

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 Summary
2. Theoretical Background
3. Methodology
4. Remediation
5. Conclusion

Executive Summary

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.

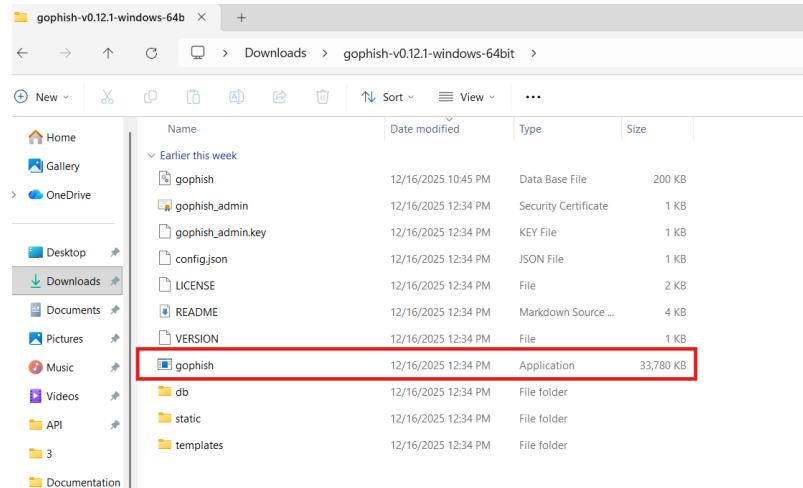
Theoretical Background

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

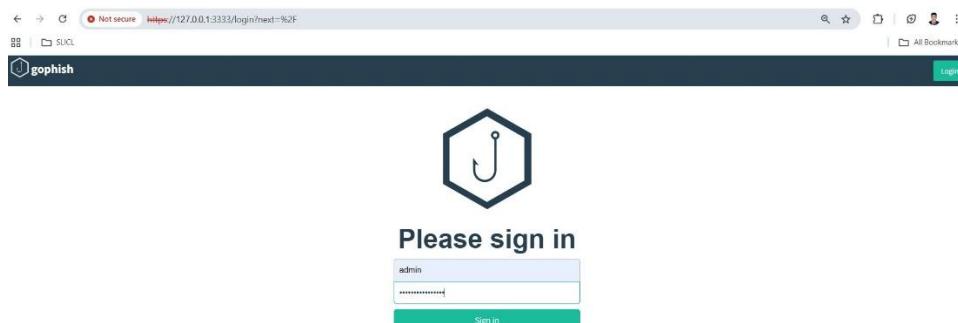
Methodology

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\gophi... + 
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_5.1_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 20191041033096_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_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://0.0.0.0:0" 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

Reset Your Password

Forgot your password? Click [here](#).

Enter your email address below to receive a password reset link.

Email Address:

[Get Reset Link](#)

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

The screenshot shows the Gophish web interface. The top navigation bar includes a back button, forward button, refresh button, and a URL bar showing 'Not secure https://127.0.0.1:3333'. Below the header is a dark navigation bar with the 'gophish' logo. The main content area has a title 'Dashboard' and a message 'No campaigns created yet. Let's create one!'. On the left, a sidebar menu is open, showing 'Dashboard' as the active item, followed by 'Campaigns', 'Users & Groups', 'Email Templates', 'Landing Pages', 'Sending Profiles', 'Account Settings', 'User Management' (with 'Admin' status), and 'Webhooks' (with 'Admin' status). At the bottom of the sidebar are links for 'User Guide' and 'API Documentation'.

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

The screenshot shows the 'Edit Sending Profile' dialog box. The left sidebar of the main window is visible, showing 'Dashboard', 'Campaigns', 'Users & Groups', 'Email Templates', 'Landing Pages', 'Sending Profiles' (selected), 'Account Settings', 'User Management' (with 'Admin' status), and 'Webhooks' (with 'Admin' status). The main area shows a list of profiles: 'Google' (selected) and 'Proton Profile'. The 'Google' profile details are displayed: Name: Google, Interface Type: SMTP, SMTP From: accounts@google.com, Host: smtp.gmail.com:465, Username: blackpearl06@gmail.com, and Password: (redacted). The 'Ignore Certificate Errors' checkbox is checked. The right side of the dialog shows a preview of an email message with recipient 'blackpearl06@gmail.com' and timestamp '2025, 7:36:05 pm'.

