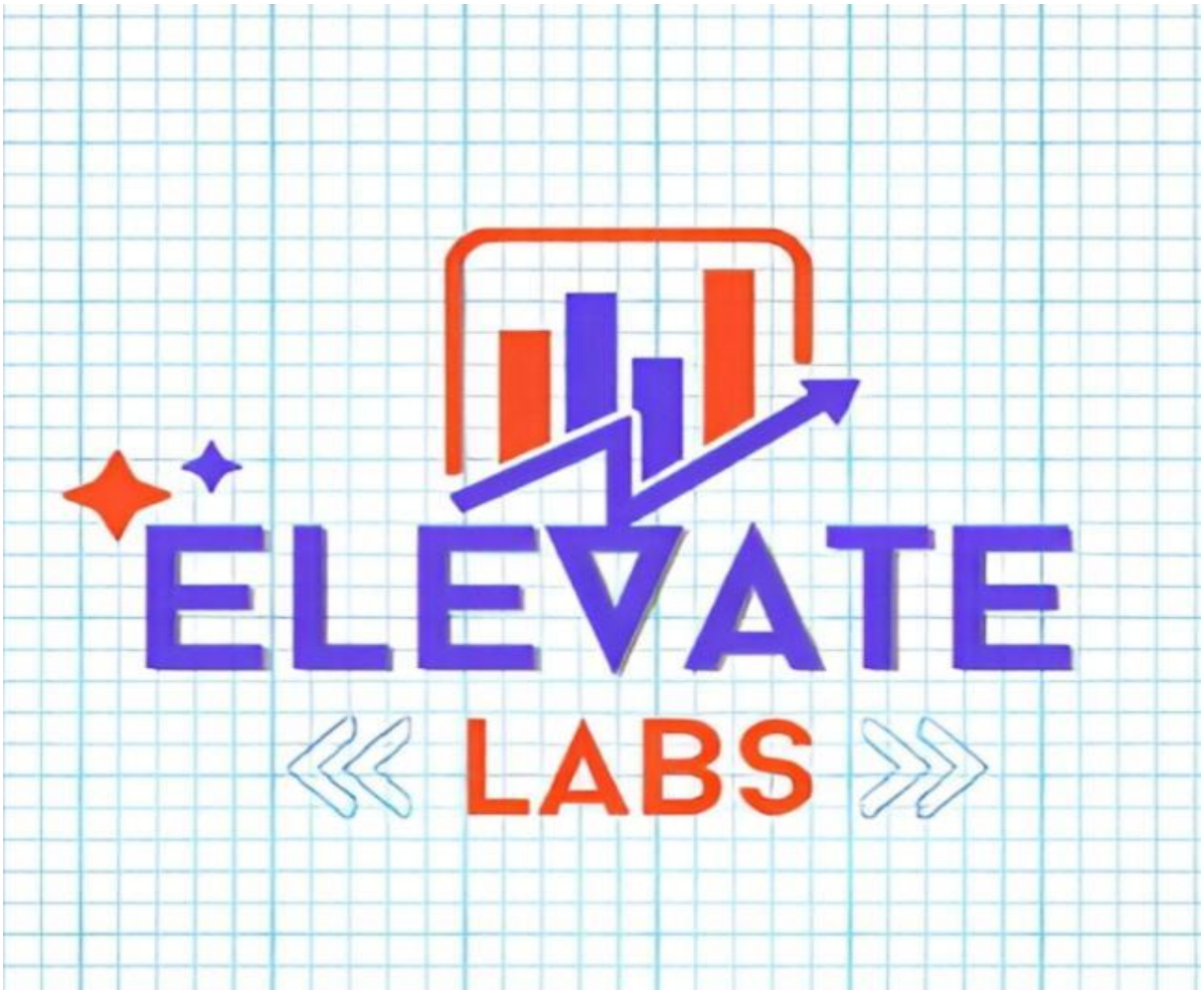
TASK 11 Phishing Attack Simulation & Detection



Name: - Ch Rohit Kumar

University: - Aditya University

Gmail: - rohitkumarrrr20@gmail.com

1. Understand phishing attacks

Phishing is a type of **social engineering attack** where attackers trick people into giving **sensitive information** such as:

- Usernames & passwords
- Bank or credit card details
- OTPs
- Personal information

The attacker **pretends to be a trusted source** (bank, company, teacher, admin, etc.).

🔹 Simple Definition

Phishing is a cyber attack where fake messages (emails, SMS, calls, or websites) are used to steal confidential information by fooling the victim.

🔹 How Phishing Works (Step-by-Step)

1. **Attacker creates a fake message**
   - Looks like it is from a trusted organization (Bank, Google, College, Amazon, etc.)
2. **Victim receives the message**
   - Email / SMS / WhatsApp / Social media / Phone call
3. **Message creates urgency or fear**
   - "Your account will be blocked"
   - "Unusual login detected"
   - "Verify now"
4. **Victim clicks a link or downloads a file**
   - Link leads to a **fake website**
   - Website looks real
5. **Victim enters credentials**
   - Username, password, OTP, card details
6. **Attacker steals the data**
   - Uses it for fraud, identity theft, or further attacks

🔹 Common Types of Phishing

1️⃣ Email Phishing

- Fake emails from banks, companies, admins
- Most common type
- Example: *"Your bank account is suspended"*

2️⃣ Smishing (SMS Phishing)

- Phishing through **SMS or WhatsApp**
- Example: *"Click here to track your parcel"*

3️⃣ Vishing (Voice Phishing)

- Phone calls pretending to be bank officials or police
- Example: *"Your KYC is expired"*

4️⃣ Spear Phishing

- Targeted attack on a **specific person**
- Uses personal details (name, role, college)

5️⃣ Clone Phishing

- Legitimate email is copied and resent with a **malicious link**

🔷 Signs of a Phishing Attack 🚩

- Urgent or threatening language
- Unknown sender address
- Spelling or grammar mistakes
- Suspicious links (shortened or strange URLs)
- Requests for OTP, password, or card details
- Attachments you were not expecting

🔷 Example (Easy)

✉️ Fake Email

Dear User, your Google account will be blocked in 24 hours. Click here to verify.

