

# 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)

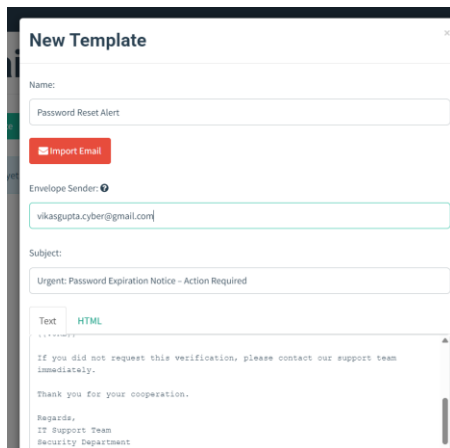
Phishing is a social engineering attack where attackers impersonate trusted entities to trick users into revealing sensitive information such as login credentials or personal data.

---

## Phishing Simulation Steps

### 1. Email Template Creation

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



**New Template**

Name: Password Reset Alert

[Import Email](#)

Envelope Sender: vikasgupta.cyber@gmail.com

Subject: Urgent: Password Expiration Notice - Action Required

Text HTML

If you did not request this verification, please contact our support team immediately.

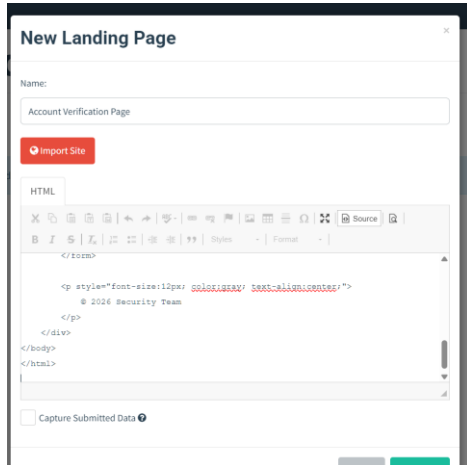
Thank you for your cooperation.

Regards,  
IT Support Team  
Security Department

---

## 2. Landing Page Setup

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



The screenshot shows a web application window titled "New Landing Page". It contains a form for configuring a landing page. The "Name:" field is labeled "Account Verification Page". Below it is a red button labeled "Import Site". The main area is a code editor with a toolbar and a text area containing the following HTML code:

```
</html>

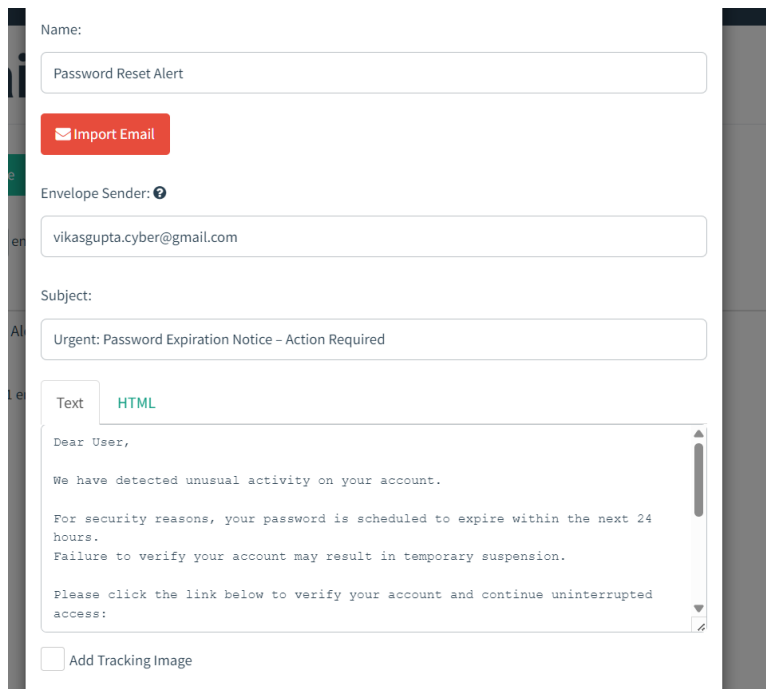
<p style="font-size:10px; color:gray; text-align:center;">
  © 2024 Security Team
</p>
</div>
</body>
</html>
```

At the bottom, there is a checkbox labeled "Capture Submitted Data" which is currently unchecked.