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]

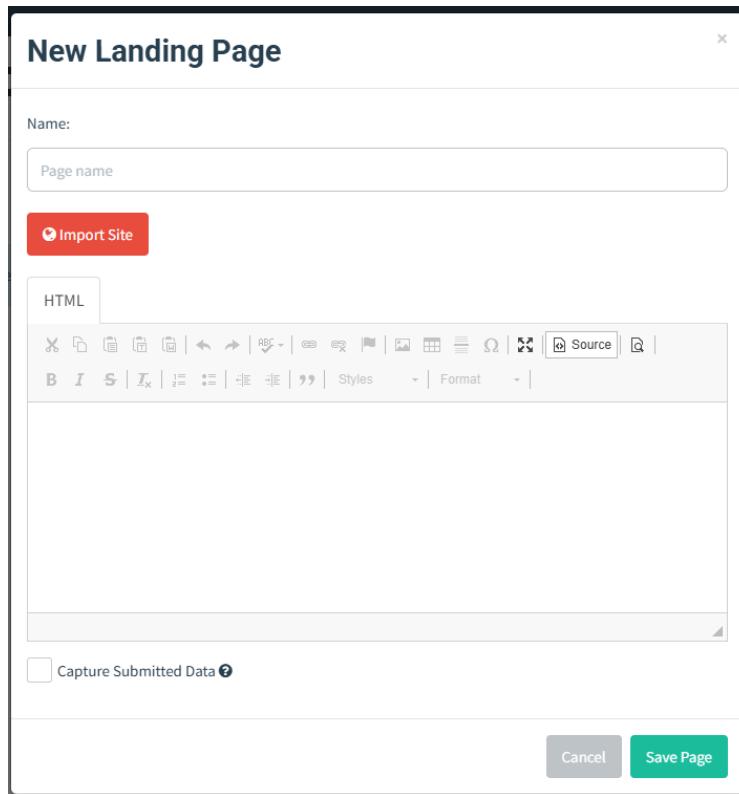
pass: This password is App password which is generate from Particular Gmail Accounts Menu

The screenshot shows the 'Google Account' settings interface. On the left, there's a sidebar with various options: Home, Personal info, Security & sign-in, Google password, Third-party connections, Data & privacy, People & sharing, and Payments & subscriptions. The 'Security & sign-in' option is highlighted. In the main area, there's a profile picture for 'Black Pearl' and a link to 'https://blackpearl@gmail.com'. Below this, a search bar contains the text 'app'. A red box highlights the 'App passwords' link under the 'Your connections to third-party apps & services' heading. Other visible links include 'Sign in with app passwords' and 'Share some access to your Google Account data with third-party apps'. At the bottom of the sidebar, there are links for Privacy, Terms, Help, and About.

The screenshot shows the 'App passwords' screen. At the top, it says 'Generated app password' and 'Your app password for your device'. Below this, a large red box highlights the generated password 'fthn igca sovl bjxb'. To the right, there's a 'Done' button. Further down, there's a section titled 'How to use it' with instructions about replacing the password in app settings. At the bottom, there's a text input field labeled 'To create a new app specific password, type a name for it below...' with 'App name' typed into it. A red box highlights this input field.

