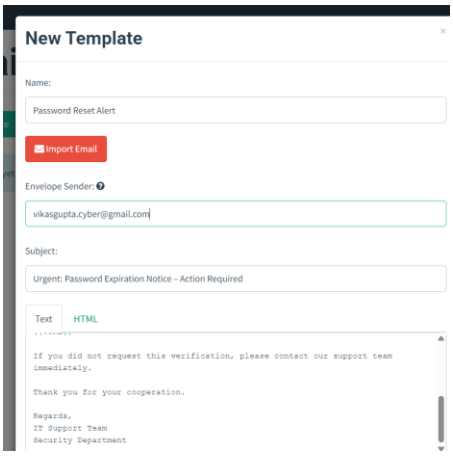
Understanding Phishing (Brief Overview)

Phishing is a social engineering attack where attackers impersonate trusted entities to trick users into revealing sensitive information such as login credentials or personal data.

Phishing Simulation Steps

1. Email Template Creation

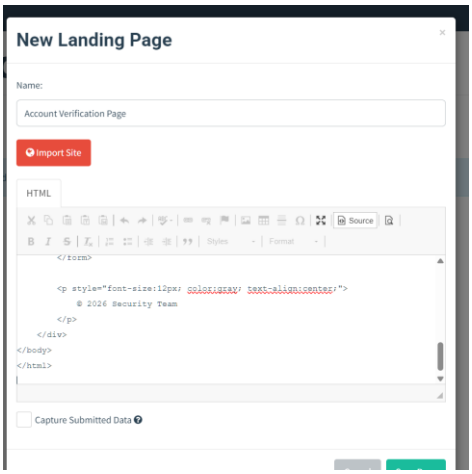
A fake but realistic email template was created to imitate a legitimate organization.



---

2. Landing Page Setup

A fake landing page was configured to capture user interaction when the phishing link is clicked.

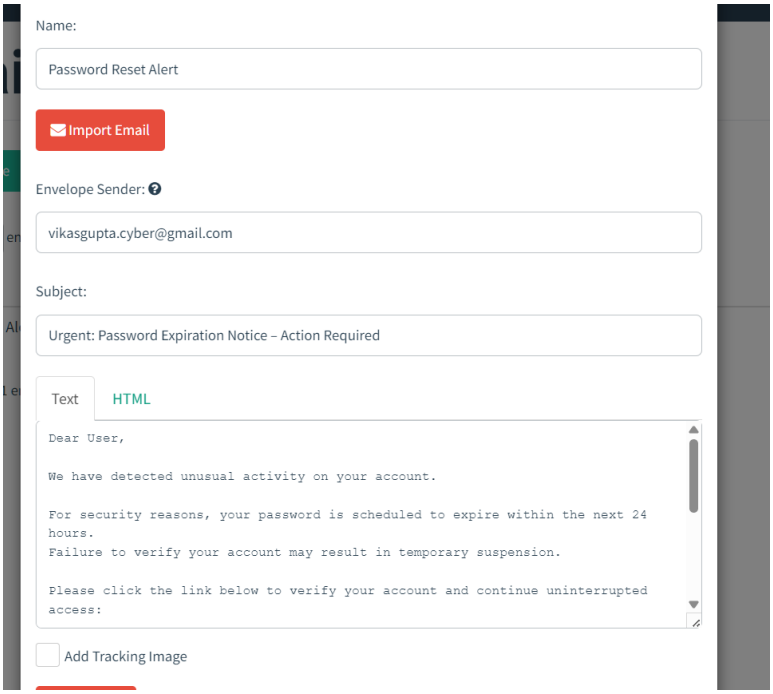


---

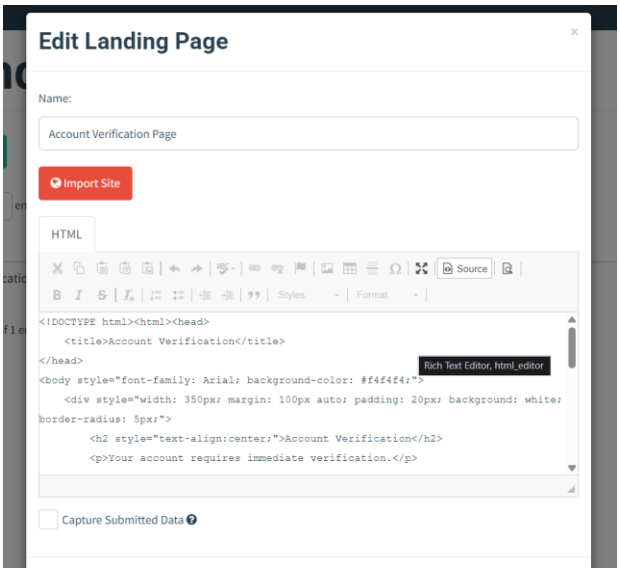
3. Phishing Campaign Setup

A phishing campaign was created by selecting:

