

Certified Ethical Hacker (CEH)

Version: 13

Topic: Phishing Email Attack by GoPhish Platform

- This report is prepared strictly for academic and authorized lab purposes only

Table of Content

1. Executive Summery
2. Theoretical Background
3. Methodology
4. Remediation
5. Conclusion

Executive Summery

The primary objective of this study is to demonstrate how phishing attacks are designed, executed, and monitored using GoPhish, while highlighting the risks such attacks pose to organizations. The assignment explores the full phishing lifecycle, including campaign planning, email template creation, landing page configuration, target user selection, and real-time tracking of user interactions such as email opens, link clicks, and credential submissions.

Theoretical Background

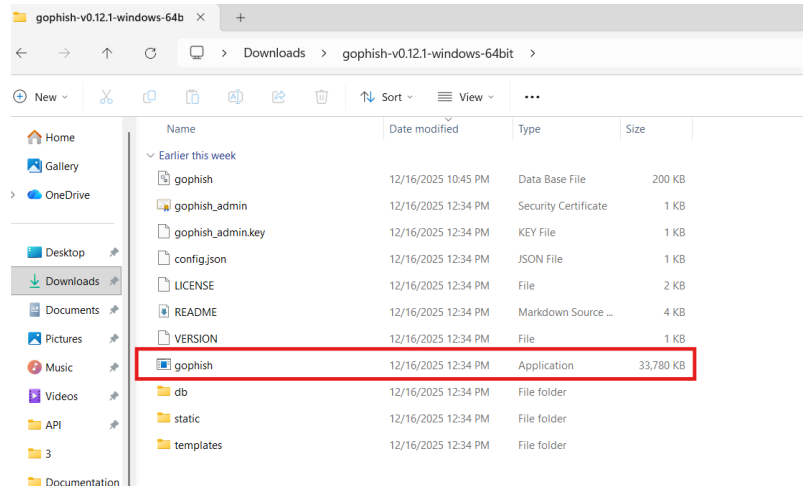
Phishing attacks can be categorized into several types, including generic phishing, spear phishing, whaling, and clone phishing. Each type varies in complexity and target specificity but shares the same fundamental goal: tricking users into performing actions that compromise security. The effectiveness of phishing highlights the human element as one of the weakest links in information security.

- In a controlled lab environment
- On intentionally Execute Phishing Email via GoPhish Platform
- For academic and training purposes only

Methodology

Step:1 We will download Gophish Tools / Application from Internet and Unzip the file and run the Application file

url for download: <https://getgophish.com/>

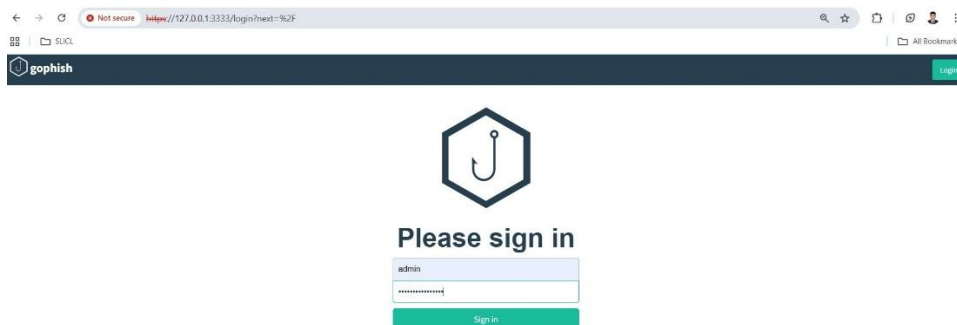


```

C:\Users\Hp\Downloads\gop...
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 20180527213640_0.7.0_store_email_request.sql
OK 20180830215615_0.7.0_send_by_date.sql
OK 20190105192341_0.8.0_rbac.sql
OK 20191104183306_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="2025-12-19T18:48:37+06:00" level=info msg="Please login with the username admin and the password 081a6f57aa34d9e8"
time="2025-12-19T18:48:37+06:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-12-19T18:48:37+06:00" level=info msg="Starting IMAP monitor manager"
time="2025-12-19T18:48:37+06:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
time="2025-12-19T18:48:37+06:00" level=info msg="Creating new self-signed certificates for administration interface"
time="2025-12-19T18:48:37+06:00" level=info msg="Starting new IMAP monitor for user admin"
time="2025-12-19T18:48:37+06:00" level=info msg="TLS Certificate Generation complete"
time="2025-12-19T18:48:37+06:00" level=info msg="Starting admin server at https://127.0.0.1:3333"

```

You will get a dynamic Username: admin & Password: **** and Local Server IP which is <https://127.0.0.1:3333>