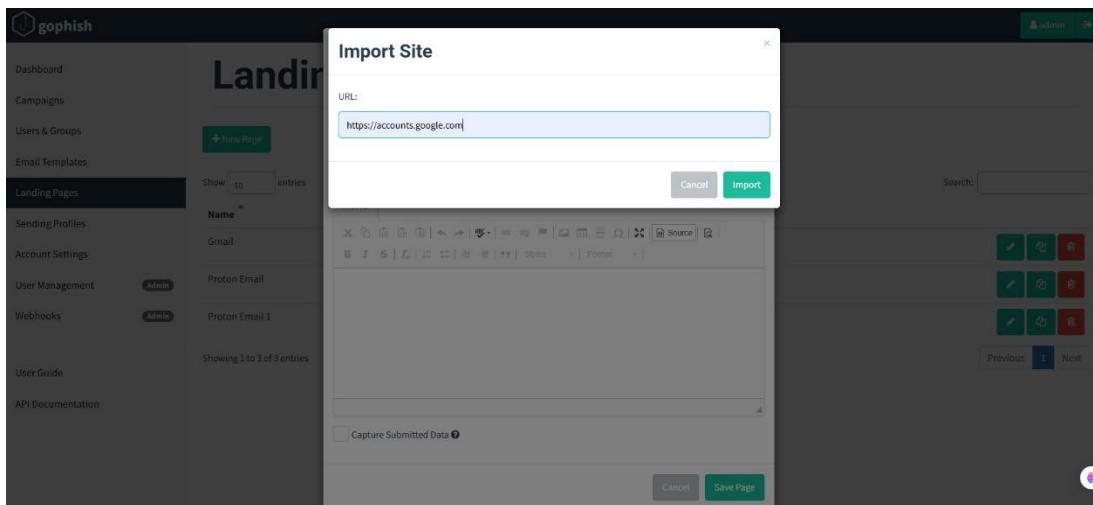
N:B > Must be enable 2 Step Verification in Google Accounts otherwise you will not be able generate App Password.

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.



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



New Landing Page

Name:

HTML

Capture Submitted Data ?

And Save page. Sometimes it will give you error, If not you can save page and after target click the email link it will redirect as Sign in option is look like Google account.

New Landing Page

template: template:73: unexpected bad character U+003D '=' in command

Name:

HTML

Capture Submitted Data ?

