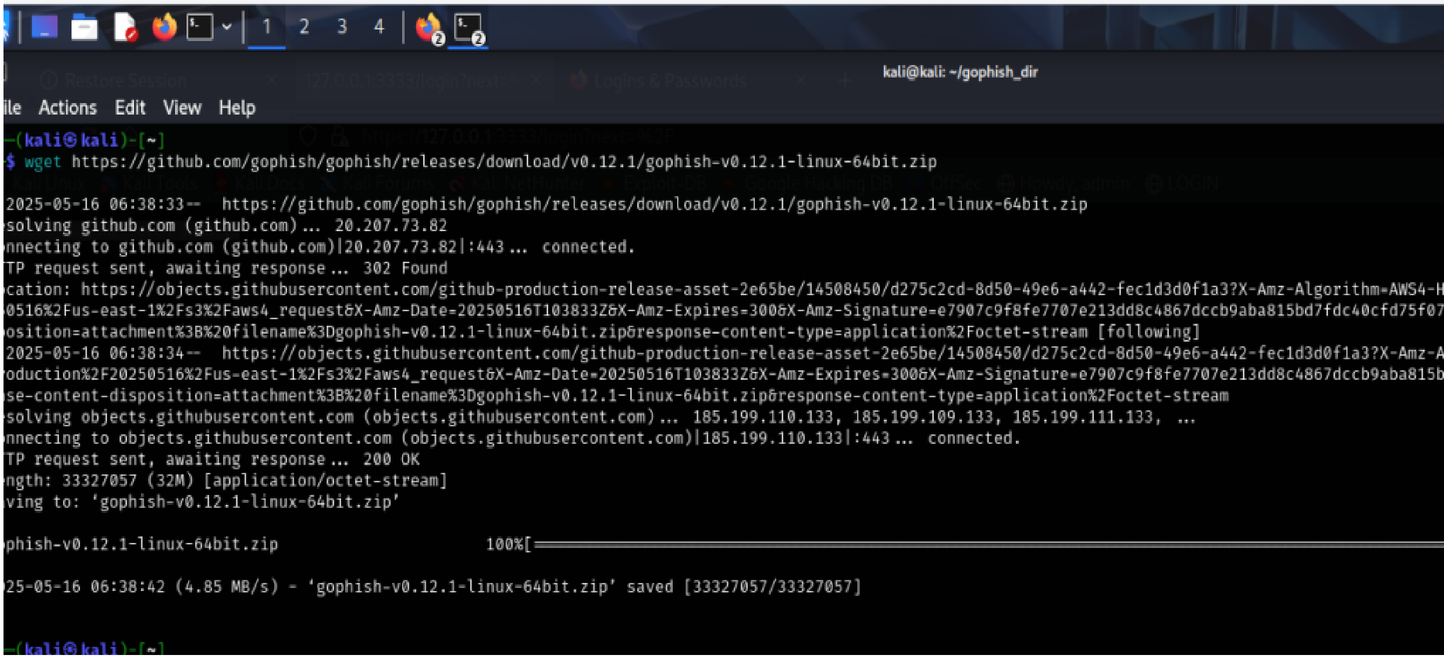
Task 2 Report: Social Engineering & Phishing Simulation

in this task we will do phishing attack using gophish and test the awareness of employees.

First we need to download gophish in kali linux machine and unzip them.



```
—(kali㉿kali)-[~]
$ wget https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip

2025-05-16 06:38:33--  https://github.com/gophish/gophish/releases/download/v0.12.1/gophish-v0.12.1-linux-64bit.zip
solving github.com (github.com)... 20.207.73.82
nnecting to github.com (github.com)|20.207.73.82|:443... connected.
TP request sent, awaiting response... 302 Found
cation: https://objects.githubusercontent.com/github-production-release-asset-2e65be/14508450/d275c2cd-8d50-49e6-a442-fec1d3d0f1a3?X-Amz-Algorithm=AWS4-H
0516%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250516T103833Z&X-Amz-Expires=300&X-Amz-Signature=e7907c9f8fe7707e213dd8c4867dccb9aba815bd7fdc40cfd75f07
osition=attachment%3B%20filename%3Dgophish-v0.12.1-linux-64bit.zip&response-content-type=application%2Foctet-stream [following]
2025-05-16 06:38:34--  https://objects.githubusercontent.com/github-production-release-asset-2e65be/14508450/d275c2cd-8d50-49e6-a442-fec1d3d0f1a3?X-Amz-A
oduction%2F20250516%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20250516T103833Z&X-Amz-Expires=300&X-Amz-Signature=e7907c9f8fe7707e213dd8c4867dccb9aba815b
se-content-disposition=attachment%3B%20filename%3Dgophish-v0.12.1-linux-64bit.zip&response-content-type=application%2Foctet-stream
solving objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.110.133, 185.199.109.133, 185.199.111.133, ...
nnecting to objects.githubusercontent.com (objects.githubusercontent.com)|185.199.110.133|:443... connected.
TP request sent, awaiting response... 200 OK
ngth: 33327057 (32M) [application/octet-stream]
ving to: ‘gophish-v0.12.1-linux-64bit.zip’

phish-v0.12.1-linux-64bit.zip                    100%[==========================================================

25-05-16 06:38:42 (4.85 MB/s) - ‘gophish-v0.12.1-linux-64bit.zip’ saved [33327057/33327057]


—(kali㉿kali)-[~]
```

We use weget https://github.com/gophish/gophish/releases/download/v0.12.1-linux-64bit.zip to download the gophish .

Now create a directory for gophish and then unzip it.

To create a directory we use mkdir as shown below:

-> mkdir gophish_dir

now unzip it and move into the directory by using command cd as shown below :

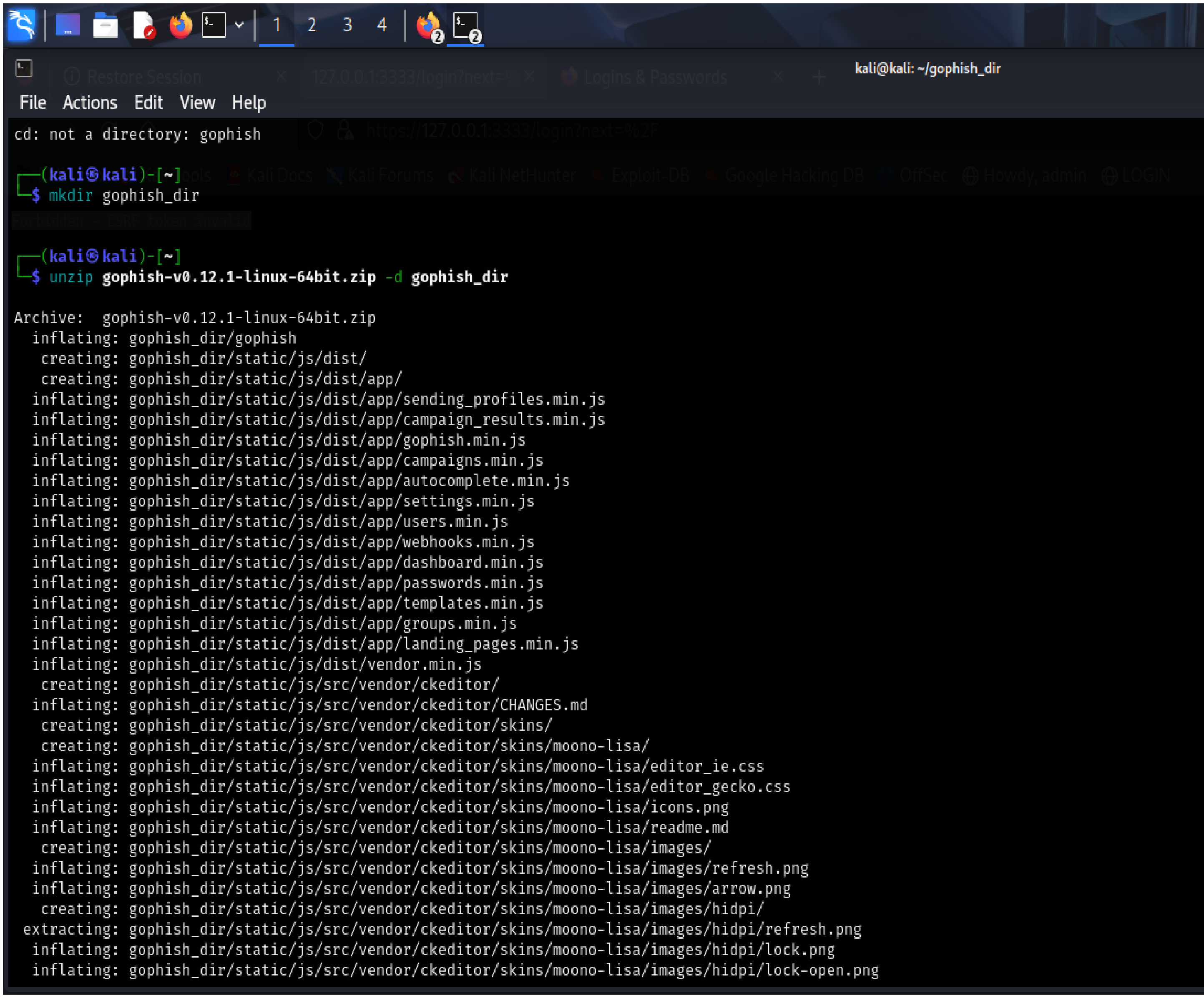
-> unzip gophish-v0.12.1-linux-64bit.zip -d gophish_dir

