

# 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)

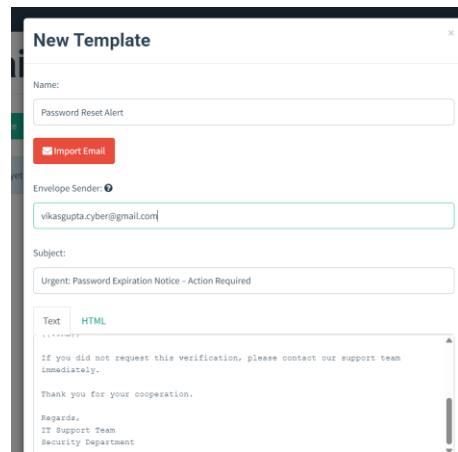
Phishing is a social engineering attack where attackers impersonate trusted entities to trick users into revealing sensitive information such as login credentials or personal data.

---

## 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.

The screenshot shows a 'New Landing Page' configuration window. At the top, there's a 'Name:' field containing 'Account Verification Page'. Below it is a red 'Import Site' button. The main area is a WYSIWYG editor with an 'HTML' tab selected. The HTML code in the editor is:

```
<p style="font-size:12px; color:#333; text-align:center;">  
© 2024 Security Team  
</p>  
</div>  
</body>  
</html>
```

At the bottom of the editor, there's a checkbox labeled 'Capture Submitted Data' with a question mark icon next to it.

## 3. Phishing Campaign Setup

A phishing campaign was created by selecting:

- Email template

The screenshot shows an 'Email template' configuration window. It includes fields for 'Name:' (set to 'Password Reset Alert'), an 'Import Email' button, 'Envelope Sender:' (set to 'vikasgupta.cyber@gmail.com'), 'Subject:' (set to 'Urgent: Password Expiration Notice - Action Required'), and a rich text editor. The rich text editor has a 'Text' tab and an 'HTML' tab (which is currently selected). The HTML content in the editor is:

```
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 of the editor, there's a checkbox labeled 'Add Tracking Image'.

- Landing page

The screenshot shows the 'Edit Landing Page' interface. At the top, there is a 'Name:' field containing 'Account Verification Page'. Below it is a red 'Import Site' button. The main area is a 'Rich Text Editor' with an 'HTML' tab selected. The HTML code is as follows:

```
<!DOCTYPE html><html><head>
<title>Account Verification</title>
</head>
<body style="font-family: Arial; background-color: #f4f4f4;">
<div style="width: 350px; margin: 100px auto; padding: 20px; background: white; border-radius: 5px;">
<h2 style="text-align:center;">Account Verification</h2>
<p>Your account requires immediate verification.</p>
</div>
</body>
</html>
```

At the bottom left is a checkbox for 'Capture Submitted Data'.

- Target email address

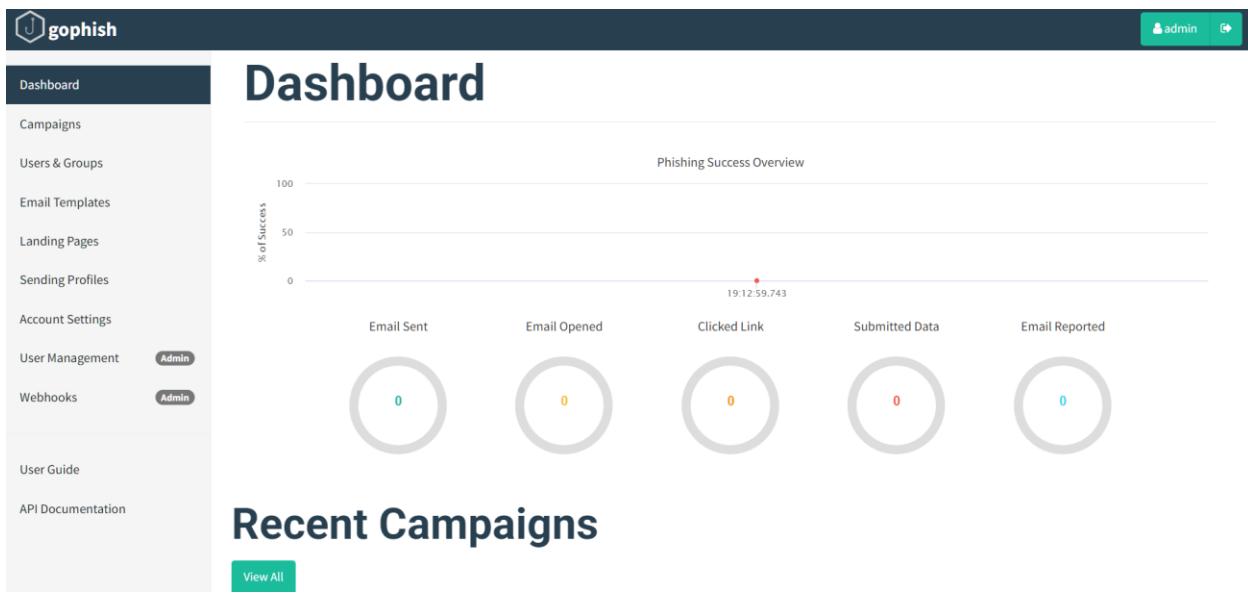
The screenshot shows the 'Edit Group' interface. At the top, there is a 'Name:' field containing 'Test User'. Below it is a red 'Bulk Import Users' button and a 'Download CSV Template' link. There are four input fields: 'First Name', 'Last Name', 'Email', and 'Position', followed by a red '+ Add' button. Below these are two search/filter controls: 'Show 10 entries' and 'Search:'. A table lists the user 'Test User' with email 'testuser@gmail...'. The table has columns for First Name, Last Name, Email, and Position. At the bottom are 'Close' and 'Save changes' buttons.

## 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.