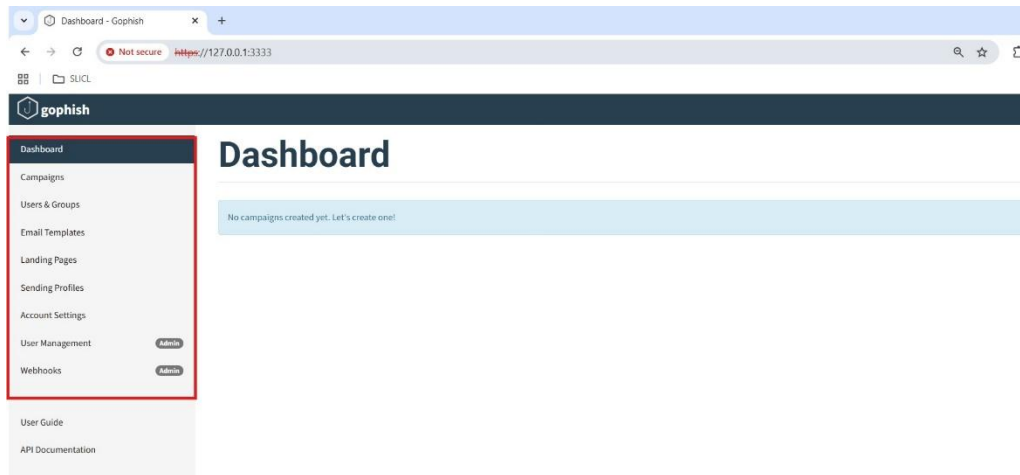


After Successful login with Dynamic user & Password you will get a UI for reset password after first login



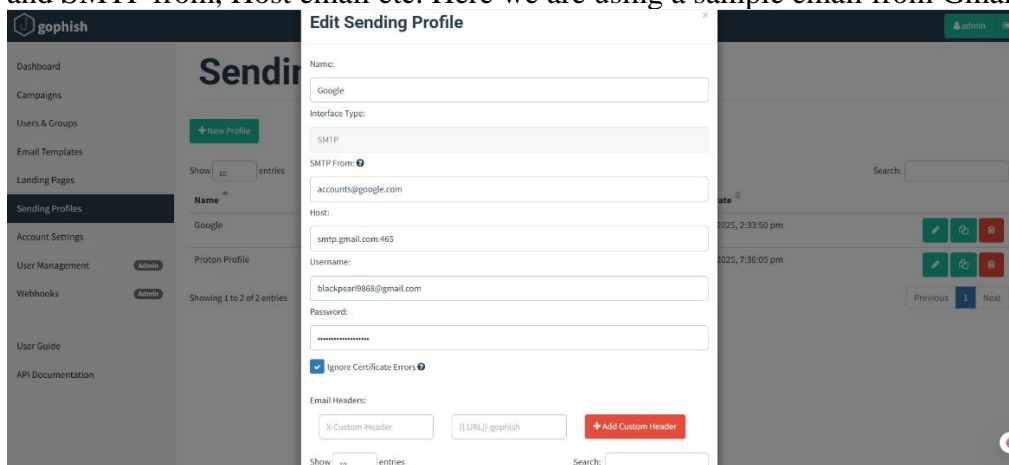
Reset Your Password

Make sure use a Strong password, After Reset password you will get Gophish Home / UI



Step:2 After Login, now we will configure step by step all the Menu. First Sending Profile > Landing Page > Email Templates > User & Groups > Campaign.

Sending Page: A sending page is include by which email address is using for the Phishing Email and SMTP from, Host email etc. Here we are using a sample email from Gmail platform



Here> Name is : Google (you can config whatever you wants)