🔗 Link opens a **fake Google login page**

👤 Victim enters email & password

❌ Account is compromised

Step 1: Download GoPhish Wget

https://github.com/gophish/gophish/releases/download/v0.12.1/gophish v0.12.1-linux-64bit.zip

Extract files:

unzip gophish-v0.12.1-linux-64bit.zip cd gophish

```
┌──(kali㉿kali)-[~]
└─$ unzip gophish-v0.12.1-linux-64bit.zip
cd gophish
Archive:  gophish-v0.12.1-linux-64bit.zip
replace gophish? [y]es, [n]o, [A]ll, [N]one, [r]ename: y
  inflating: gophish
   creating: static/js/dist/
   creating: static/js/dist/app/
  inflating: static/js/dist/app/sending_profiles.min.js
  inflating: static/js/dist/app/campaign_results.min.js
  inflating: static/js/dist/app/gophish.min.js
  inflating: static/js/dist/app/campaigns.min.js
  inflating: static/js/dist/app/autocomplete.min.js
  inflating: static/js/dist/app/settings.min.js
  inflating: static/js/dist/app/users.min.js
  inflating: static/js/dist/app/webhooks.min.js
  inflating: static/js/dist/app/dashboard.min.js
  inflating: static/js/dist/app/passwords.min.js
  inflating: static/js/dist/app/templates.min.js
  inflating: static/js/dist/app/groups.min.js
  inflating: static/js/dist/app/landing_pages.min.js
  inflating: static/js/dist/vendor.min.js
   creating: static/js/src/vendor/ckeditor/
  inflating: static/js/src/vendor/ckeditor/CHANGES.md
   creating: static/js/src/vendor/ckeditor/skins/
   creating: static/js/src/vendor/ckeditor/skins/moono-lisa/
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/editor_ie.css
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/editor_gecko.css
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/icons.png
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/readme.md
   creating: static/js/src/vendor/ckeditor/skins/moono-lisa/images/
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/images/refresh.png
  inflating: static/js/src/vendor/ckeditor/skins/moono-lisa/images/arrow.png
```

Give execution permission:

chmod +x gophish

```
┌──(kali㉿kali)-[~]
└─$ chmod +x gophish
```

Step 2: Start GoPhish Server Run

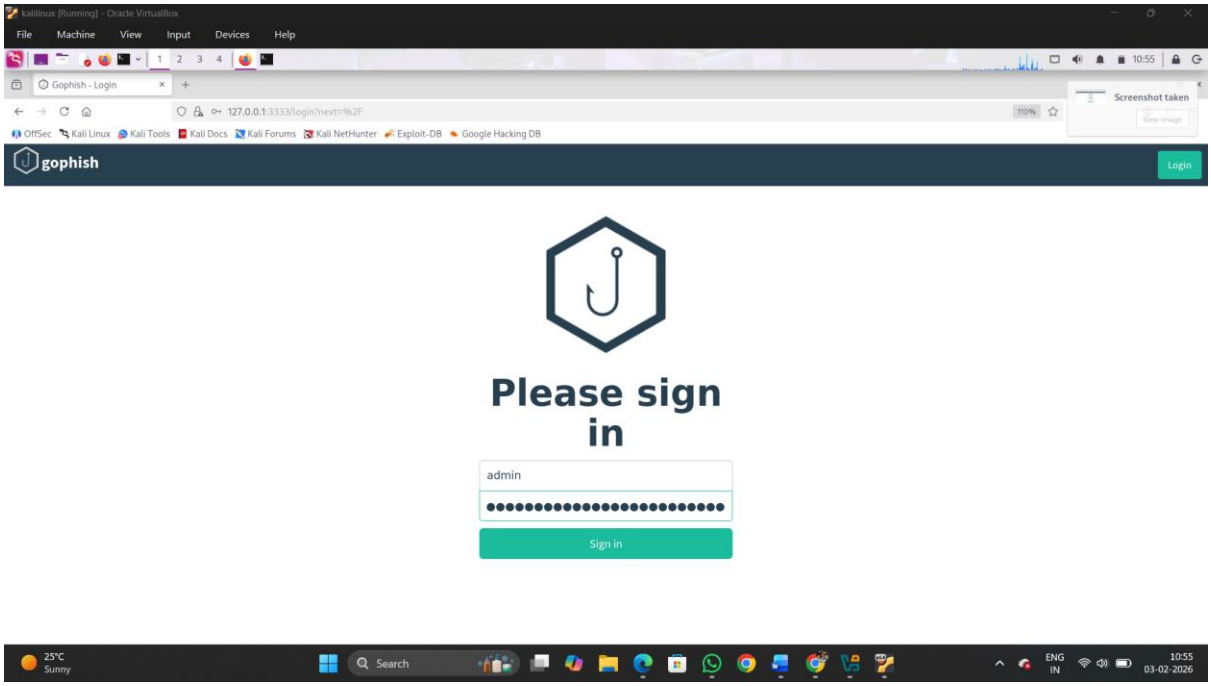
GoPhish: sudo ./gophish

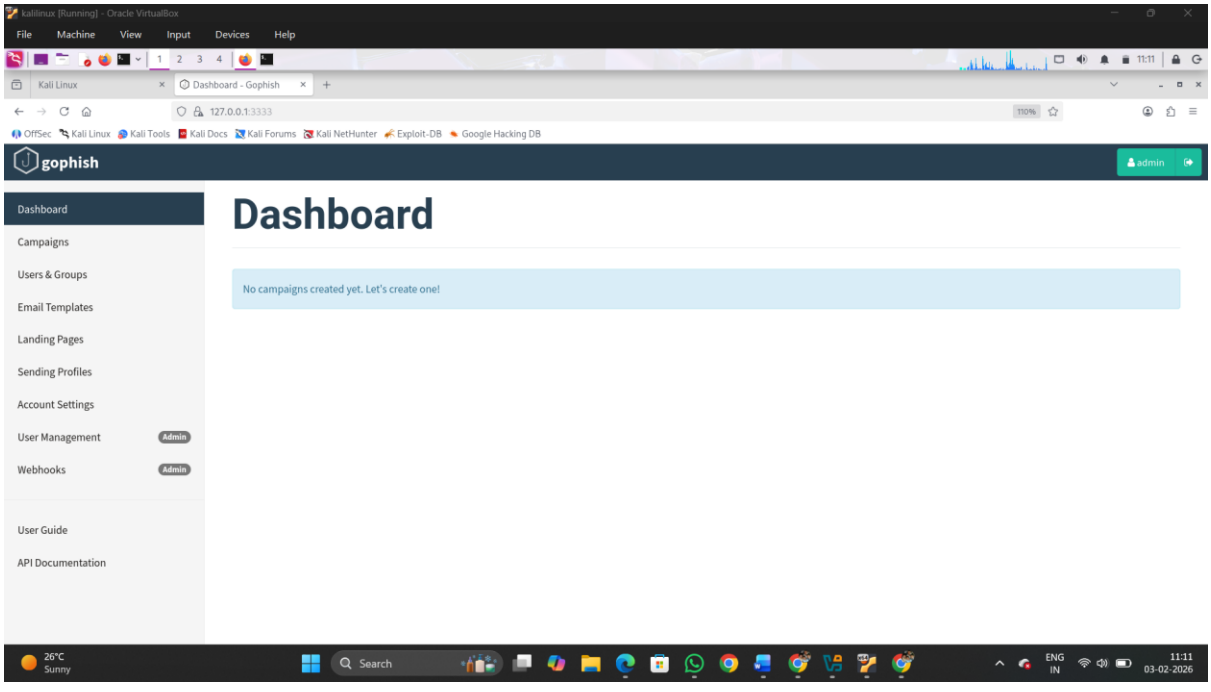
```
┌──(kali㉿kali)-[~]
└─$ sudo ./gophish

[sudo] password for kali:
time="2026-02-03T10:41:17+05:30" level=warning msg="No contact address has been configured."
time="2026-02-03T10:41:17+05:30" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: migrating db environment 'production', current version: 0, target: 20220321133237
OK    20160118194630_init.sql
OK    20160131153104_0.1.2_add_event_details.sql
OK    20160211211220_0.1.2_add_ignore_cert_errors.sql
OK    20160217211342_0.1.2_create_from_col_results.sql
OK    20160225173824_0.1.2_capture_credentials.sql
OK    20160227180335_0.1.2_store-smtp-settings.sql
OK    20160317214457_0.2_redirect_url.sql
OK    20160605210903_0.2_campaign_scheduling.sql
OK    20170104220731_0.2_result_statuses.sql
OK    20170219122503_0.2.1_email_headers.sql
OK    20170827141312_0.4_utc_dates.sql
OK    20171027213457_0.4.1_maillogs.sql
OK    20171208201932_0.4.1_next_send_date.sql
OK    20180223101813_0.5.1_user_reporting.sql
OK    20180524203752_0.7.0_result_last_modified.sql
OK    20180527213648_0.7.0_store_email_request.sql
OK    20180830215615_0.7.0_send_by_date.sql
OK    20190105192341_0.8.0_rbac.sql
OK    20191104103306_0.9.0_create_webhooks.sql
OK    20200116000000_0.9.0_imap.sql
OK    20200619000000_0.11.0_password_policy.sql
OK    20200730000000_0.11.0_imap_ignore_cert_errors.sql
OK    20200914000000_0.11.0_last_login.sql
OK    20201201000000_0.11.0_account_locked.sql
OK    20220321133237_0.4.1_envelope_sender.sql
time="2026-02-03T10:41:18+05:30" level=info msg="Please login with the username admin and the password 46a5d3f3acef9204"
time="2026-02-03T10:41:18+05:30" level=info msg="Creating new self-signed certificates for administration interface"
```

Step 3: Access GoPhish Dashboard

Open browser and go to:

https://127.0.0.1:3333





Step 4: Create Email Template

1. Dashboard → Email Templates

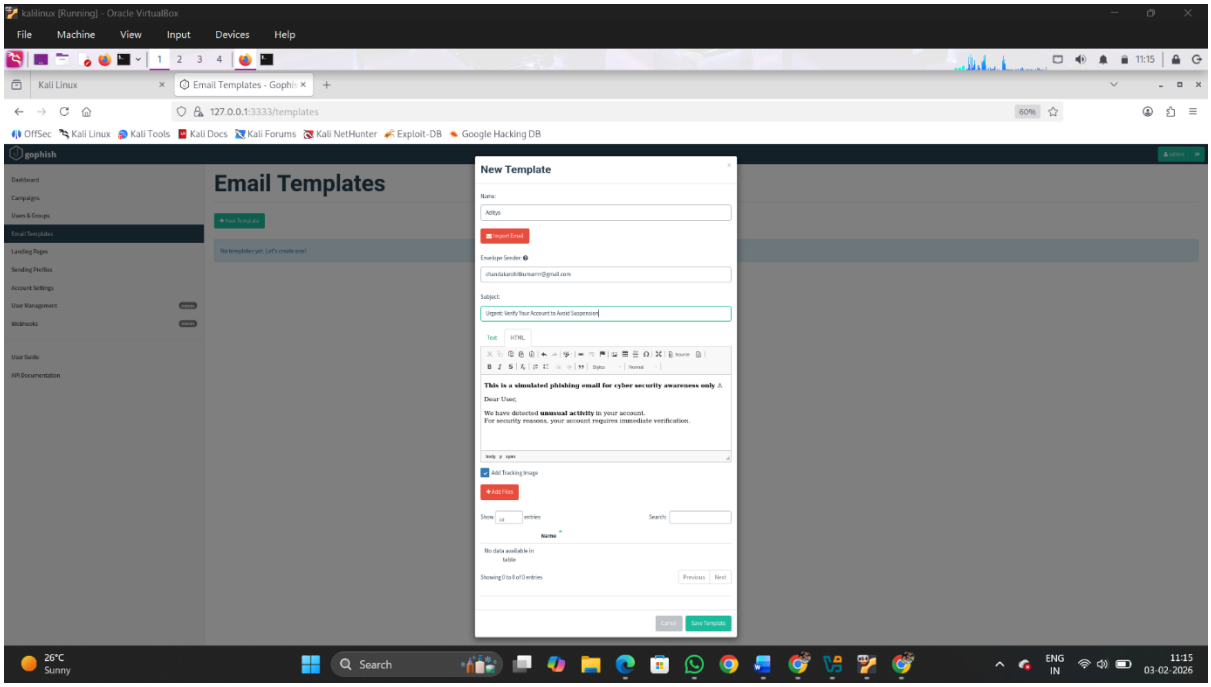
2. Click New Template

3. Enter details:

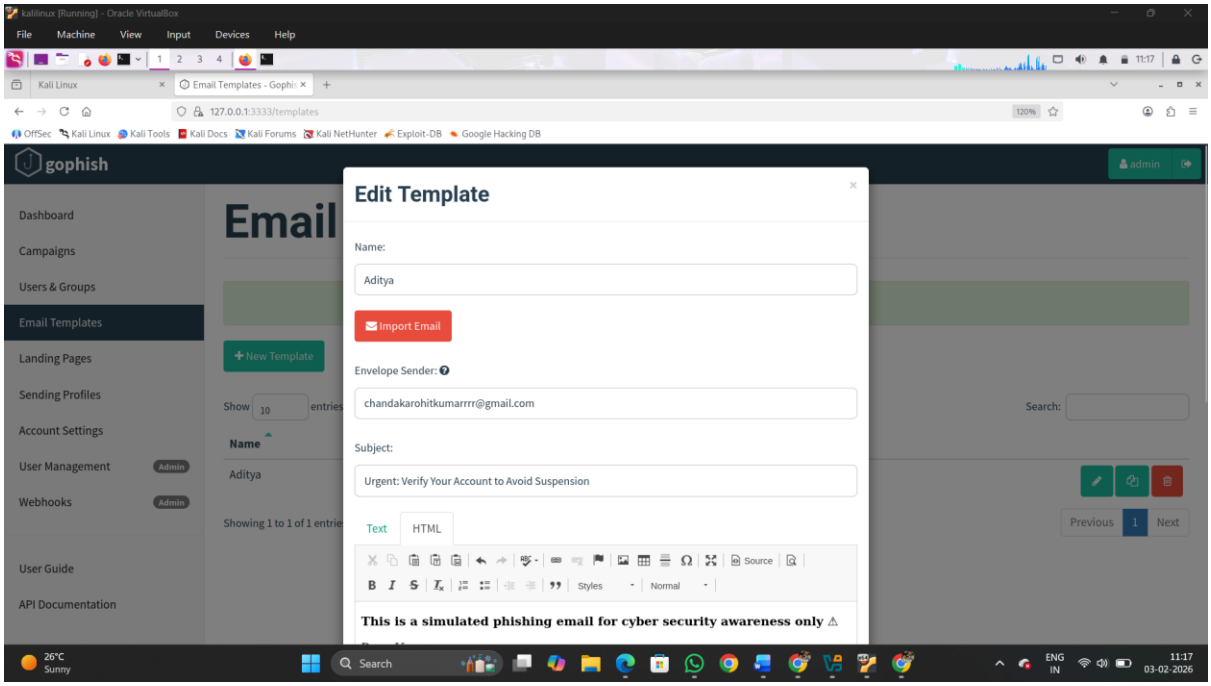
Name: Security Awareness

Email o Subject: Security Awareness Notification

From: IT Security Team

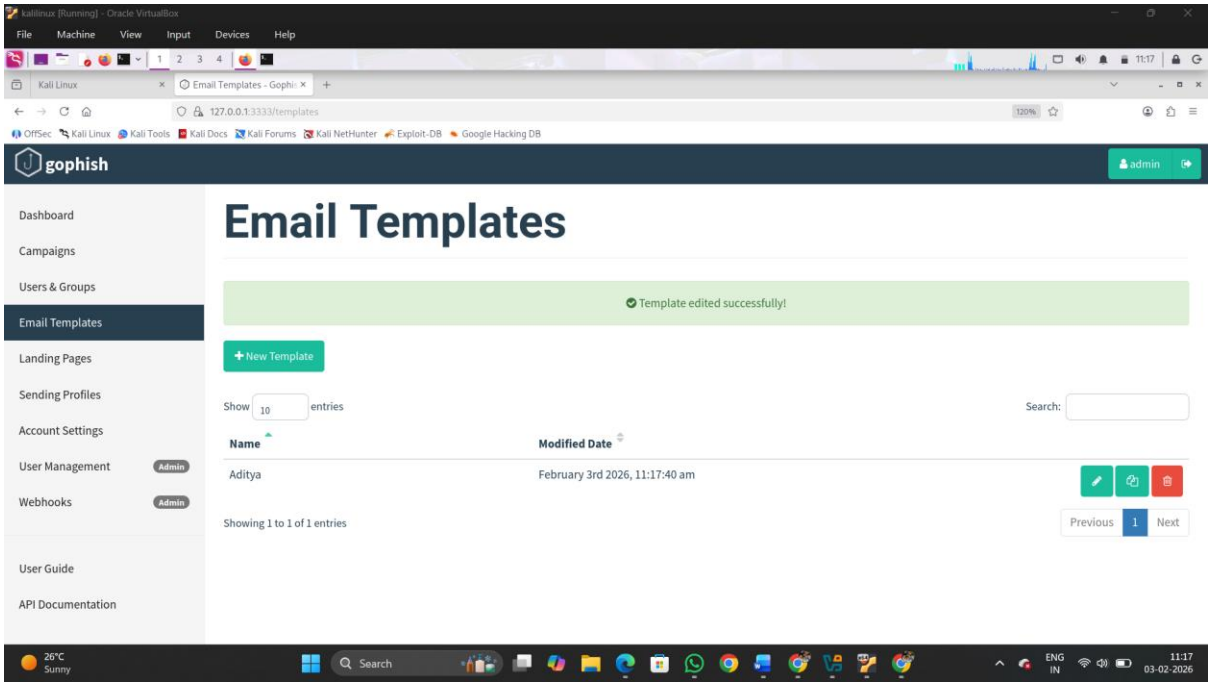


Step 5: Add Email Body (Training Purpose)