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

Edit Landing Page

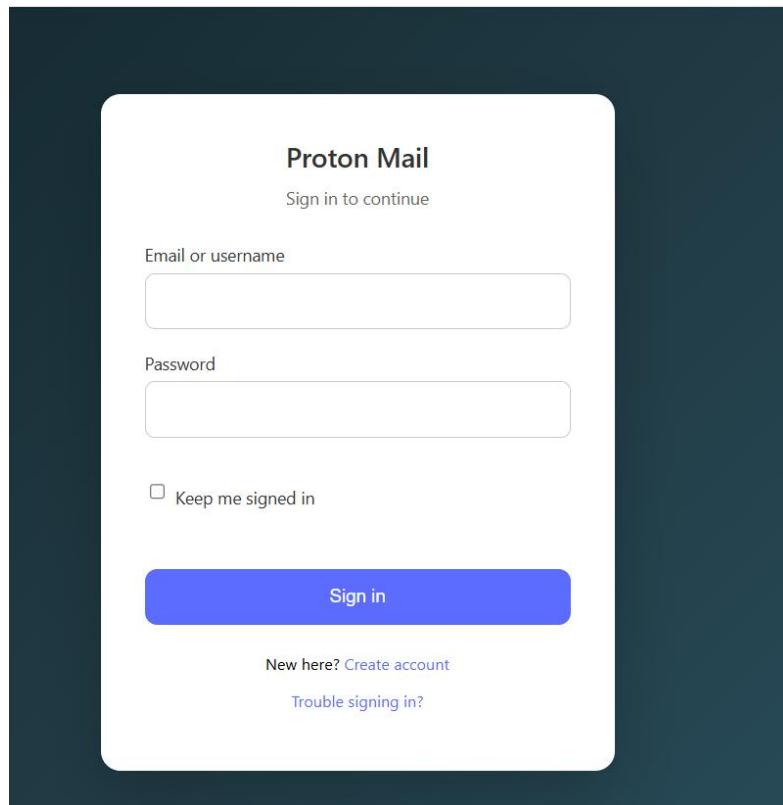
Name:
Proton Email

HTML

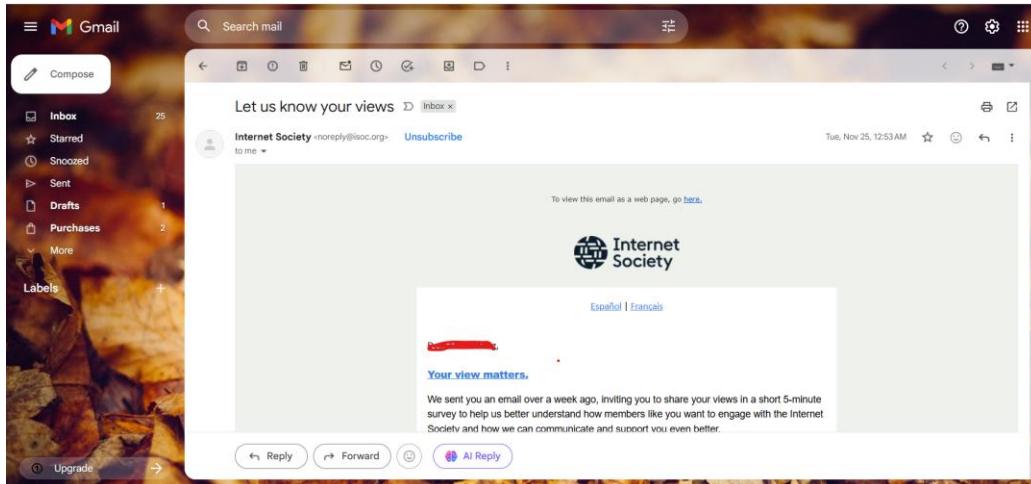
```
<!DOCTYPE html><html lang="en"><head>
<meta charset="UTF-8"/>
<title>Secure Sign In</title>
<meta name="viewport" content="width=device-width, initial-scale=1.0"/>

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

Capture Submitted Data ?



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.