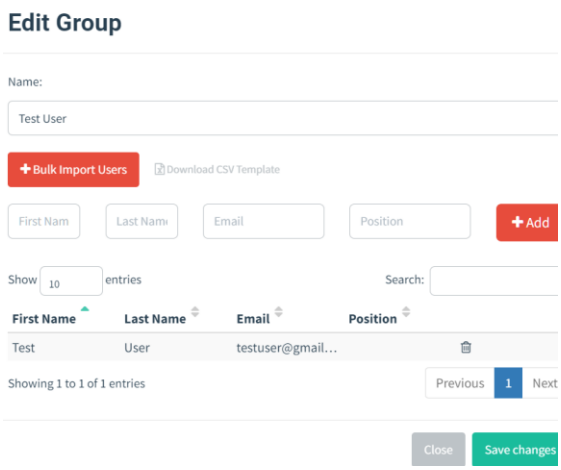
- Email template



- Landing page



- Target email address



---

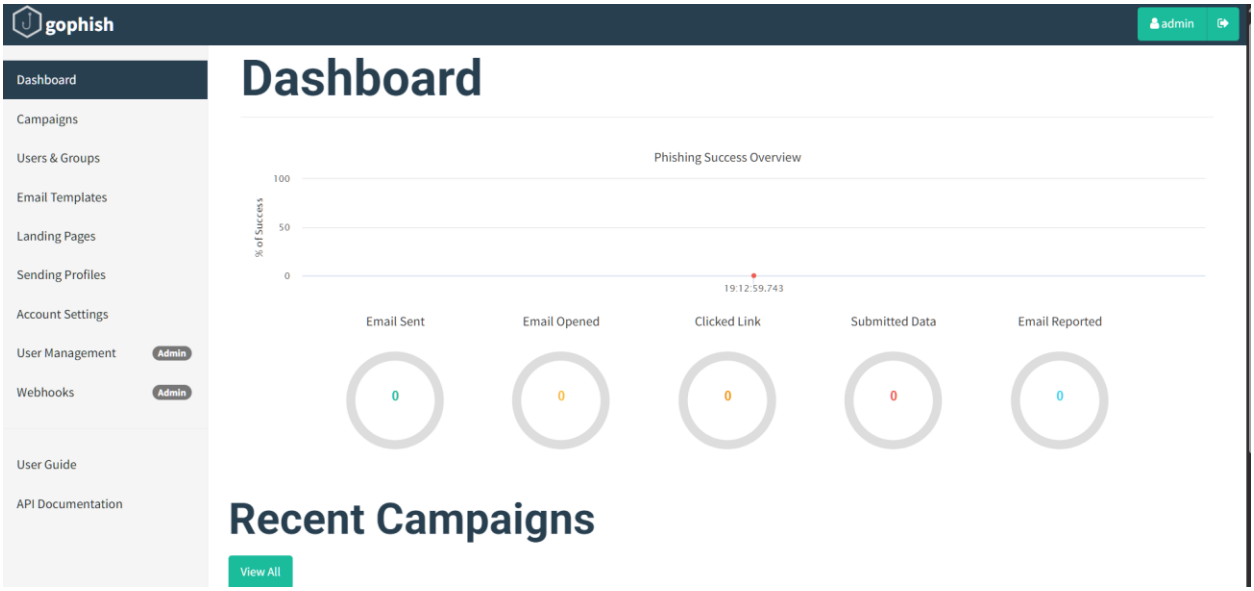
4. Sending Test Phishing Email

The phishing email was sent to a test user to simulate a real-world attack scenario.

---

5. Tracking Results

User actions such as email opened, link clicked, and data submitted were monitored.



Identifying Phishing Red Flags

- Suspicious sender email address
- Urgent or threatening language
- Unknown or shortened links
- Requests for sensitive information
- Poor grammar or spelling mistakes

Prevention & Awareness

- User awareness training
- Email filtering and spam detection
- Verifying links and senders
- Multi-factor authentication (MFA)
- Reporting suspicious emails

Deliverable

Phishing Simulation Report including:

- Objective
- Methodology
- Screenshots
- Results
- Observations
- Prevention techniques

Final Outcome

Increased awareness of social engineering attacks and improved understanding of phishing detection and prevention techniques.