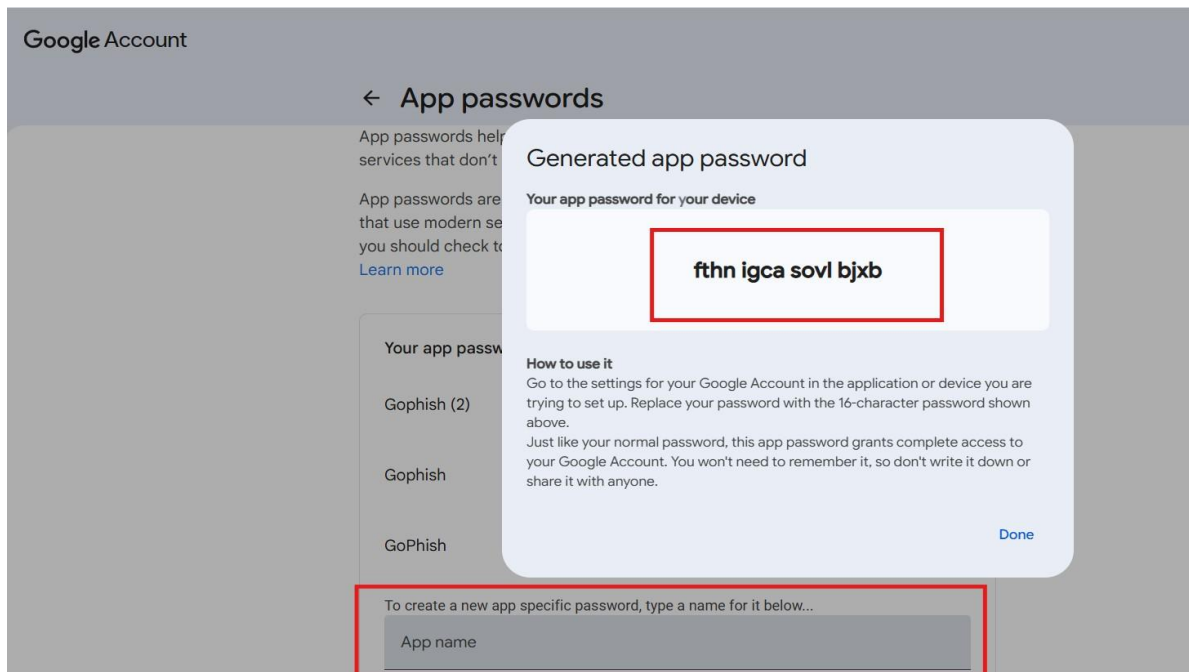
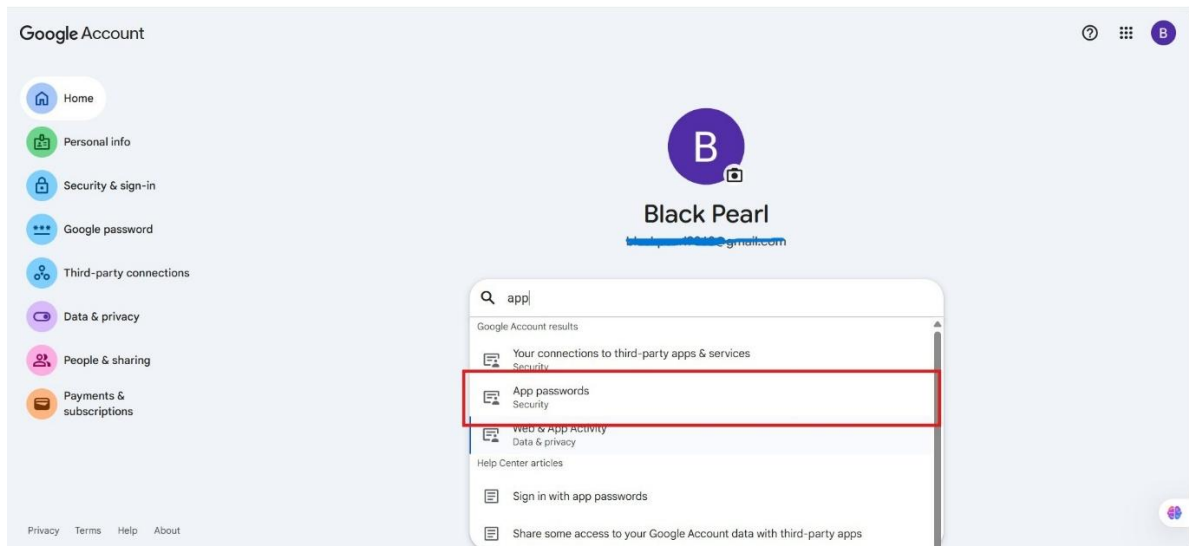
Interface Type: by default SMTP