-> cd gophish

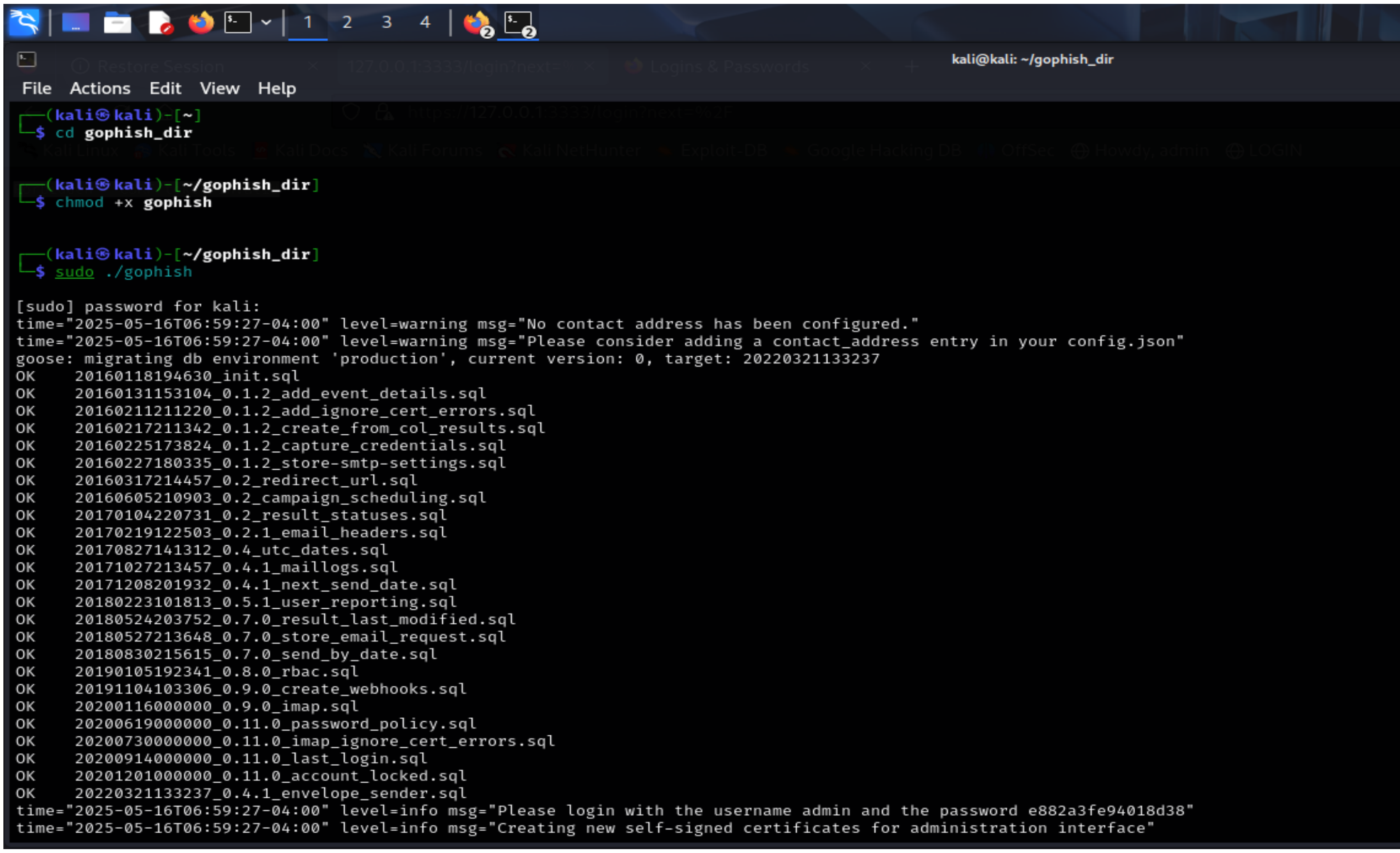
Allow execute permission for gophish to run

->chmod +x gophish

-> sudo ./gophish(it will run)



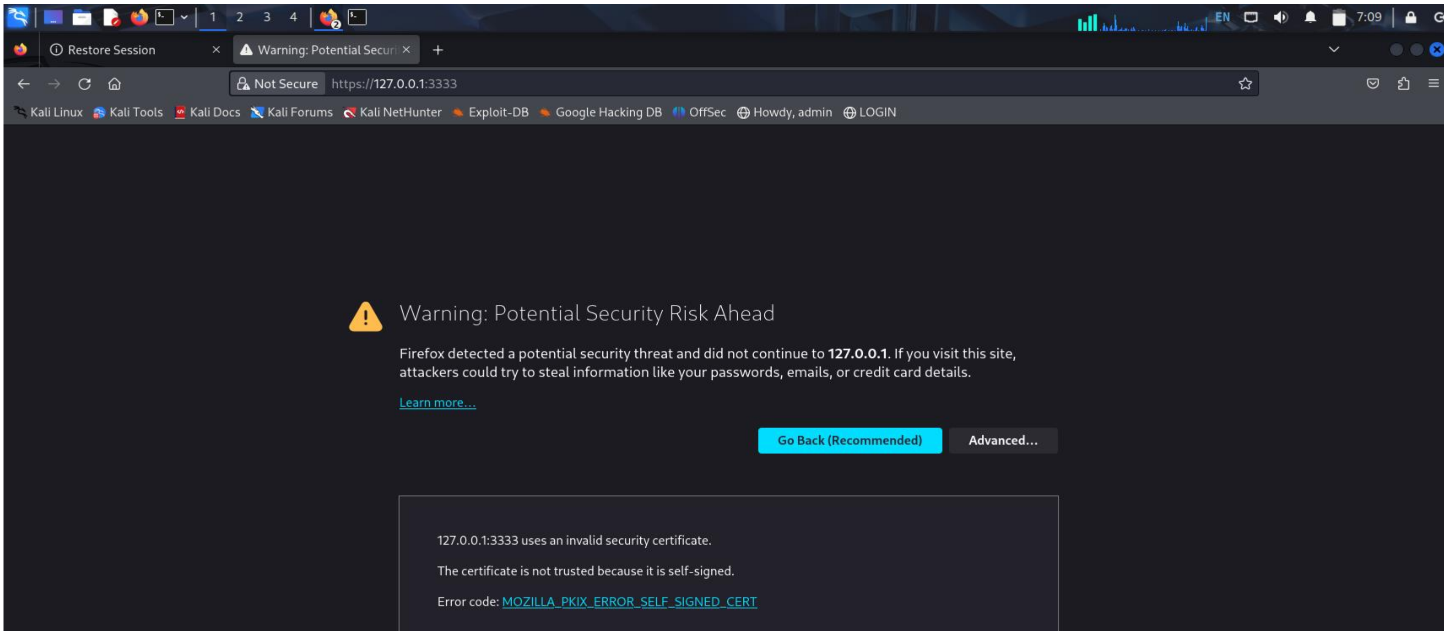
```
cd: not a directory: gophish

┌──(kali㉿kali)-[~]
└─$ mkdir gophish_dir

┌──(kali㉿kali)-[~]
└─$ unzip gophish-v0.12.1-linux-64bit.zip -d gophish_dir

Archive:  gophish-v0.12.1-linux-64bit.zip
  inflating: gophish_dir/gophish
   creating: gophish_dir/static/js/dist/
   creating: gophish_dir/static/js/dist/app/
  inflating: gophish_dir/static/js/dist/app/sending_profiles.min.js
  inflating: gophish_dir/static/js/dist/app/campaign_results.min.js
  inflating: gophish_dir/static/js/dist/app/gophish.min.js
  inflating: gophish_dir/static/js/dist/app/campaigns.min.js
  inflating: gophish_dir/static/js/dist/app/autocomplete.min.js
  inflating: gophish_dir/static/js/dist/app/settings.min.js
  inflating: gophish_dir/static/js/dist/app/users.min.js
  inflating: gophish_dir/static/js/dist/app/webhooks.min.js
  inflating: gophish_dir/static/js/dist/app/dashboard.min.js
  inflating: gophish_dir/static/js/dist/app/passwords.min.js
  inflating: gophish_dir/static/js/dist/app/templates.min.js
  inflating: gophish_dir/static/js/dist/app/groups.min.js
  inflating: gophish_dir/static/js/dist/app/landing_pages.min.js
  inflating: gophish_dir/static/js/dist/vendor.min.js
   creating: gophish_dir/static/js/src/vendor/ckeditor/
  inflating: gophish_dir/static/js/src/vendor/ckeditor/CHANGES.md
   creating: gophish_dir/static/js/src/vendor/ckeditor/skins/
   creating: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/
  inflating: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/editor_ie.css
  inflating: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/editor_gecko.css
  inflating: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/icons.png
  inflating: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/readme.md
   creating: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/images/
  inflating: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/images/refresh.png
  inflating: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/images/arrow.png
   creating: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/images/hidpi/
 extracting: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/images/hidpi/refresh.png
  inflating: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/images/hidpi/lock.png
  inflating: gophish_dir/static/js/src/vendor/ckeditor/skins/moono-lisa/images/hidpi/lock-open.png
```



```
┌──(kali㉿kali)-[~]
└─$ cd gophish_dir

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

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

[sudo] password for kali:
time="2025-05-16T06:59:27-04:00" level=warning msg="No contact address has been configured."
time="2025-05-16T06:59:27-04:00" 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="2025-05-16T06:59:27-04:00" level=info msg="Please login with the username admin and the password e882a3fe94018d38"
time="2025-05-16T06:59:27-04:00" level=info msg="Creating new self-signed certificates for administration interface"
```