Step 6: Save Template

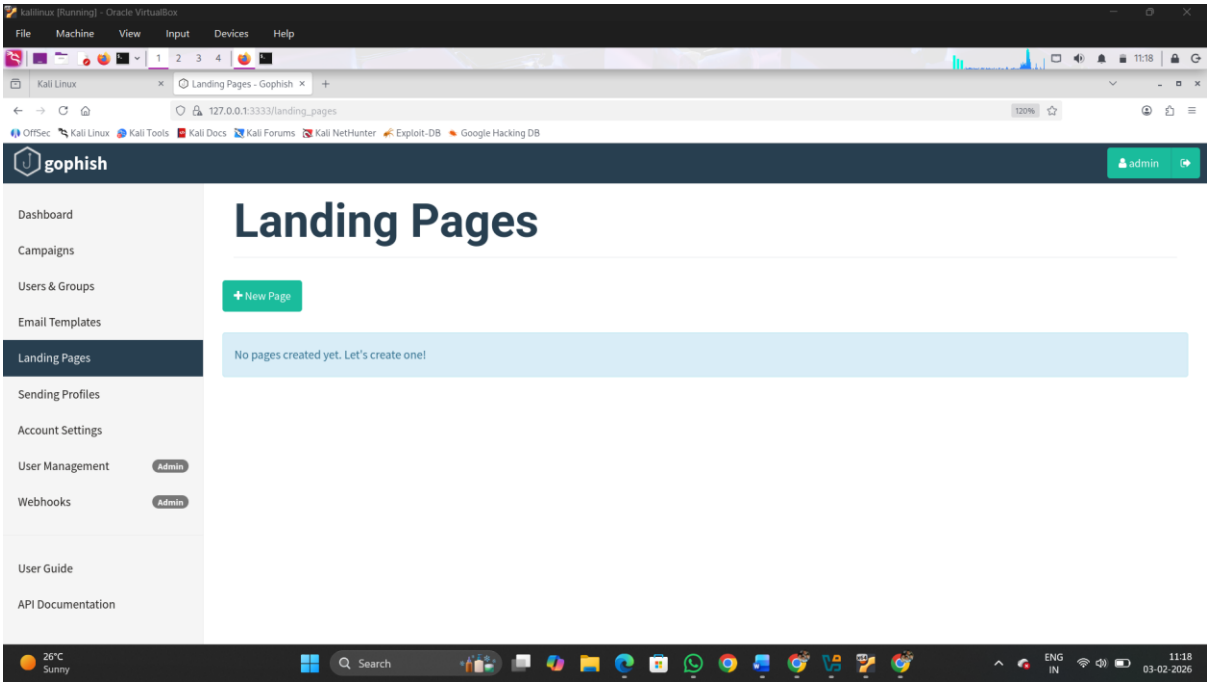
- Click Save Template
- Email template is successfully created



2. Setup Landing Page

Step 1: Open GoPhish Dashboard • Start GoPhish • Open browser • Go to:

Step 2: Navigate to Landing Pages • Dashboard → Landing Pages • Click New Page



Step 3: Create Landing Page Details Fill the following fields:

• Name: Security Awareness Page

• HTML Content:

Step 4: Configure Page Settings

Enable / Disable options carefully:

• Capture Submitted Data: OFF

• Capture Passwords: OFF

• Redirect to URL:

Step 5: Save Landing Page

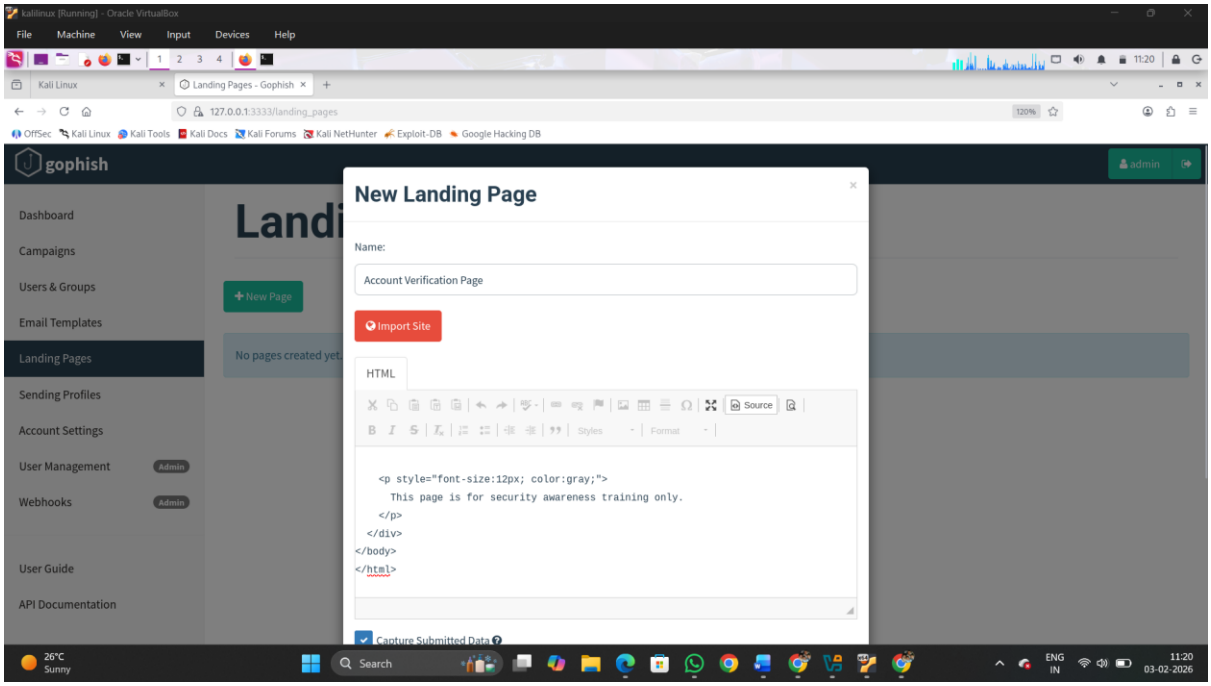
• Click Save Page

• Landing page is now created successfully

Step 6: Link Landing Page to Email Template

• Go to Email Templates

• Edit your template • Use:



3. Send test phishing email

Step 1: Create Sending Profile (If Not Created)

1. GoPhish Dashboard → Sending Profiles

2. Click New Profile

3. Fill details: o Name: Test SMTP Profile

o From: IT Security itsecurity@test.com

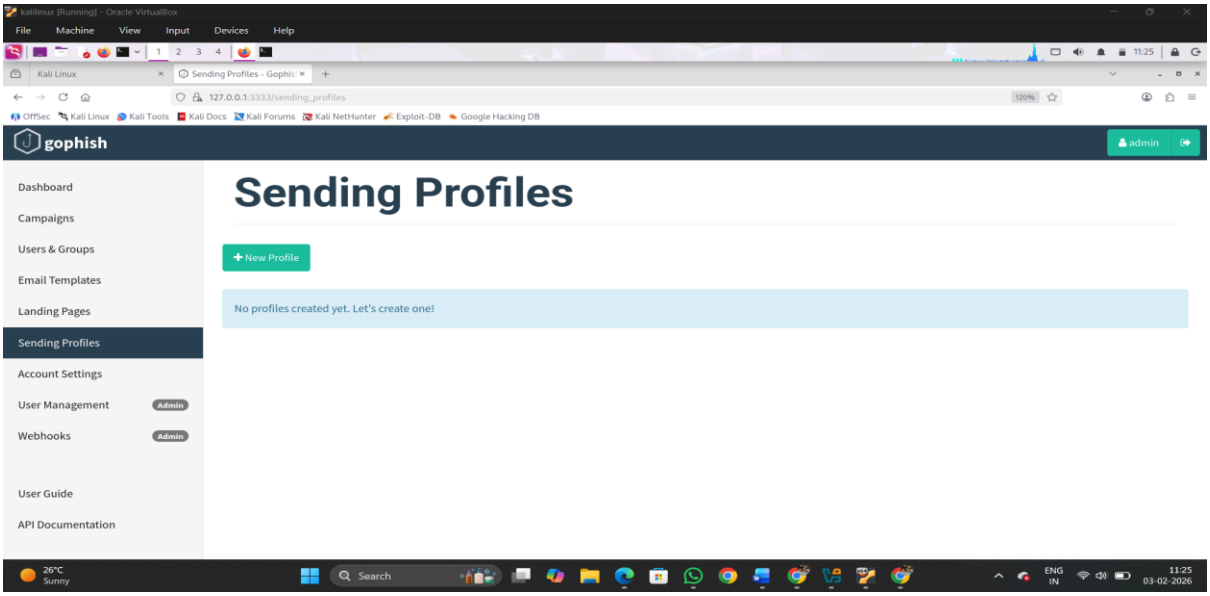
o Host: smtp.gmail.com:587 (example)