SMTP from: as we are using google platform > accounts@google.com

Host: smtp.google.com:465

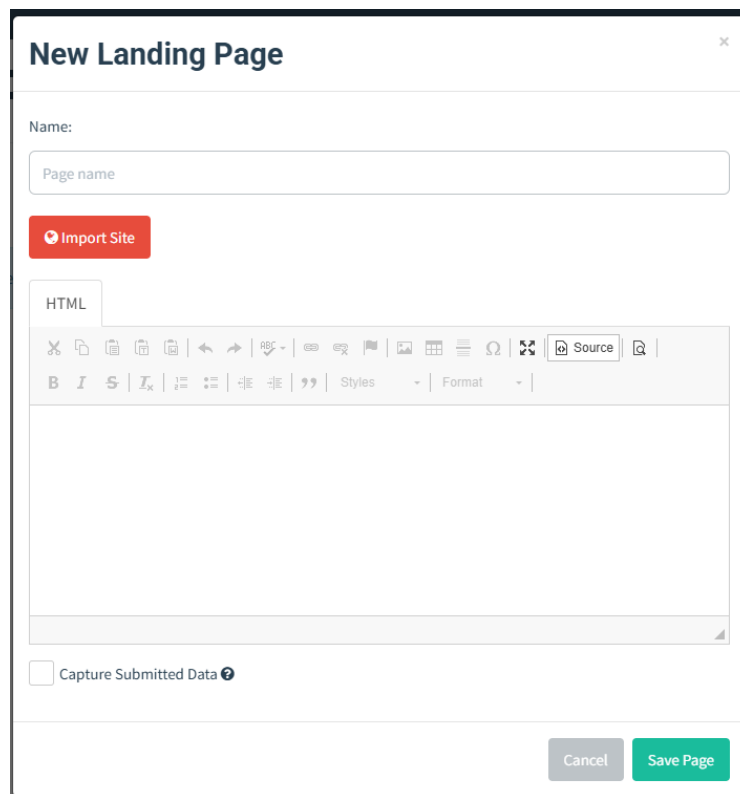
Username: *****@gmail.com [as we are using gmail account]

pass: This password is App password which is generate from Particular Gmail Accounts Menu



N:B > Must be enable 2 Step Verification in Google Accounts otherwise you will not be able generate App Password.

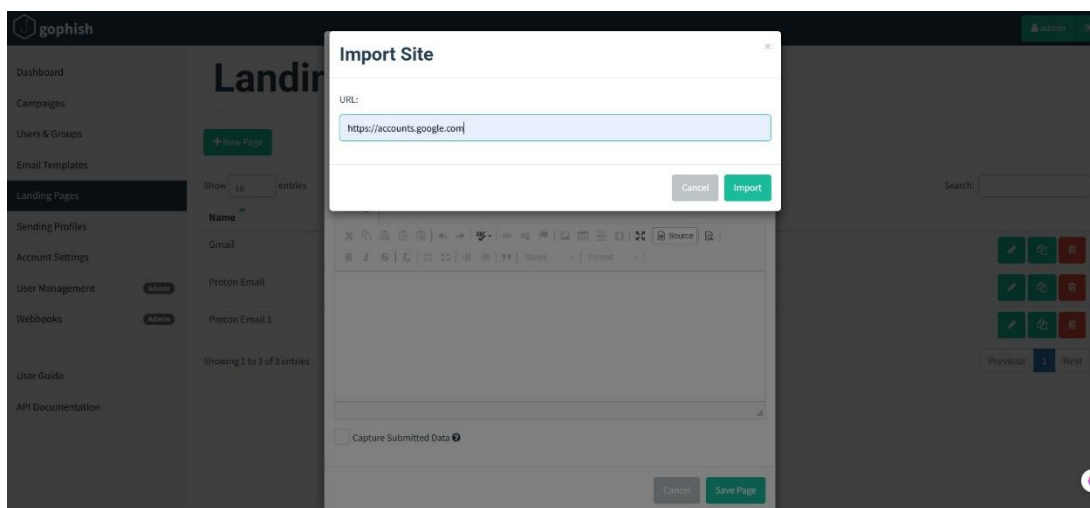
Step:3 Now we will configure Landing Page [This is most important part of Gophish platform]
Landing Page: A landing page is include a Site that Target will redirect after click the Email Link that you are going to send.



The screenshot shows the 'New Landing Page' form in the Gophish application. At the top, there's a title 'New Landing Page' with a close button. Below it is a 'Name:' label followed by a text input field containing 'Page name'. A red button labeled 'Import Site' is positioned below the input field. Underneath is a tab labeled 'HTML'. Below the tab is a rich text editor with various icons for text formatting (bold, italic, underline, strikethrough, link, unlink, bulleted list, numbered list, indent, outdent, quote) and a 'Source' button. At the bottom of the form, there is a checkbox labeled 'Capture Submitted Data' with a help icon. At the very bottom, there are two buttons: 'Cancel' and 'Save Page'.

Here, Name> As you you like.

You can add a HTML code if you have one or you can import a HTML code from a link, we will use 2 html code. One is from direct link which is Gmail platform and another is own writing a html code exactly look like Proton Mail platform



The screenshot shows the Gophish dashboard with the 'Import Site' dialog box open. The dashboard has a dark sidebar with navigation links: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages (selected), Sending Profiles, Account Settings, User Management, Webhooks, User Guide, and API Documentation. The main area shows a 'Landing Pages' table with columns for Name, Email, and Proton Email. The 'Import Site' dialog has a 'URL:' label and a text input field containing 'https://accounts.google.com'. It also has 'Cancel' and 'Import' buttons. The background shows the 'New Landing Page' form from the previous image, slightly dimmed.