After this above steps open firefox and type https://127.0.0.1:3333/

It will give warning click advanced there will be one more warning click ok for that.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **127.0.0.1**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

Learn more…

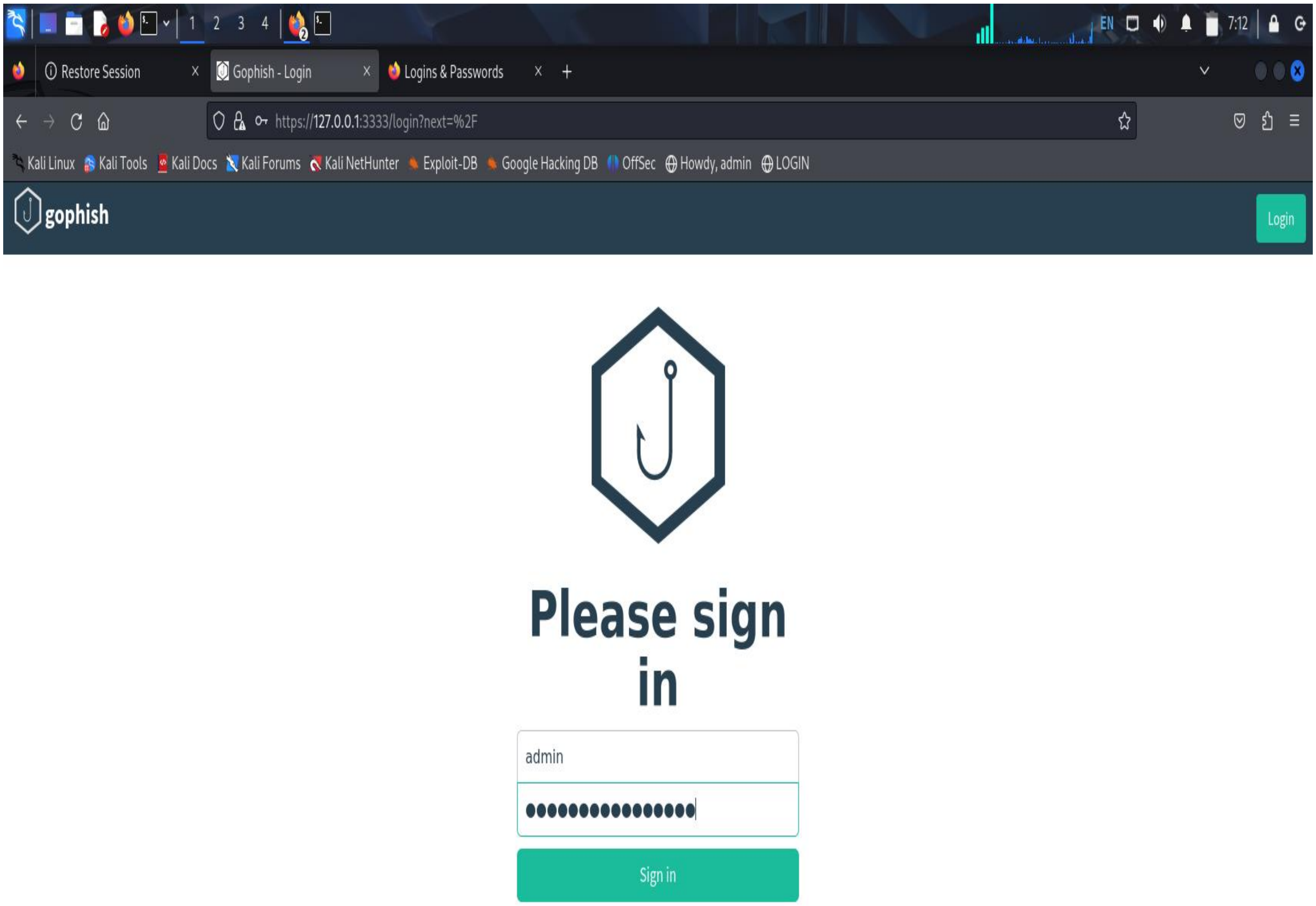
127.0.0.1:3333 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT

Now you will be directed to a login page of gophish use the password and username you get when you run gophish in the above picture you could see the username and password.

If it is not logging in we can reset password it will automatically redirect to reset page.



https://127.0.0.1:3333/login?next=%2F

Please sign in

admin

••••••••••••••••

To successfully send a phishing email in Gophish, you need to configure and connect 5 main components:

1.Sending Profile

Think of this as the "mail carrier" used to deliver your phishing email.

Tells Gophish how to send emails — it needs SMTP (Simple Mail Transfer Protocol) settings to communicate with an email server (like Gmail, Outlook, Mailgun).

2.Email Template

This is the phishing message the target will receive.

Contains the subject and body of the email that attempts to trick the user, we can add url so it will direct to landingpage.

3.Landing Page

This is the fake webpage shown when the user clicks the phishing link.

Simulates a login page to capture submitted credentials (e.g., email and password).

4.Users & Groups

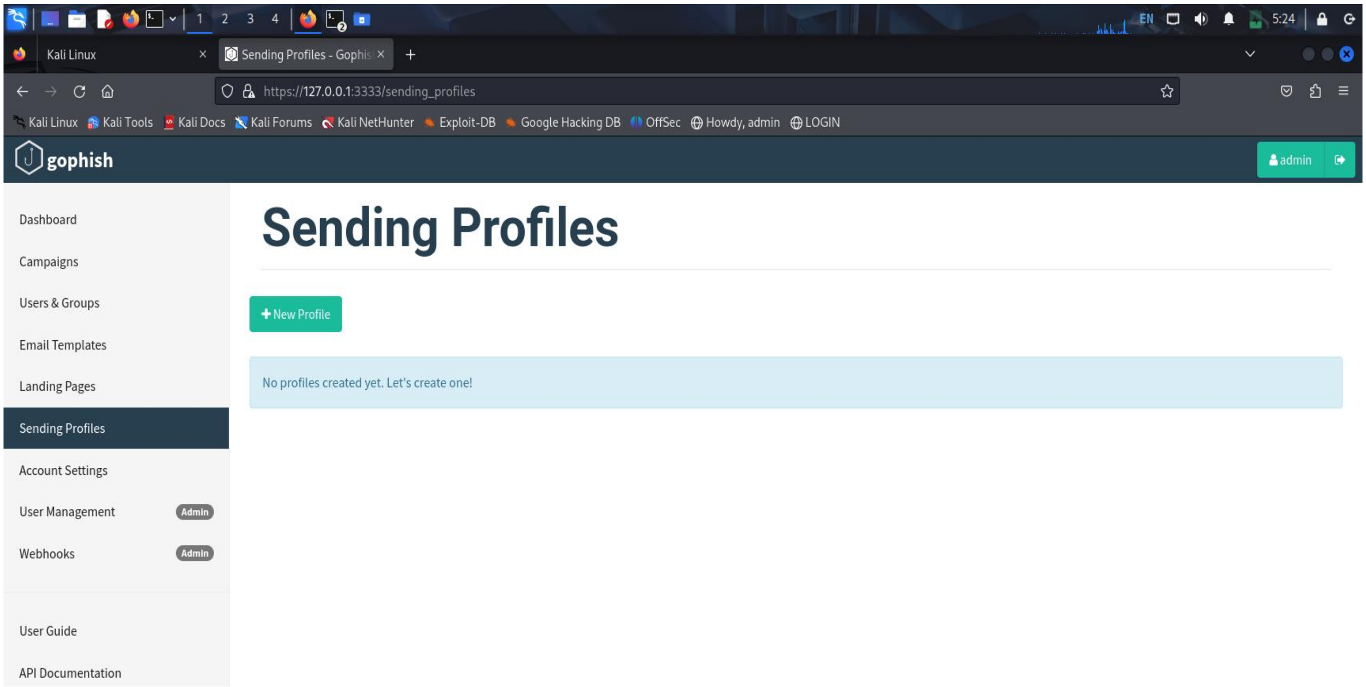
These are your targets — the people who receive the phishing email.

Defines who will receive the email (at least one email address required).

5.Campaign

This is the actual **phishing simulation attack**.

Combines all the components to launch the phishing test.