## 3. Phishing Campaign Setup

A phishing campaign was created by selecting:

- Email template



The screenshot shows a web application window titled "Email template". It contains a form for configuring an email template. The "Name:" field is labeled "Password Reset Alert". Below it is a red button labeled "Import Email". The "Envelope Sender:" field is labeled with a question mark icon and contains the email address "vikasgupta.cyber@gmail.com". The "Subject:" field is labeled and contains the text "Urgent: Password Expiration Notice – Action Required". The main area is a text editor with a toolbar and a text area containing the following text:

Dear User,

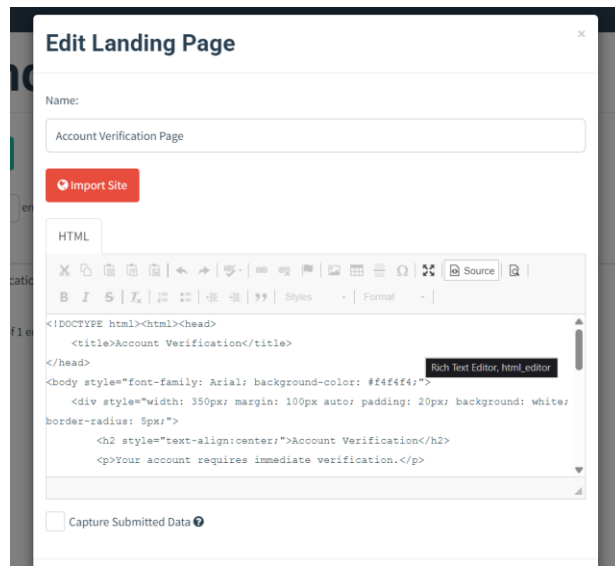
We have detected unusual activity on your account.

For security reasons, your password is scheduled to expire within the next 24 hours. Failure to verify your account may result in temporary suspension.

Please click the link below to verify your account and continue uninterrupted access:

At the bottom, there is a checkbox labeled "Add Tracking Image" which is currently unchecked.

- Landing page



- Target email address

### Edit Group

Name:

[+ Bulk Import Users](#) [Download CSV Template](#)

[+ Add](#)

Show  entries Search:

First Name	Last Name	Email	Position	
Test	User	testuser@gmail...		

Showing 1 to 1 of 1 entries [Previous](#) [1](#) [Next](#)

[Close](#) [Save changes](#)

---

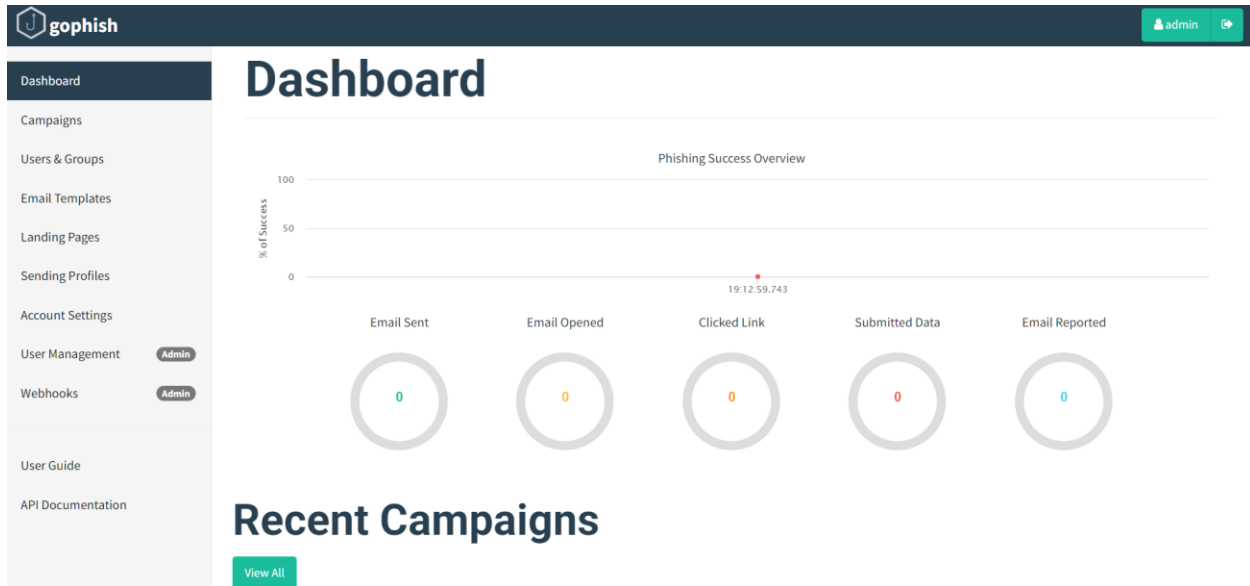
## 4. Sending Test Phishing Email

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.