Another One we will use own HTML code which look like Proton mail login page.

OWN HTML code which look like Proton Mail logo

Edit Landing Page

Name:

Proton Email

Import Site

HTML

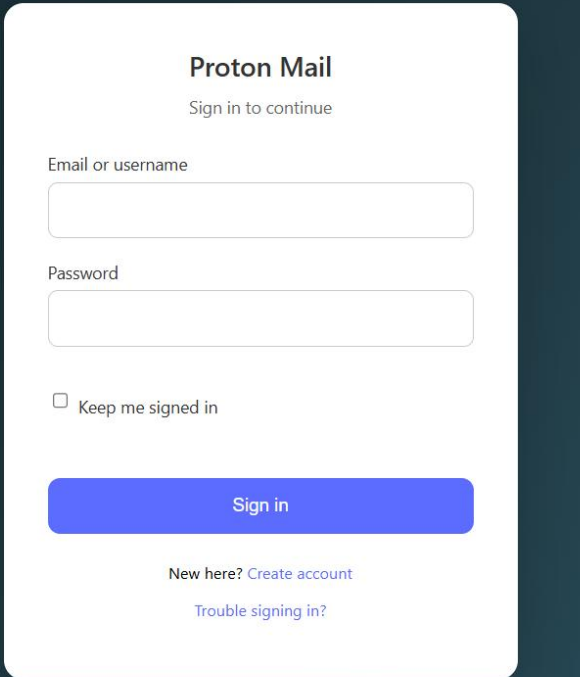
X Copy Paste Undo Redo ABC Font Color Background Color Bulleted List Numbered List Link Unlink Table Row Column Link Preview Source Help

<!DOCTYPE html><html lang="en"><head>
<meta charset="UTF-8"/>
<title>Secure Sign In</title>
<meta name="viewport" content="width=device-width, initial-scale=1.0"/>

<style>
 * {
 box-sizing: border-box;

Capture Submitted Data ?

Cancel Save Page

The image shows the Proton Mail sign-in interface. It features a dark blue background with a white rounded rectangle in the center. Inside the rectangle, the text "Proton Mail" is displayed in a large, bold, black font. Below it, the text "Sign in to continue" is shown in a smaller, regular black font. There are two input fields: the first is labeled "Email or username" and the second is labeled "Password". Both fields are empty and have a light gray border. Below the password field, there is a checkbox labeled "Keep me signed in". At the bottom of the white rectangle, there is a large, rounded blue button with the text "Sign in" in white. Below the button, there is a link that says "New here? Create account" and another link below it that says "Trouble signing in?".