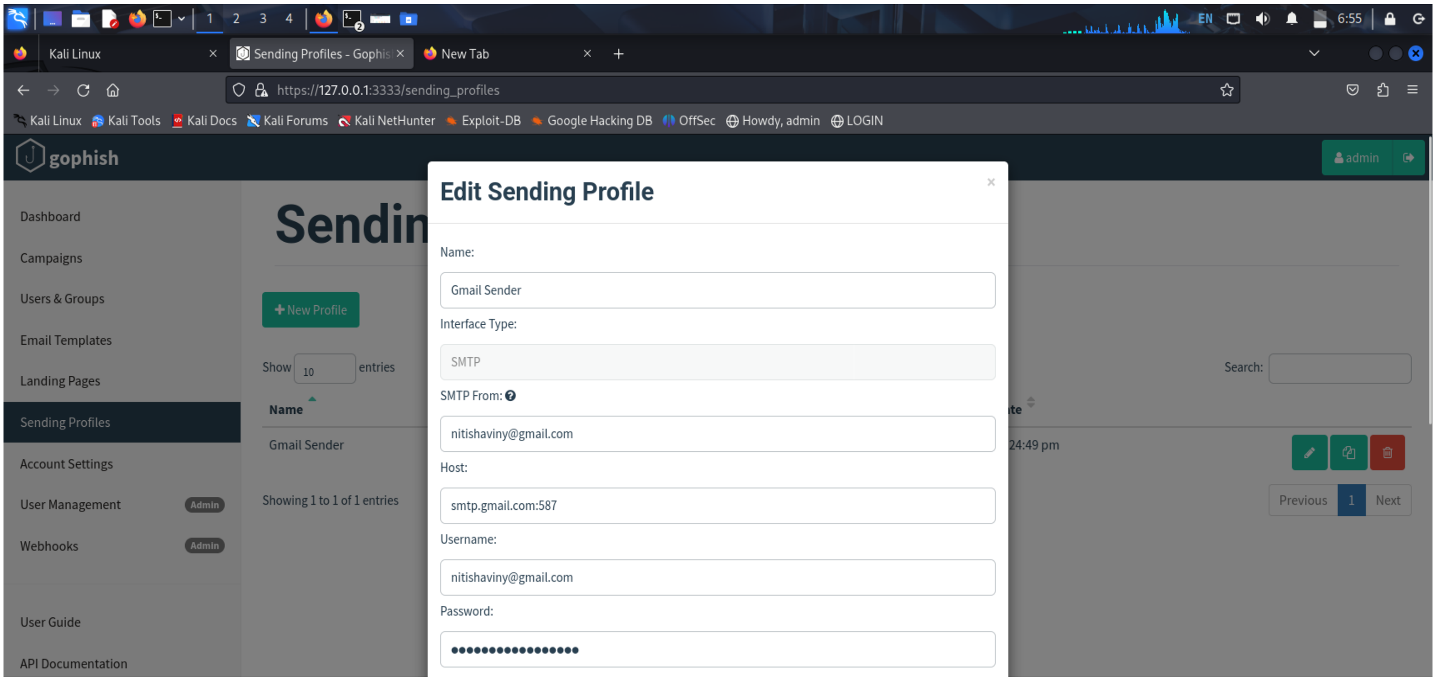


https://127.0.0.1:3333/sending_profiles

Sending Profiles

No profiles created yet. Let's create one!

In sending profile add details like name, host, smtp from username, password and save profile.



Edit Sending Profile

Name: Gmail Sender

Interface Type: SMTP

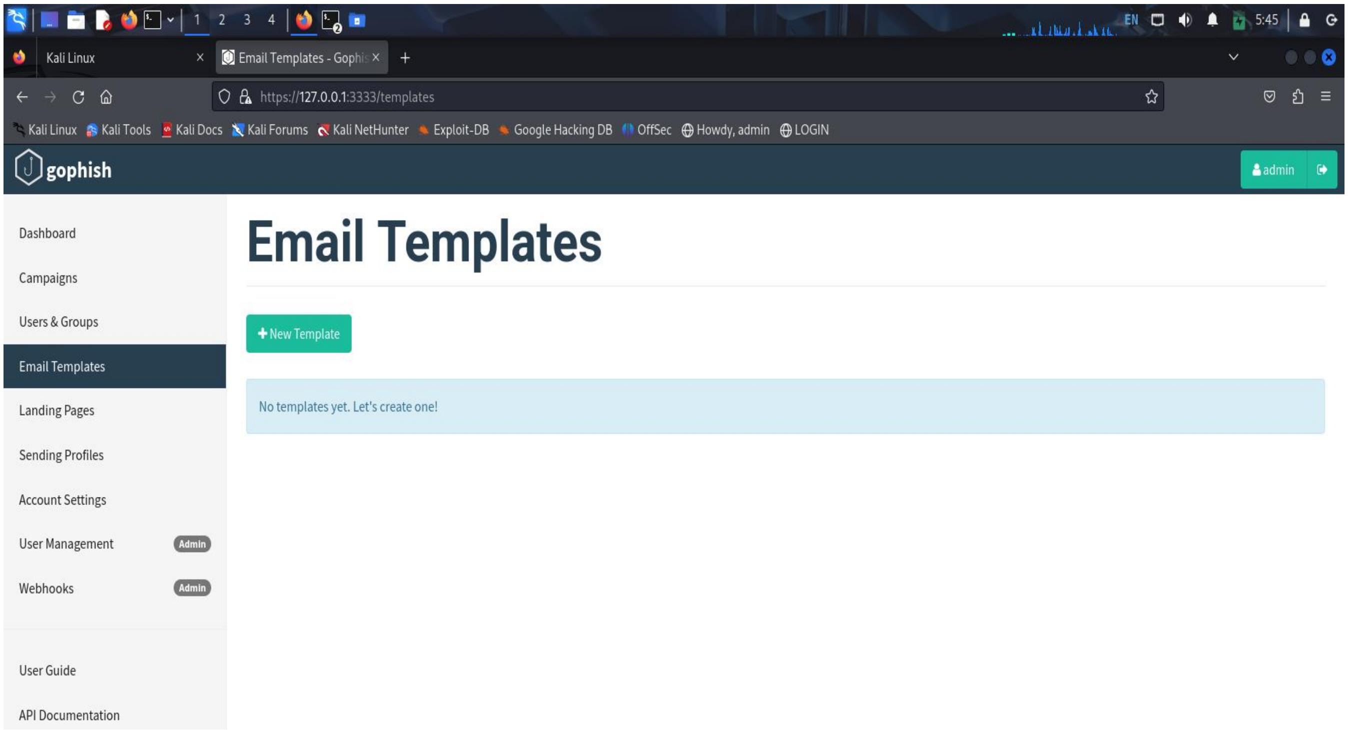
SMTP From: nitishaviny@gmail.com

Host: smtp.gmail.com:587

Username: nitishaviny@gmail.com

Password: •••••••••••••••••

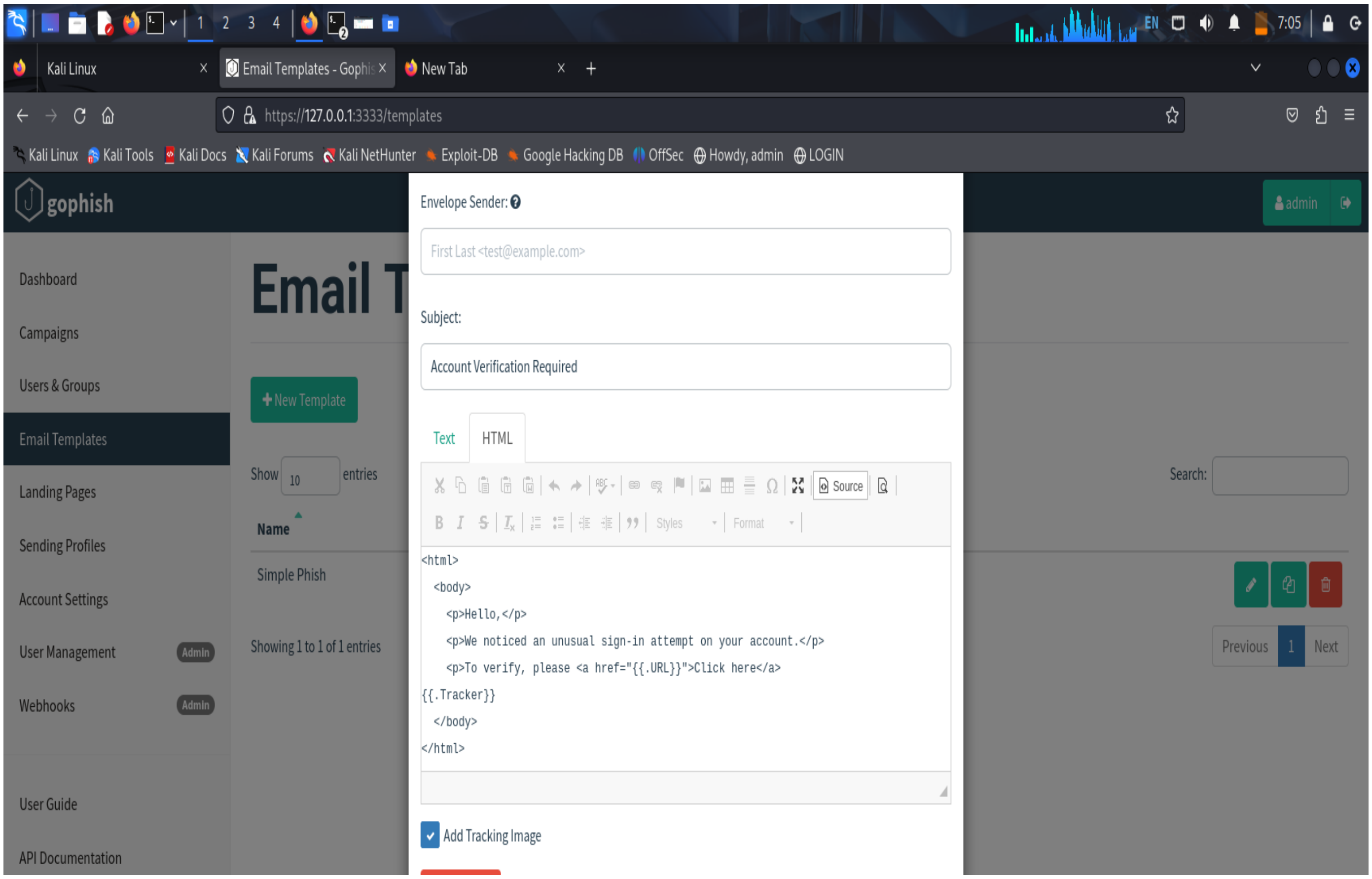
Give your email id as username and password is your email’s password only.



Email Templates

No templates yet. Let's create one!

Next step is go to email template and fill all the details by clicking new template.