Original Message

Message ID	<5dbd74d9-a9df-4f3d-b1b3-04c1dca42494@iad4s12mta1031.xt.local>
Created at:	Tue, Nov 25, 2025 at 12:52 AM (Delivered after 34 seconds)
From:	Internet Society <noreply@soc.org>
To:	[REDACTED]
Subject:	Let us know your views
SPP:	PASS with IP 13.110.239.168 Learn more
DKIM:	'PASS' with domain s12.y.mc.salesforce.com Learn more
DMARC:	'PASS' Learn more

[Download Original](#) [Copy to clipboard](#)

Paste it as in our Gophish platform >

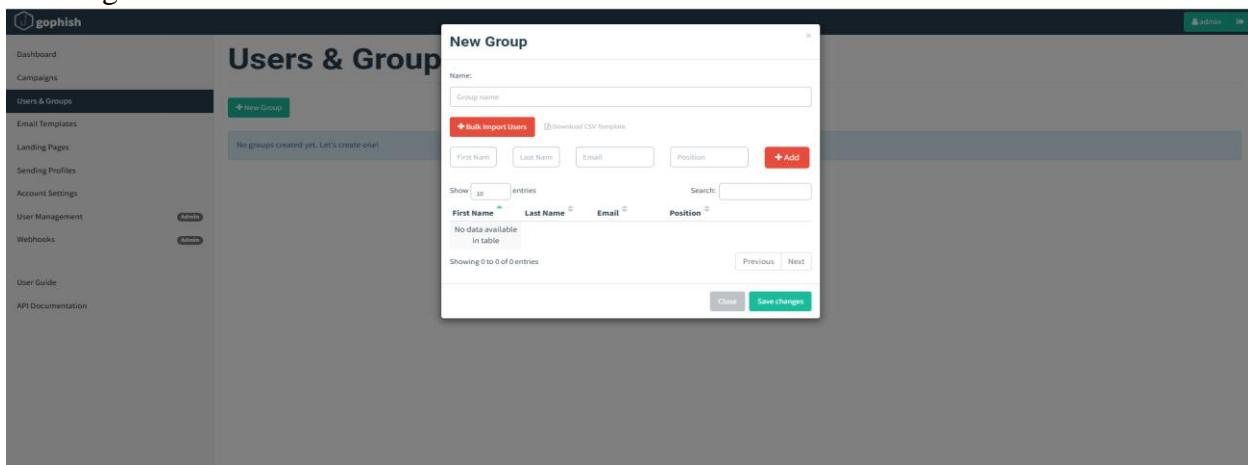
Here> Name: add a name

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.

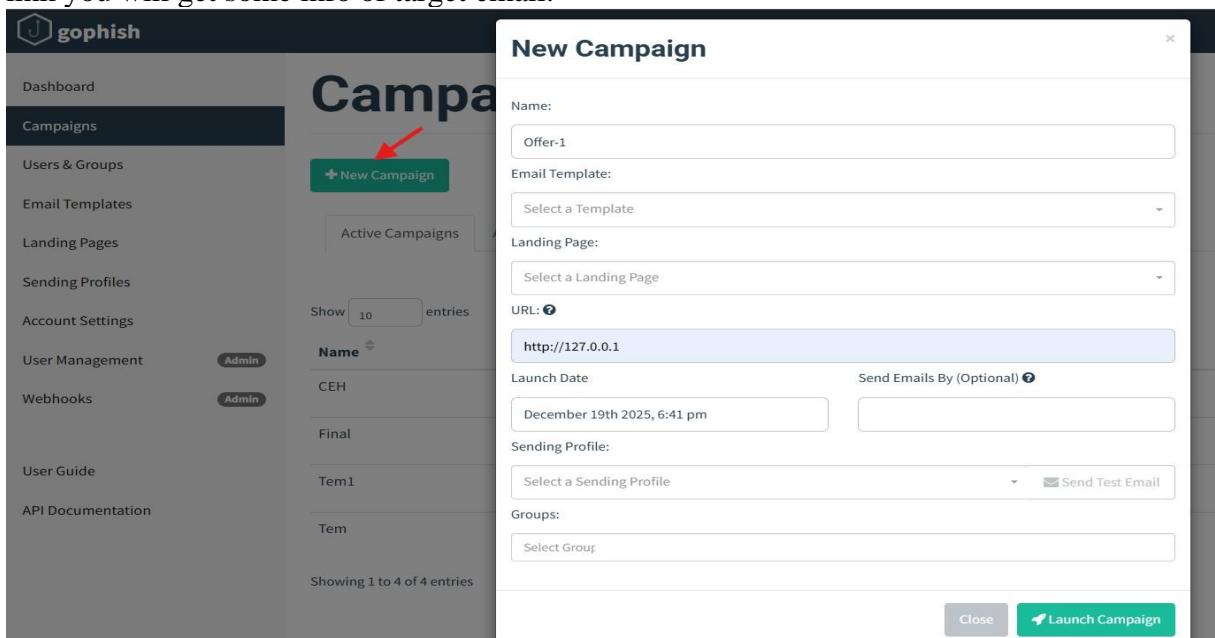
HTML code: copy paste from **show original**.

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

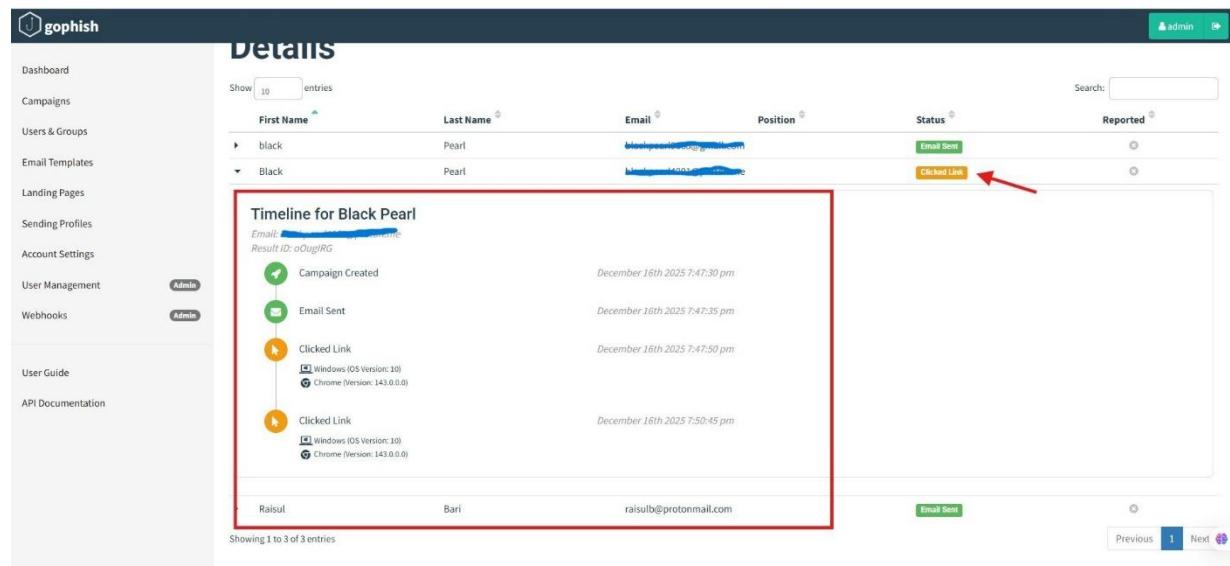
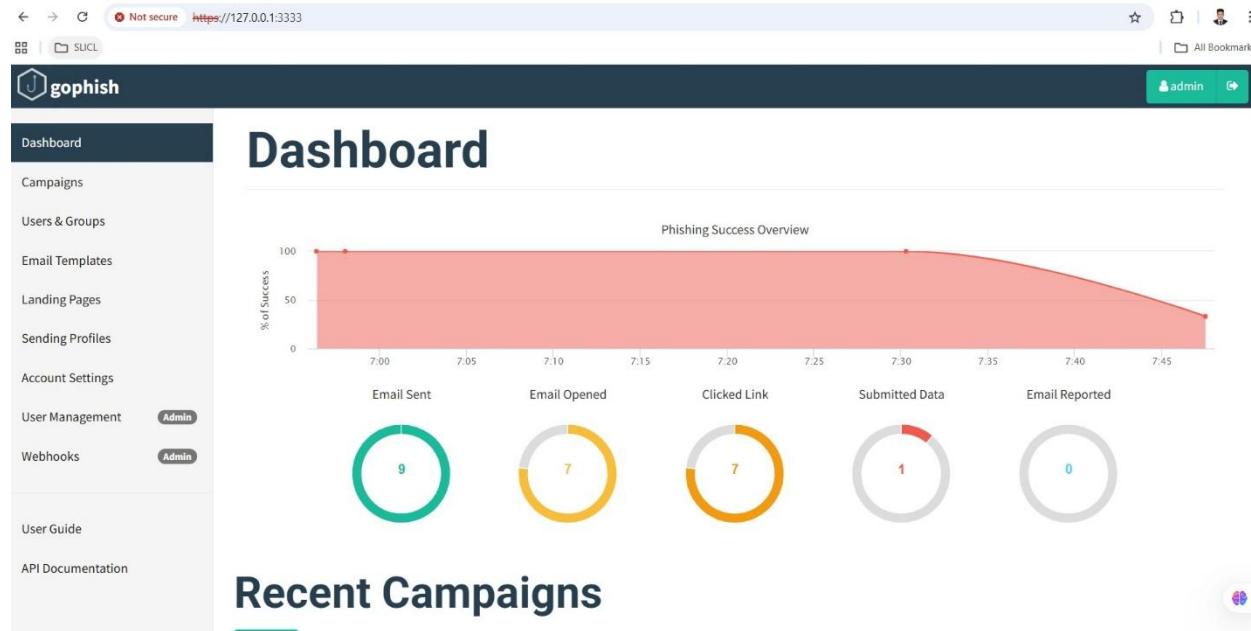


You can add Multiple Email address by +Add.

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>