Proton Mail

Sign in to continue

Email or username

Password

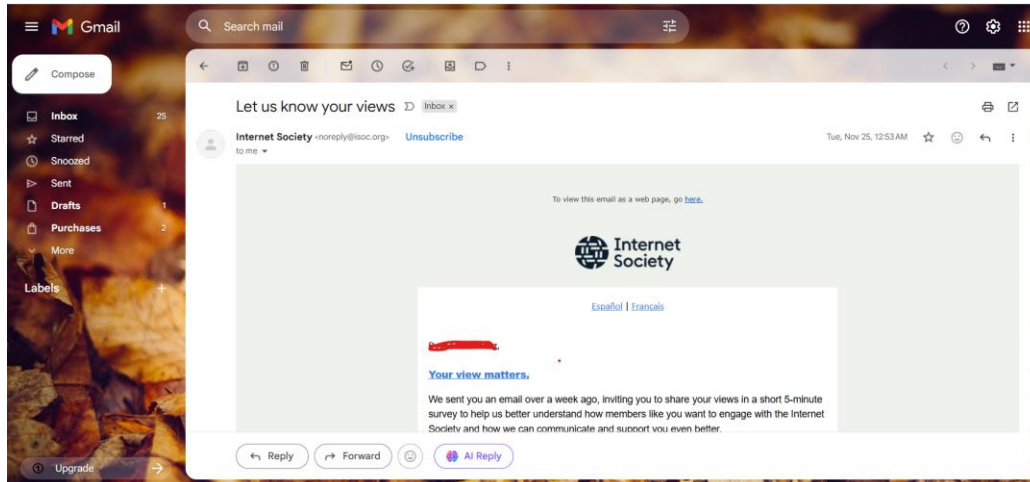
☐ Keep me signed in

Sign in

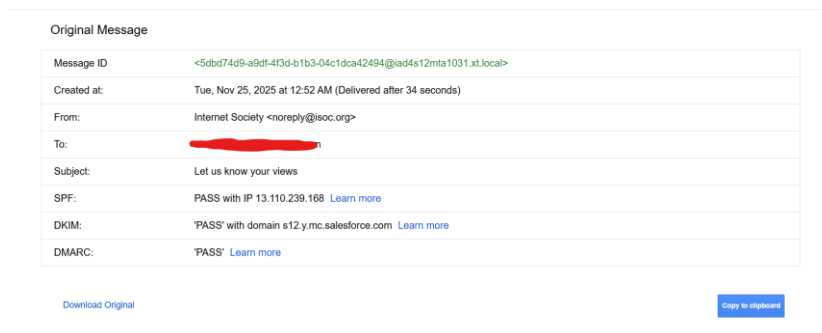
New here? [Create account](#)

[Trouble signing in?](#)

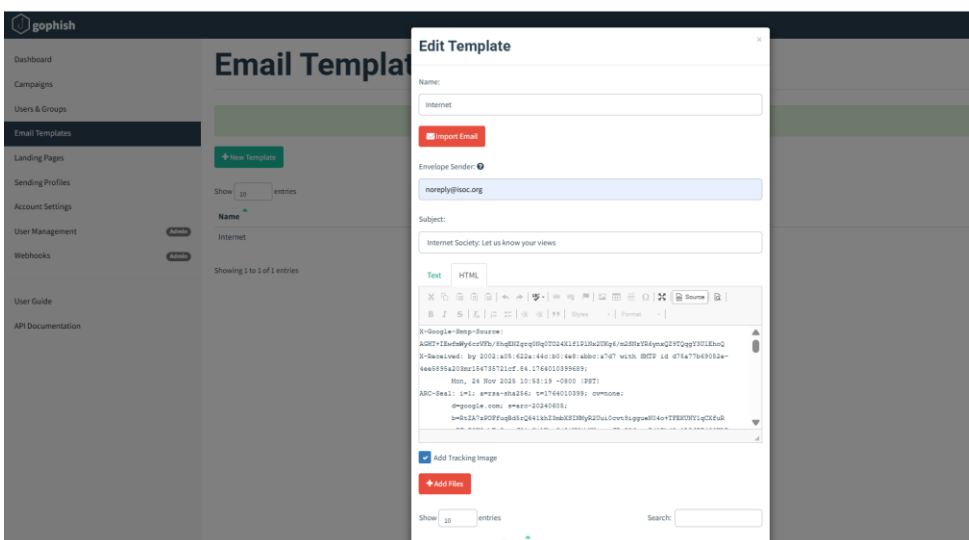
Step 3: Once, Landing Page is configured, we will configure Email template. You can generate Email template from several source, Like Here will Generate a Email Template from Real Google account and import it our Gophish platform.



This a email which are internet Society and we will use this temaplte fro our own. So here we need the code which will find out by > Top bottom you are seeing three dots > show original > copy clipboard.



Paste it as in our Gophish platform >



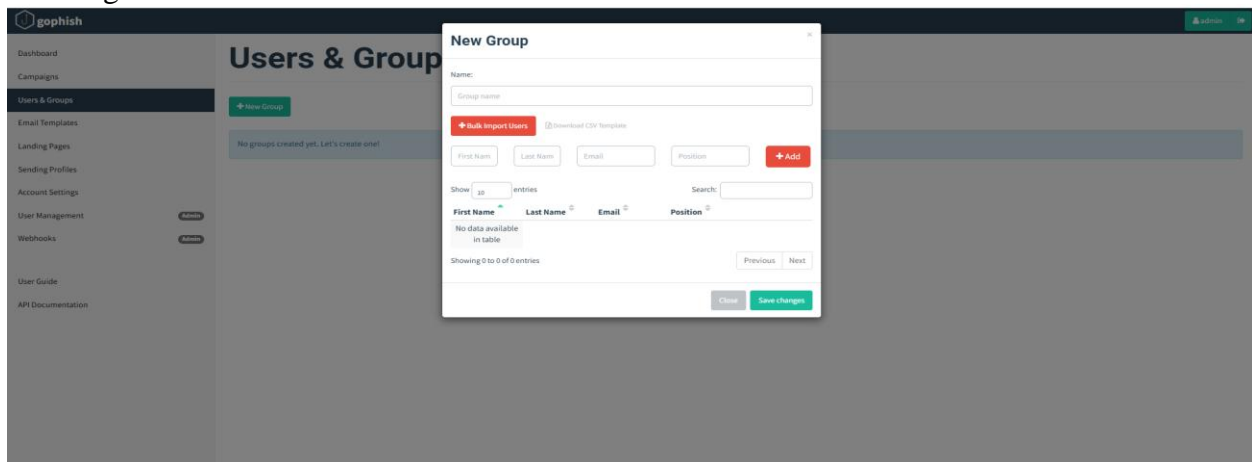
Here> Name: add a name

Envelop Sender: As it was from internet society

Subject: As it was from Email Subject or you add config as your own Subject that will look like real.