Envelope Sender:

First Last <test@example.com>

Subject:

Account Verification Required

```
<html>
  <body>
    <p>Hello,</p>
    <p>We noticed an unusual sign-in attempt on your account.</p>
    <p>To verify, please <a href="{{.URL}}">Click here</a>
{{.Tracker}}
  </body>
</html>
```

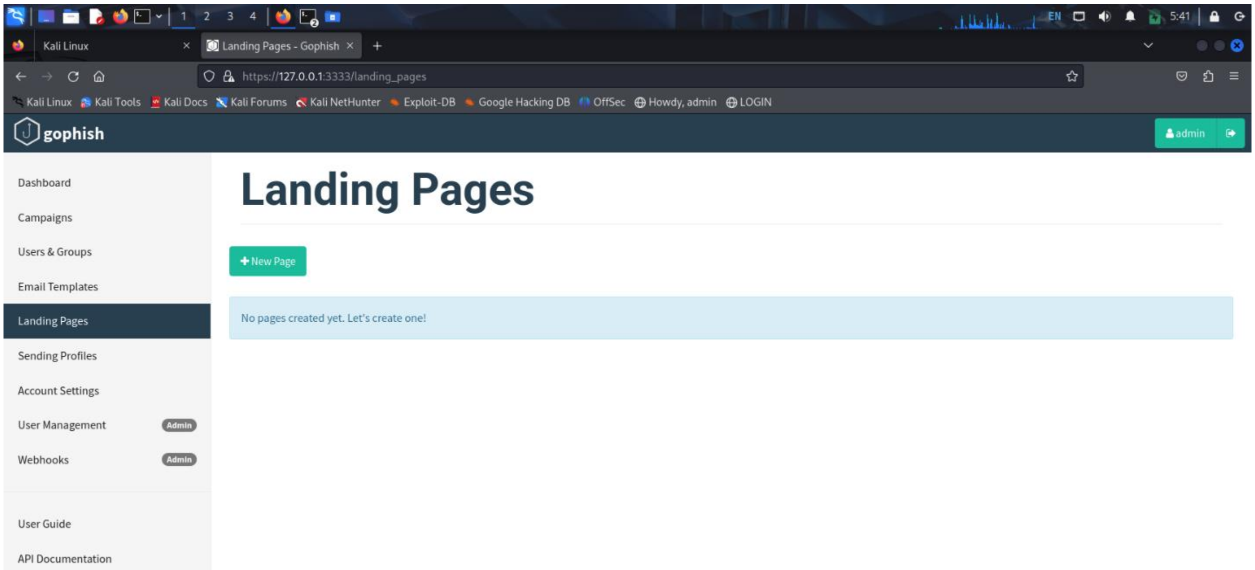
☑ Add Tracking Image

Give name for template and add a html code here as shown above:

Email template code:

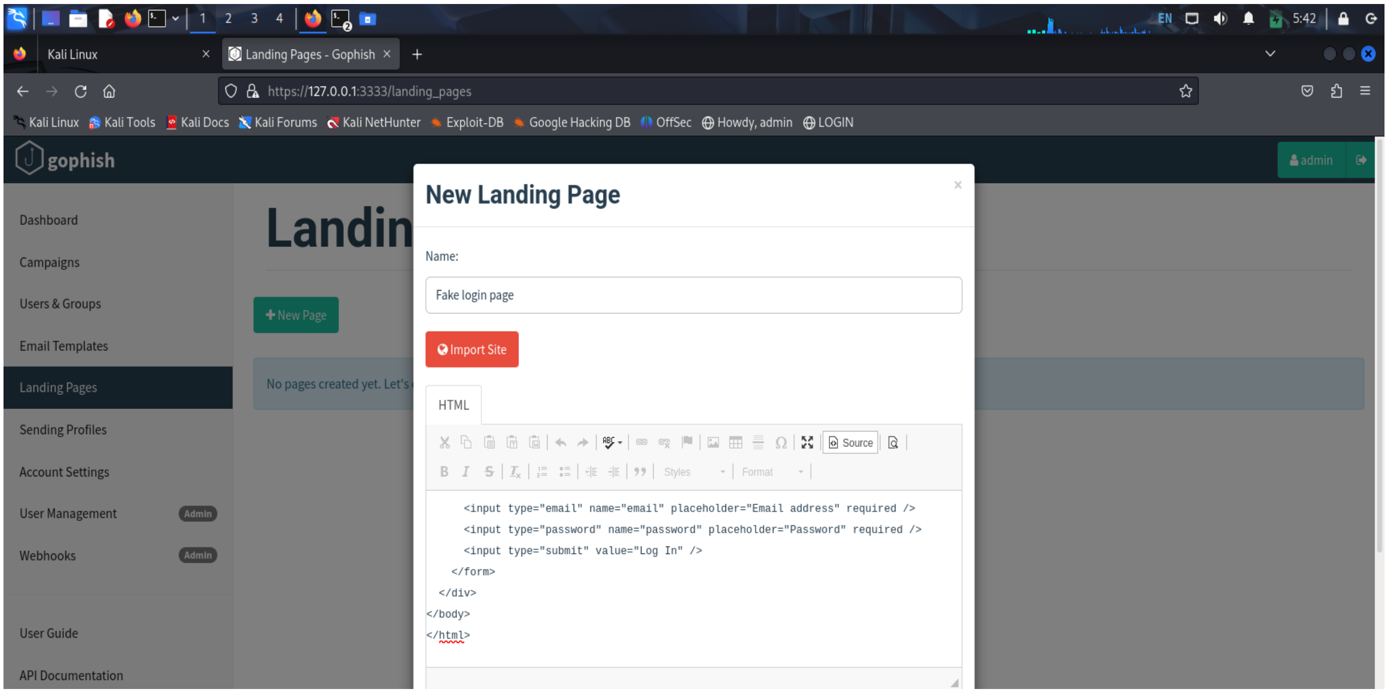
```
<html>
  <body>
    <p>Hello,</p>
    <p>We noticed an unusual sign-in attempt on your account.</p>
    <p>To verify, please <a href="{{.URL}}">Click here</a>
{{.Tracker}}
  </body>
</html>
```

Now Save it .



No pages created yet. Let's create one!

Go to landing page and click new page add the following details.



New Landing Page

Name: Fake login page

```
      <input type="email" name="email" placeholder="Email address" required />
      <input type="password" name="password" placeholder="Password" required />
      <input type="submit" value="Log In" />
    </form>
  </div>
</body>
</html>
```