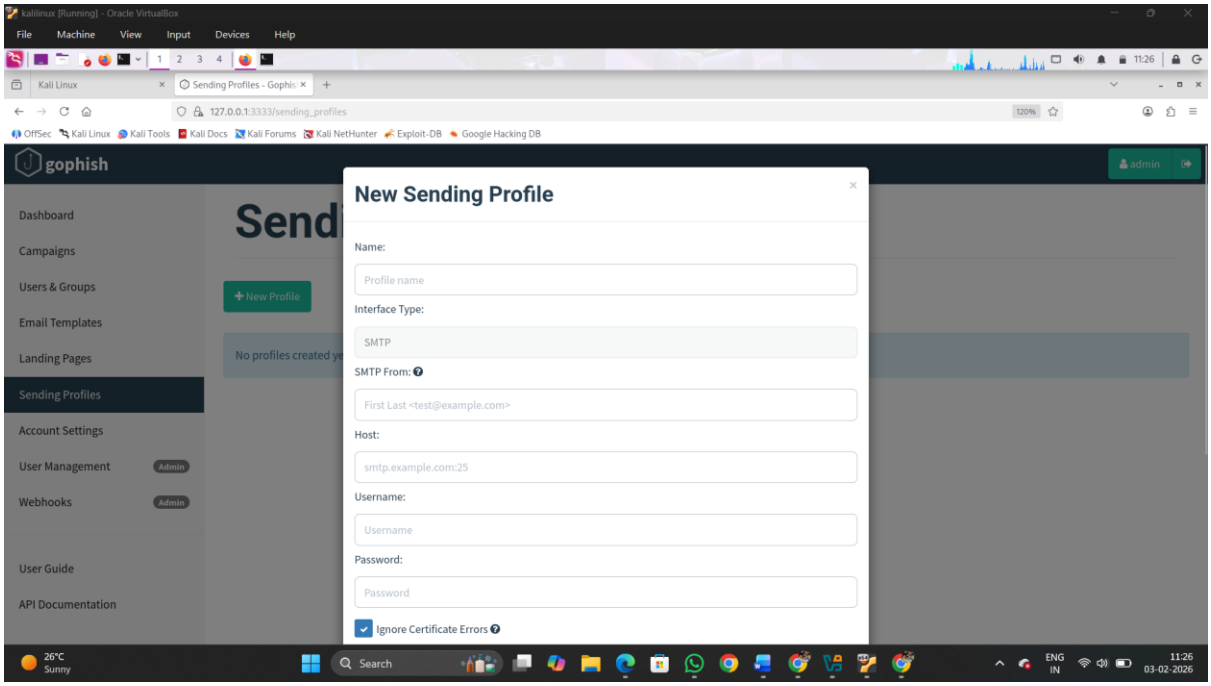
o Username: sender email

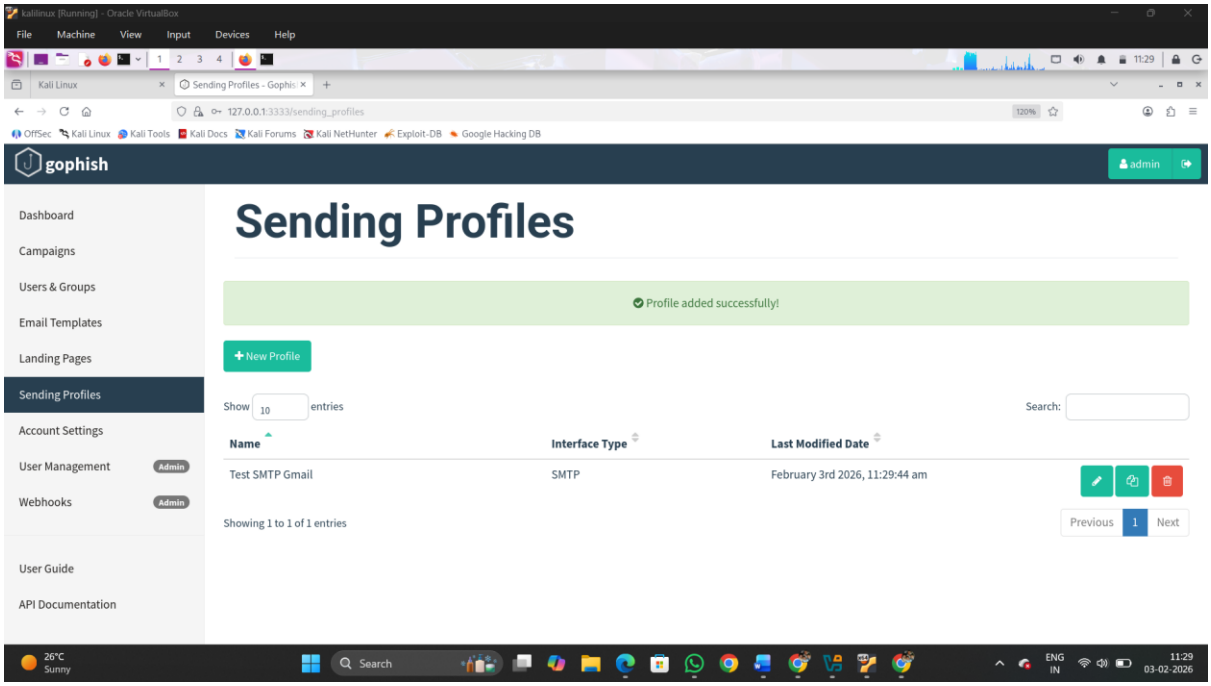
o Password: app password

4. Enable TLS

5. Click Save Profile




gophish
admin
Dashboard
Campaigns
Users & Groups
Email Templates
Landing Pages
Sending Profiles
Account Settings
User Management
Webhooks
User Guide
API Documentation
New Sending Profile
Name:
Profile name
Interface Type:
SMTP
SMTP From:
First Last <test@example.com>
Host:
smtp.example.com:25
Username:
Username
Password:
Password
Ignore Certificate Errors