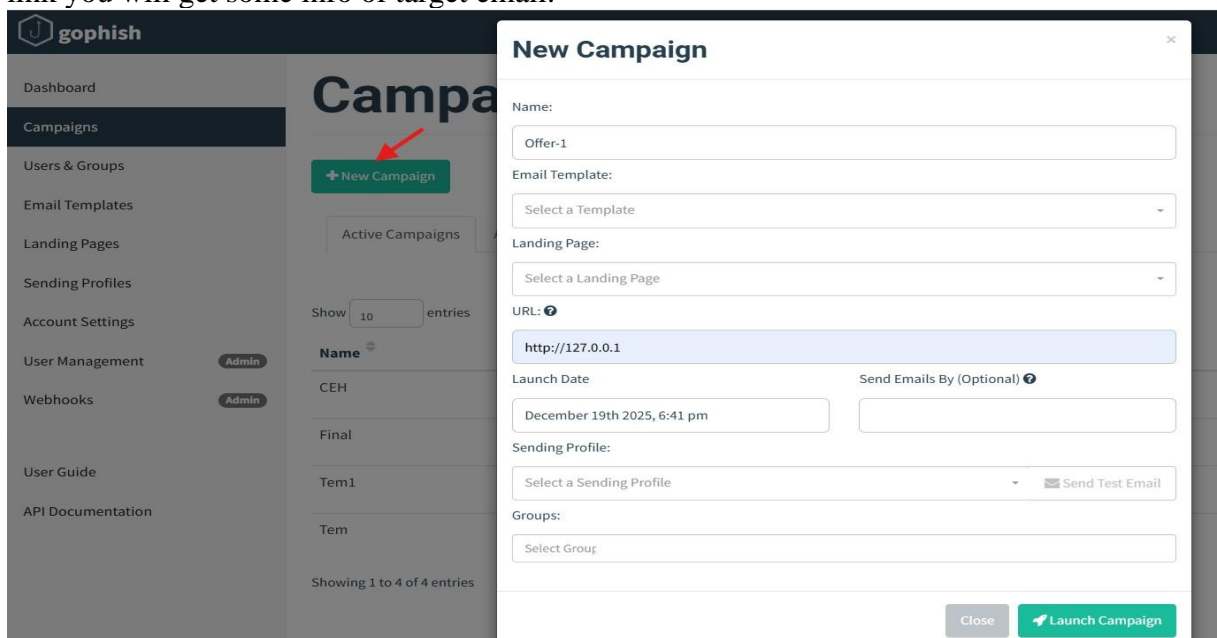
HTML code: copy paste from *show original*.

Step 4: Now we will configure User & Groups. This is included in which email you want to send Phishing Email.