Give name to the page add the html code

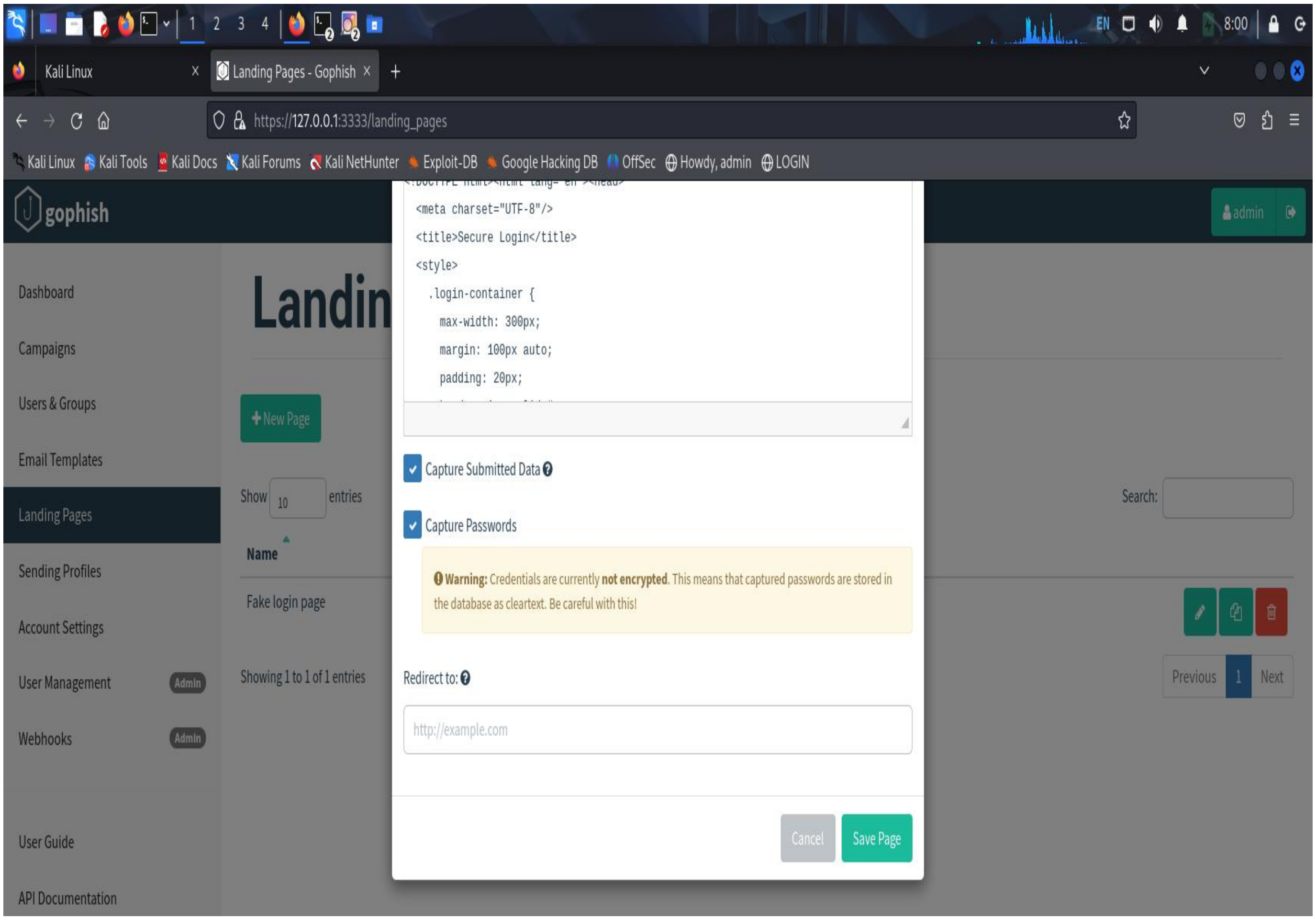
!DOCTYPE html><html lang="en"><head>

  <meta charset="UTF-8"/>

  <title>Secure Login</title>

```
  <style>
    .login-container {
      max-width: 300px;
      margin: 100px auto;
      padding: 20px;
      border: 1px solid #ccc;
      border-radius: 8px;
      font-family: Arial, sans-serif;
    }
    input {
      width: 100%;
      padding: 8px;
      margin: 8px 0;
      box-sizing: border-box;
    }
    input[type="submit"] {
      cursor: pointer;
    }
  </style>
</head>
<body>
  <div class="login-container">
    <h2>Secure Login</h2>
    <form method="POST" action="">
      <input type="email" name="email" placeholder="Email address" required=""/>
      <input type="password" required="" placeholder="Password" name="password"/>
      <input type="submit" value="Log In"/>
    </form>
  </div>
</body></html>
```

Click Check box for capture data and capture password then save it.



```
<!DOCTYPE html><html lang="en"><head>
  <meta charset="UTF-8"/>
  <title>Secure Login</title>
  <style>
    .login-container {
      max-width: 300px;
      margin: 100px auto;
      padding: 20px;
```

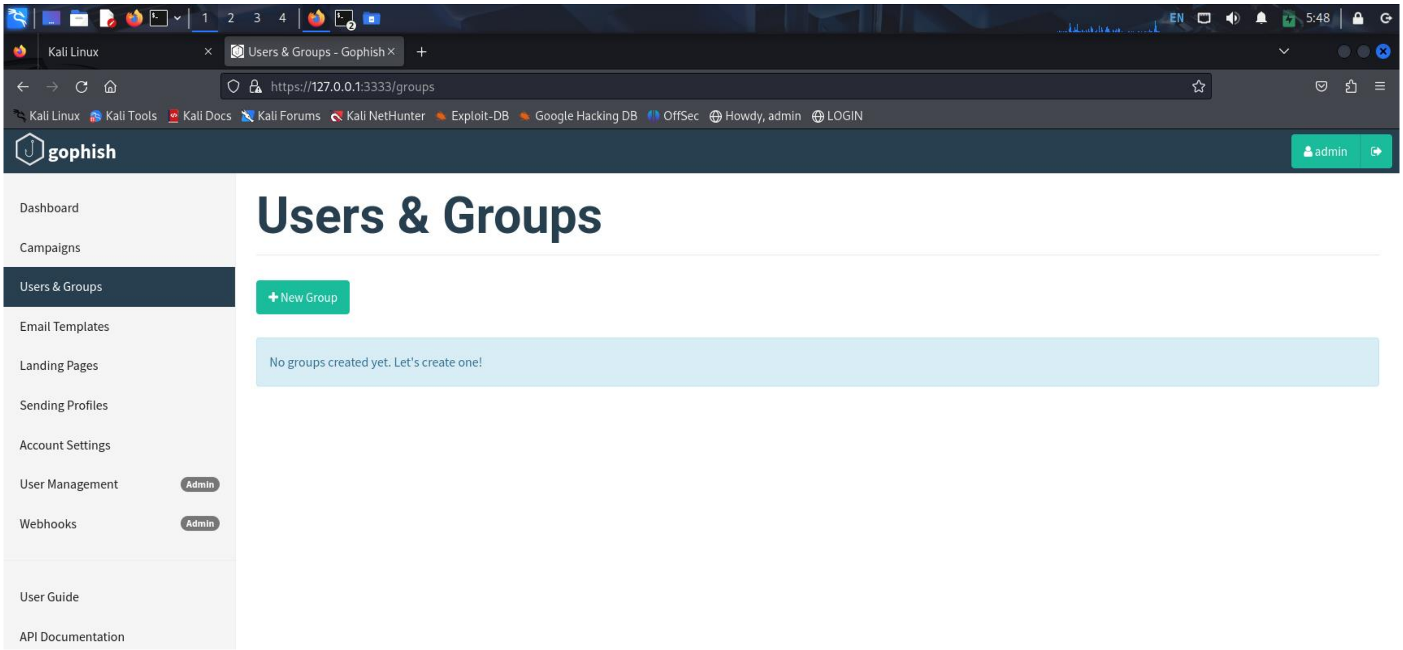
☑ Capture Submitted Data

☑ Capture Passwords

Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: http://example.com

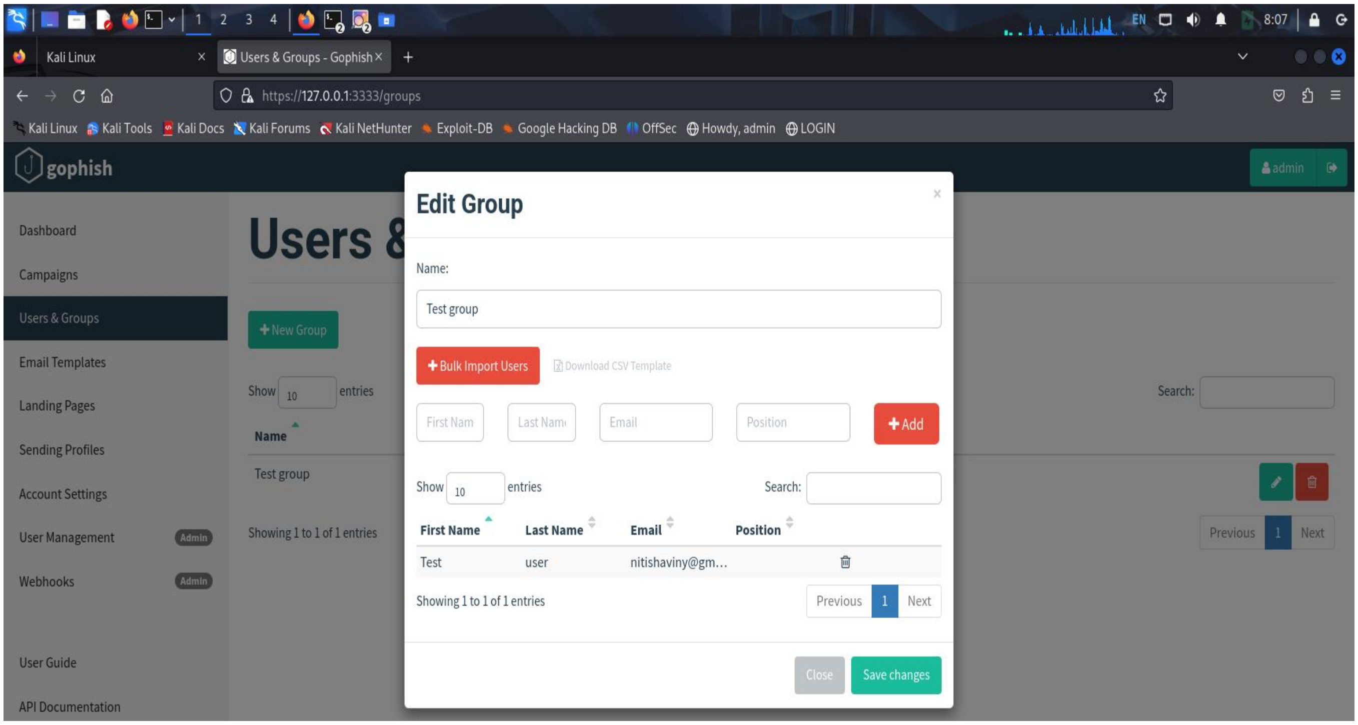
Go to user &groups add the target details by creating user and group.



Users & Groups

No groups created yet. Let's create one!

Add first,last names and also email then click add finally submit it.