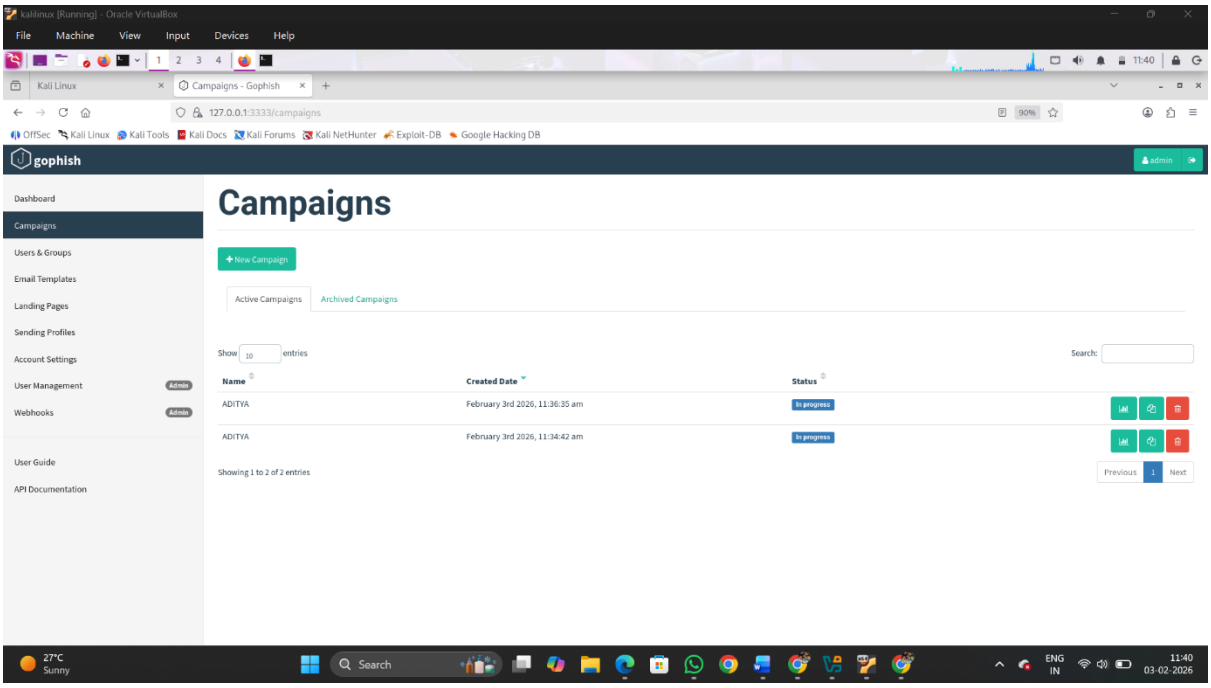


4. Track responses.

   Step 1: Open Campaign Dashboard

   Open GoPhish dashboard

   Click on Campaigns Select the running or completed campaign

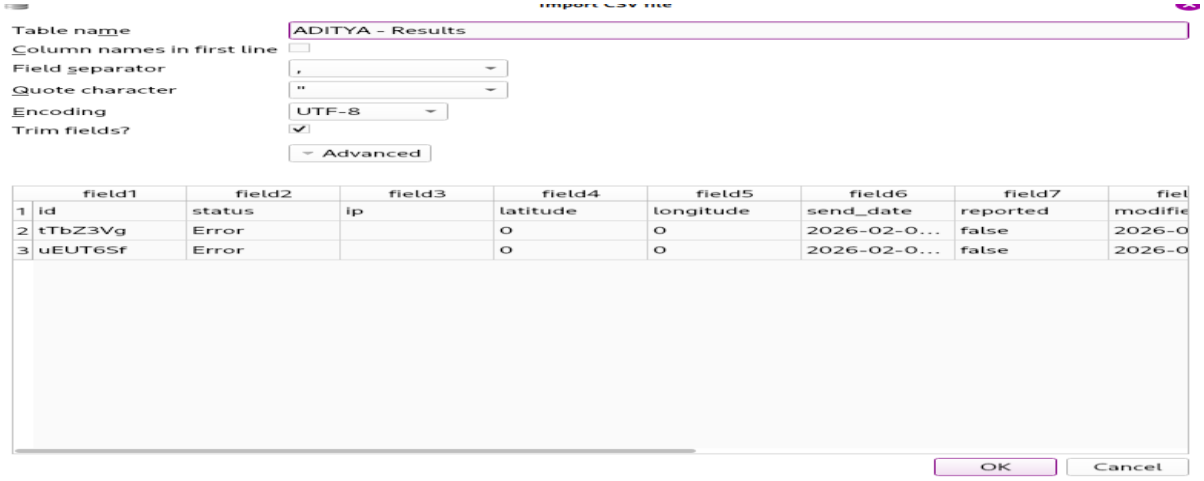


Step 2: View Campaign Statistics On the campaign page,

observe the following metrics

Emails Sent – total number of emails delivered

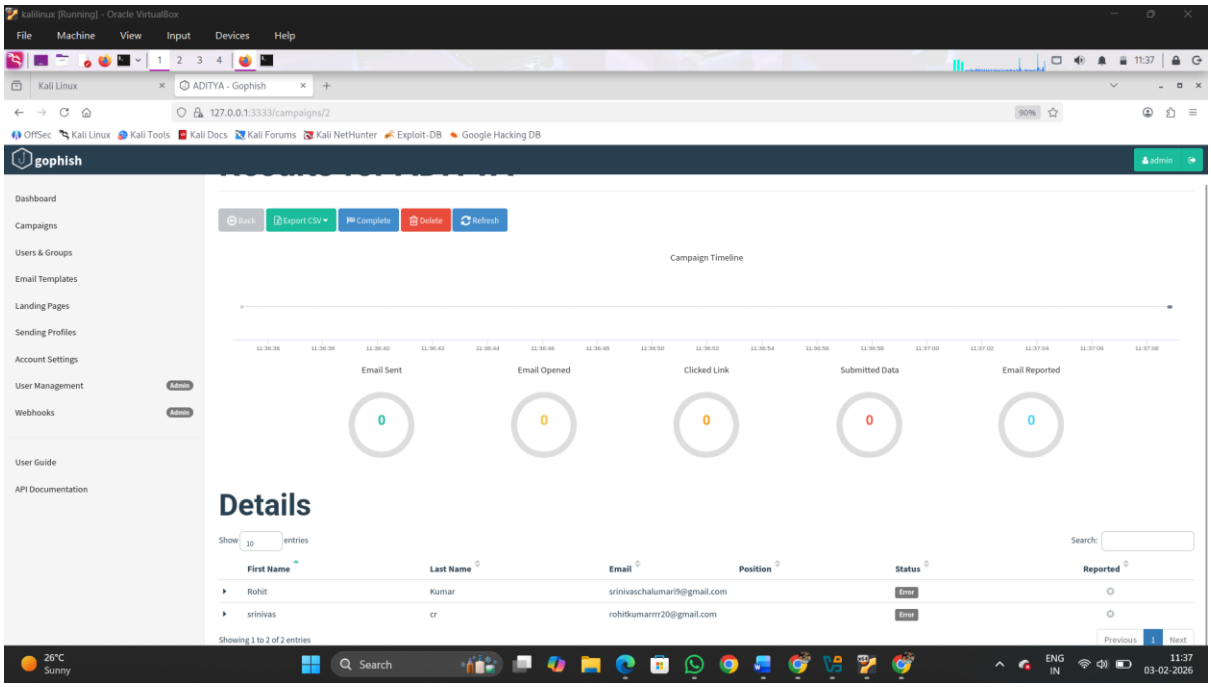
Emails Opened – number of users who opened the email



Clicked Links – users who clicked the phishing link

Submitted Data – users who entered information

Reported – users who reported the email (if enabled)



Step 3: Timeline Analysis View the timeline graph Analyze when users interacted with the email Identify quick clicks indicating high risk

Step 4: Export Results Click Export Results (CSV)

Save the report for documentation or lab record

6. Identify Red Flags

Phishing red flags are common warning signs that suggest an email may be fake or harmful. These signs help users recognize suspicious messages before taking any action. In GoPhish awareness campaigns, such red flags are deliberately added to email templates to demonstrate how attackers exploit trust, urgency, and curiosity. Learning to identify these indicators increases user awareness and helps prevent real-world phishing attacks.

7. Learn Prevention

Phishing prevention involves strategies and best practices used to protect individuals and organizations from phishing attacks. Since phishing mainly targets human behavior rather than technical flaws, prevention focuses on user education, safe email handling practices, and security controls. Understanding phishing prevention reduces the likelihood of successful attacks and helps avoid data breaches, financial losses, and identity theft.

8. Document Simulation

- GoPhish is used as a tool for phishing awareness and simulation
- A phishing email template is designed for the campaign
- A landing page is configured to safely capture user interactions
- An SMTP sending profile is set up for email delivery
- A user group containing test email addresses is created
- A campaign is launched using the selected email template and landing page
- Test phishing emails are sent to users
- User actions such as email opening and link clicking are monitored
- Phishing red flags are identified from the email content
- Campaign results are analyzed to improve user awareness and training effectiveness