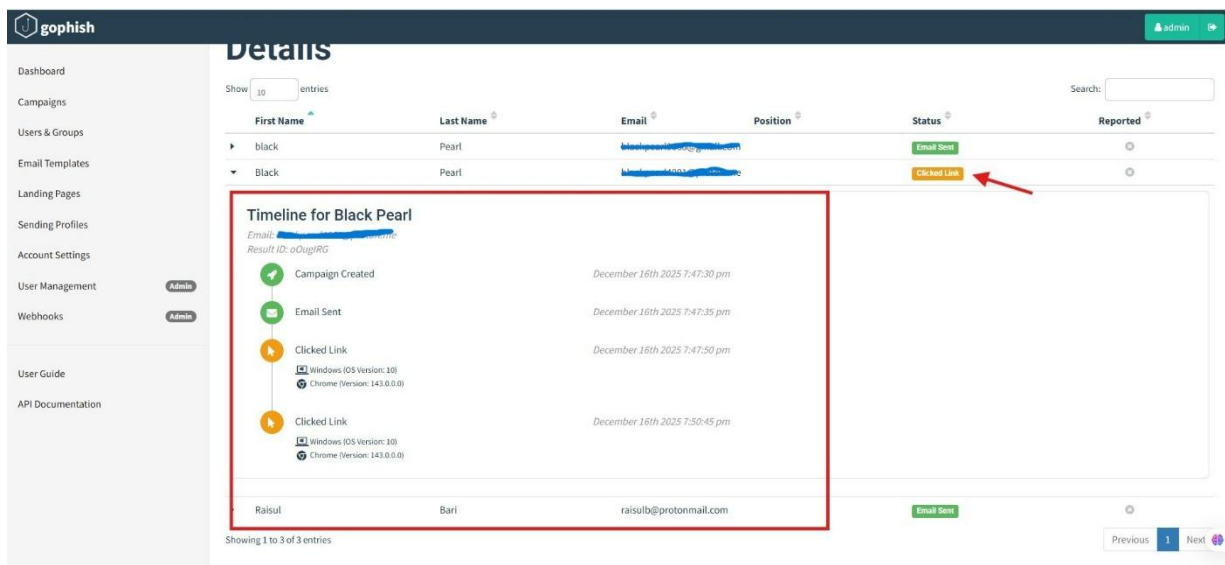
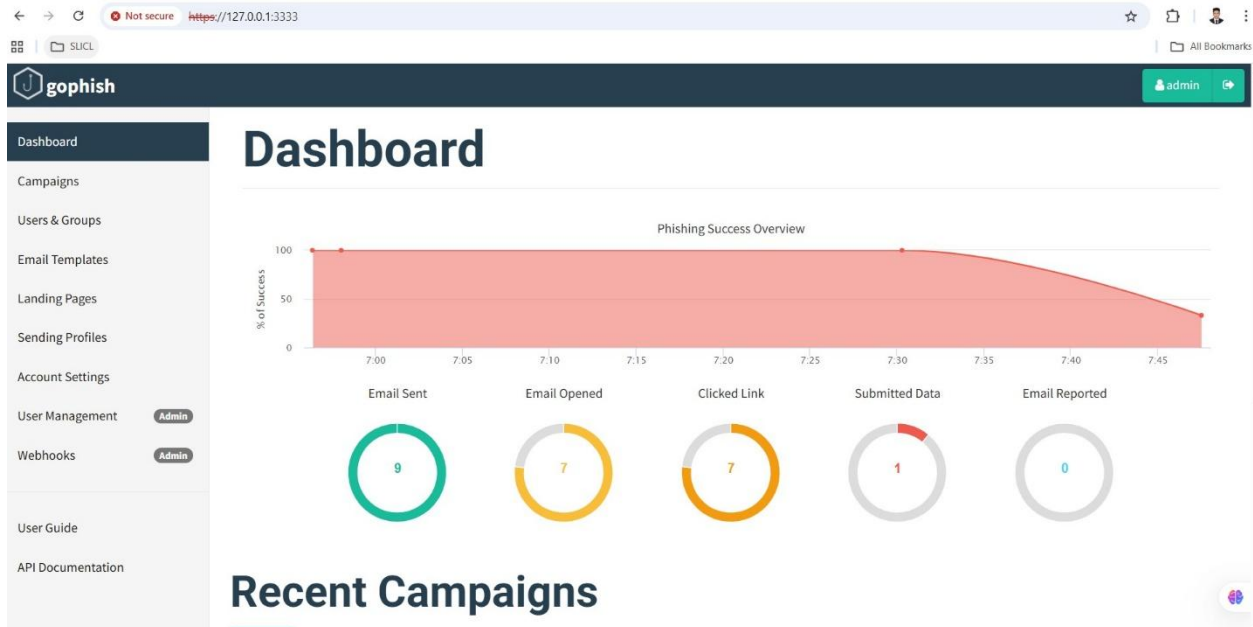


You can add Multiple Email address by +Add.

Step 5: Now we will Configure a Campaign which will include Sending Page> Landing Page > Email Template > User & Groups. After Successfully Configured all the items, Target Email will get a Email from your real Email but Redirect to your Own Landing Page and After clicking any link you will get some info of target email.



Step 6: Once Campaign Generate, you will get a Dashboard Like below, Including How Many Emails you have send, how many Target Has open the email and click your redirect link.



Remediation:

Regular security awareness training, focusing on how to identify phishing emails, suspicious links, and fake login pages. Employees should be trained to verify sender addresses, avoid clicking unknown links, and report suspected phishing attempts immediately.

Organizations should strengthen email security controls, including spam filters, email gateways, and authentication mechanisms such as SPF, DKIM, and DMARC. Implementing **Multi-factor authentication (MFA)** can significantly reduce the impact of compromised credentials obtained through phishing.

Conclusion

Phishing email attacks remain a critical cybersecurity threat due to their reliance on human behavior rather than technical vulnerabilities. This assignment demonstrated how the GoPhish platform can be used to simulate real-world phishing attacks in a controlled and ethical manner. The findings show that user awareness plays a vital role in preventing phishing incidents. In conclusion, combining phishing simulations, user training, and strong technical controls is essential for reducing phishing risks and strengthening an organization's overall security posture.

Reference: <https://www.youtube.com/watch?v=Yes4oc046hY>