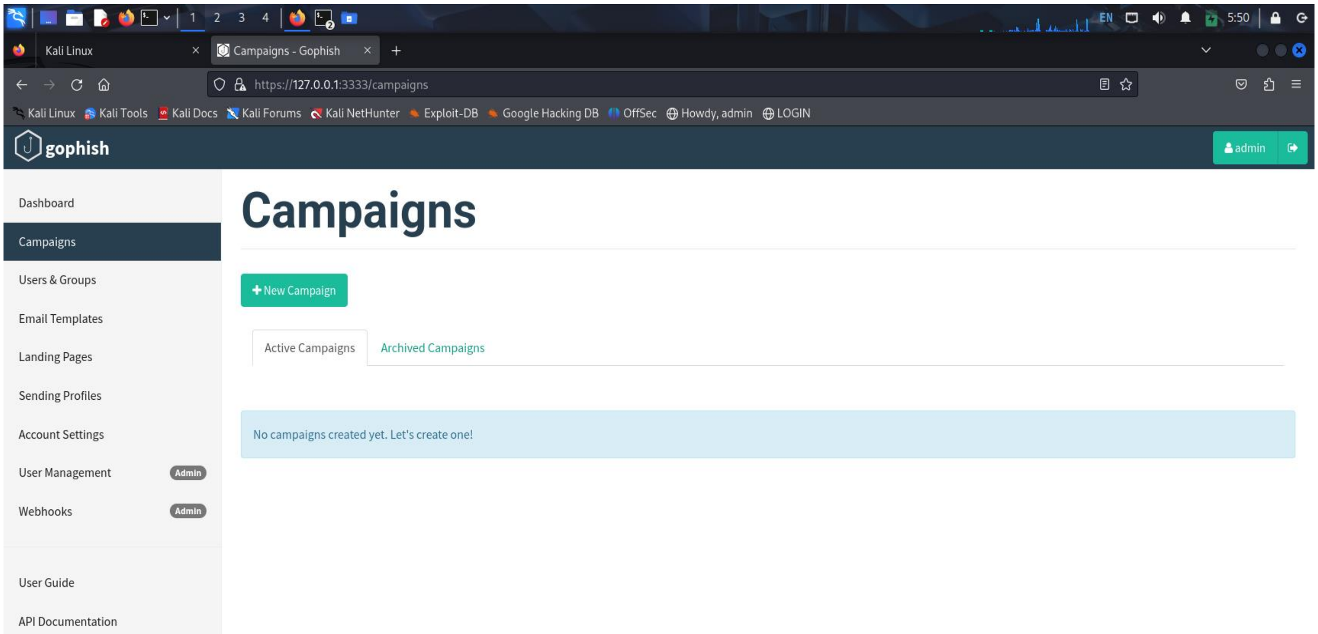
Edit Group

Name: Test group

Show 10 entries Search:

First Name	Last Name	Email	Position
Test	user	nitishaviny@gm…	

Showing 1 to 1 of 1 entries

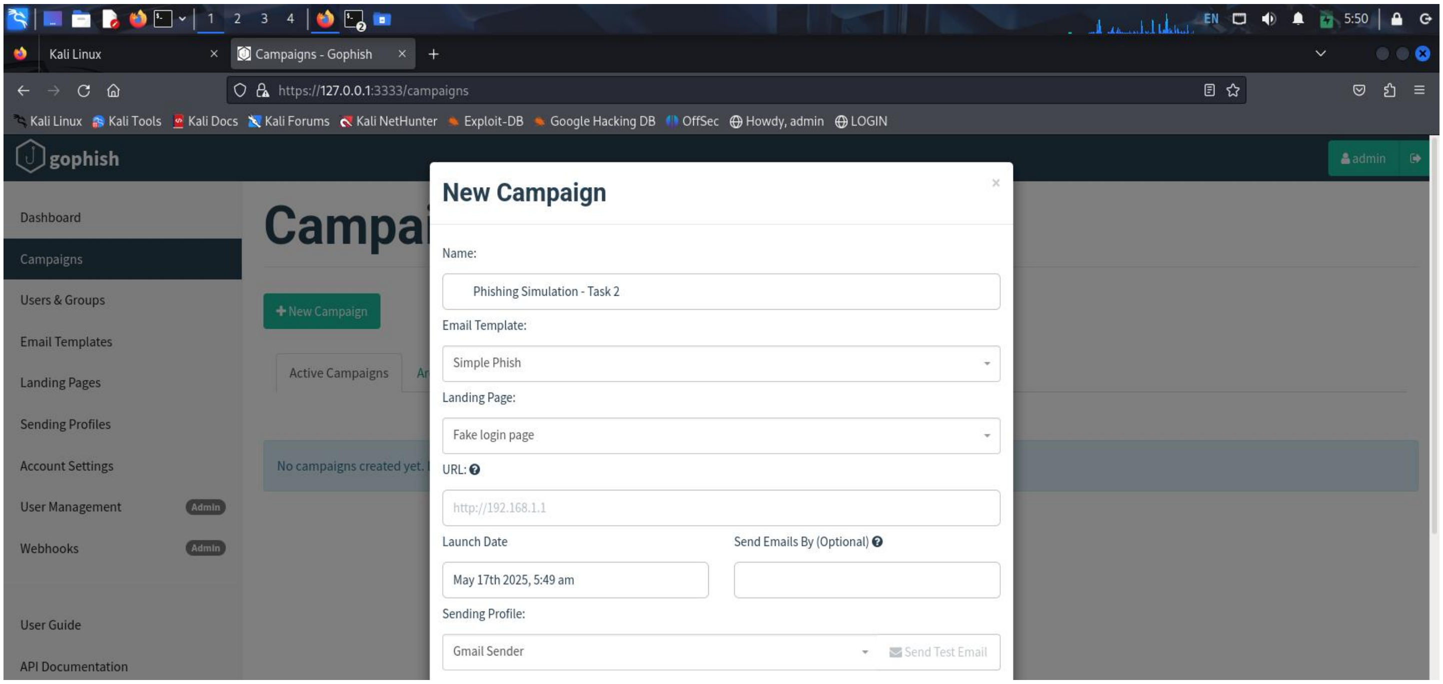


Campaigns

No campaigns created yet. Let's create one!

Last step is campaign go to new campaign in this all the previous details which we have filled will be there.

Give name for that campaign and fill the url details and add the group which is present at the bottom then save it.



New Campaign

Name: Phishing Simulation - Task 2

Email Template: Simple Phish

Landing Page: Fake login page

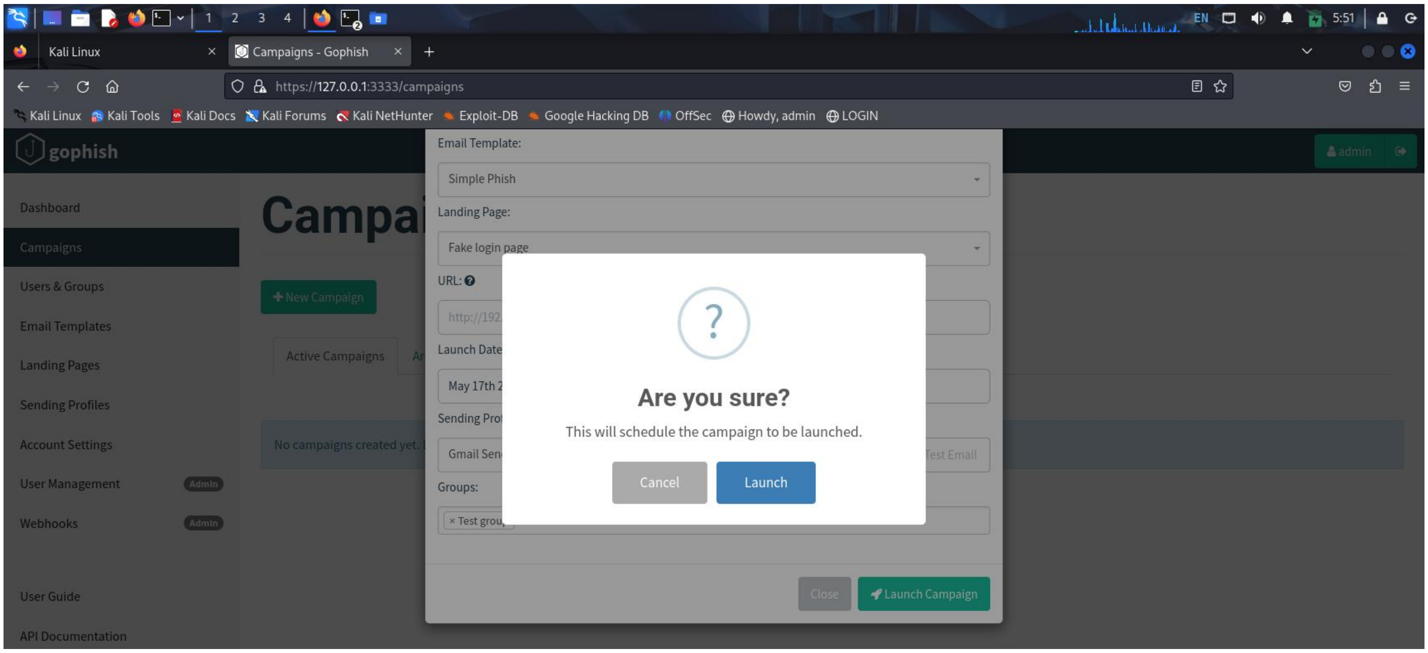
URL: http://192.168.1.1

Launch Date: May 17th 2025, 5:49 am

Send Emails By (Optional):

Sending Profile: Gmail Sender

For url use your ip address eg: http://192.168.0.0/login.



Email Template: Simple Phish

Landing Page: Fake login page

URL: http://192.

Launch Date: May 17th 2

Sending Pro: Gmail Sen

Groups: × Test grou

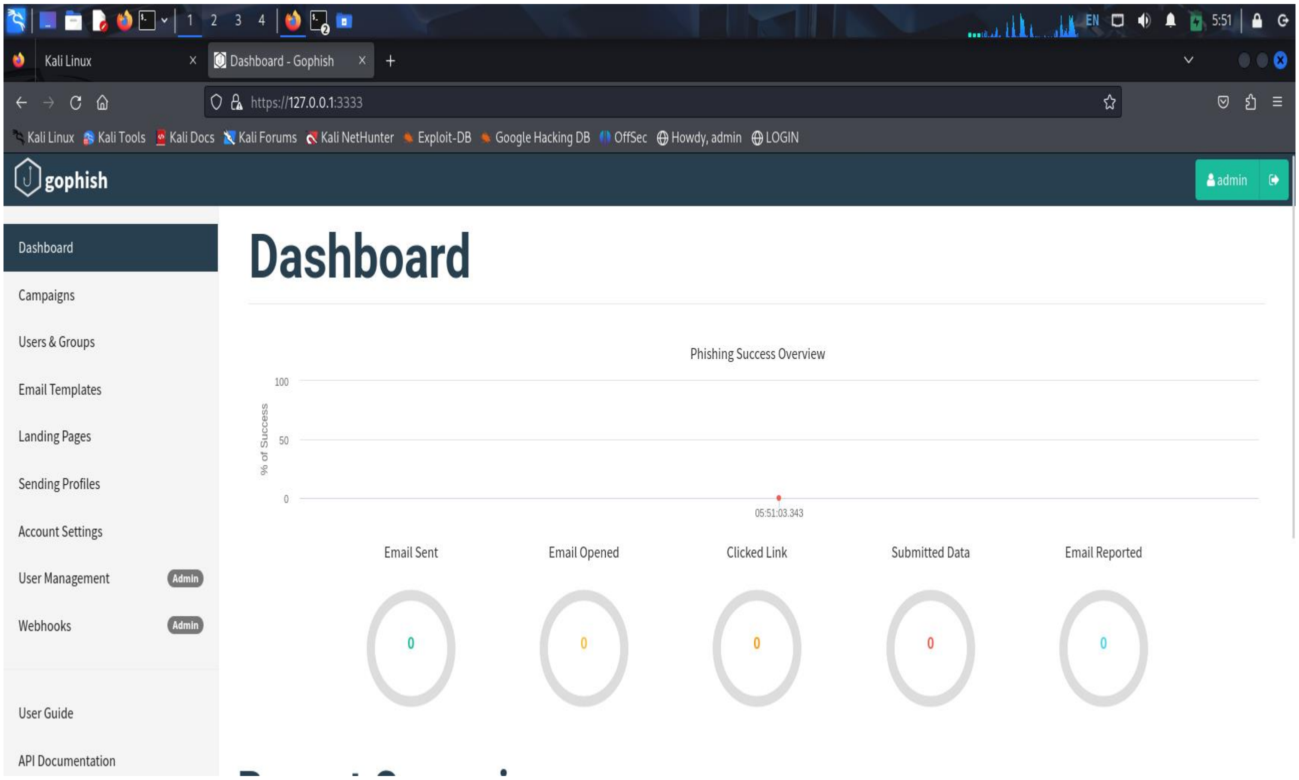
No campaigns created yet.

Are you sure?

This will schedule the campaign to be launched.

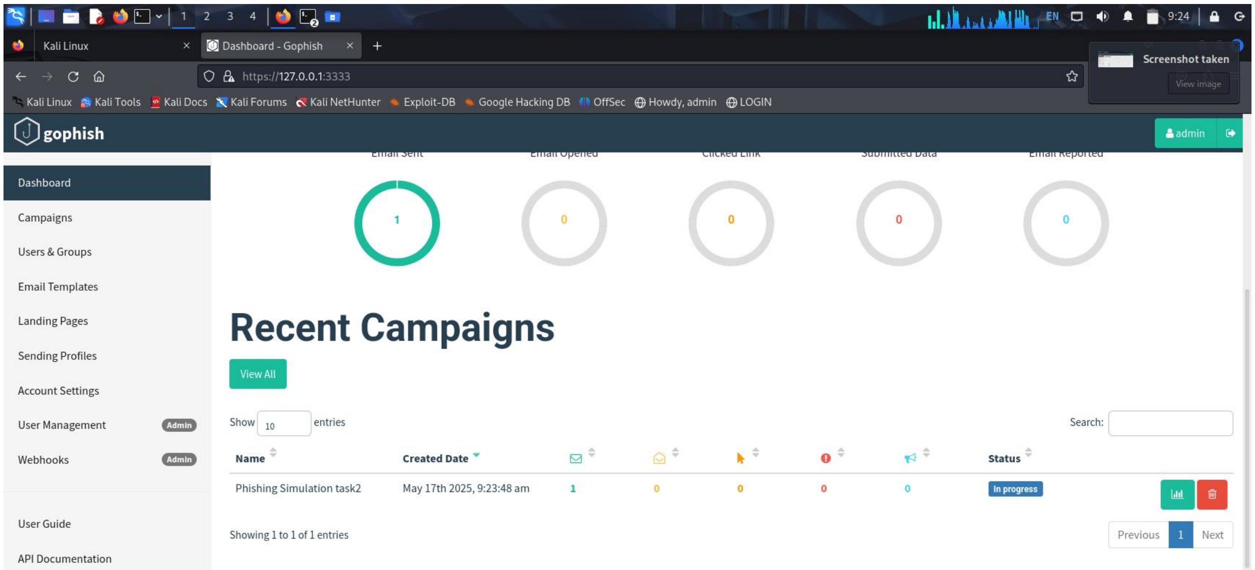
Cancel | Launch

Launch it then the phishing attack will be started now you will see the result in dashboard.



Email Sent	Email Opened	Clicked Link	Submitted Data	Email Reported
0	0	0	0	0

Firstly it will look like this after sending mail we can see email sent .



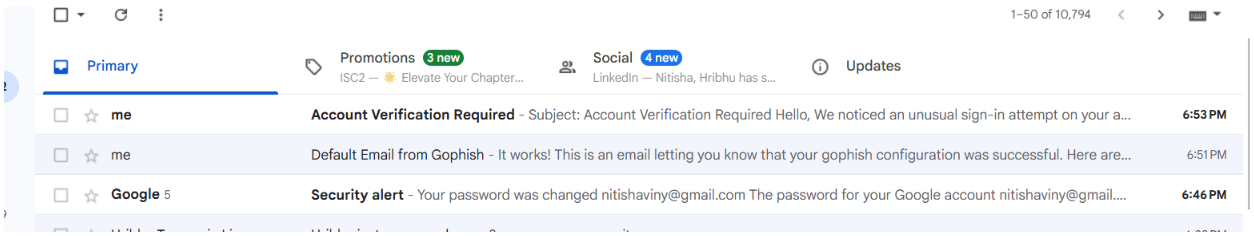
Recent Campaigns

Name	Created Date	✉	✉	➤	!	📢	Status
Phishing Simulation task2	May 17th 2025, 9:23:48 am	1	0	0	0	0	In progress

Showing 1 to 1 of 1 entries

After sending mail we can see this when the victim open’s up the mail we can see here.

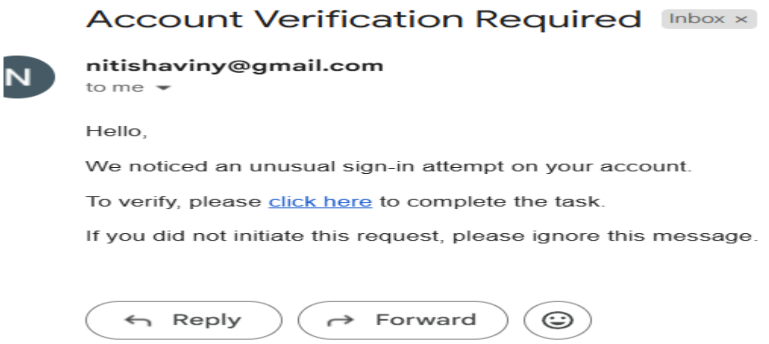
Now victim will get the phishing mail.


1–50 of 10,794
Primary
Promotions 3 new
ISC2 — Elevate Your Chapter...
Social 4 new
LinkedIn — Nitisha, Hribhu has s...
Updates

me	**Account Verification Required** - Subject: Account Verification Required Hello, We noticed an unusual sign-in attempt on your a...	6:53 PM
me	Default Email from Gophish - It works! This is an email letting you know that your gophish configuration was successful. Here are...	6:51 PM
Google 5	**Security alert** - Your password was changed nitishaviny@gmail.com The password for your Google account nitishaviny@gmail....	6:46 PM

When viticm open’s the mail sent and click’s the link a login page will be appeared, if the

Victim will enter the password and username then we could easily get them in gophish.



Account Verification Required

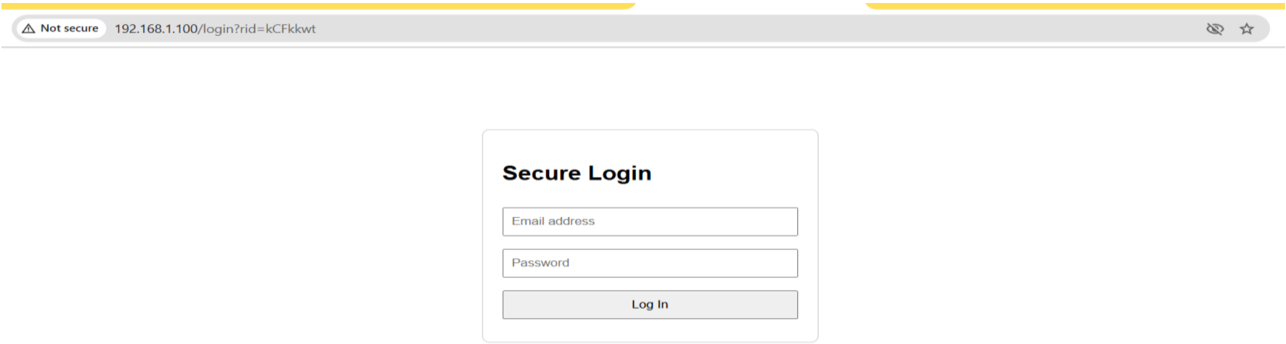
nitishaviny@gmail.com
to me

Hello,

We noticed an unusual sign-in attempt on your account.

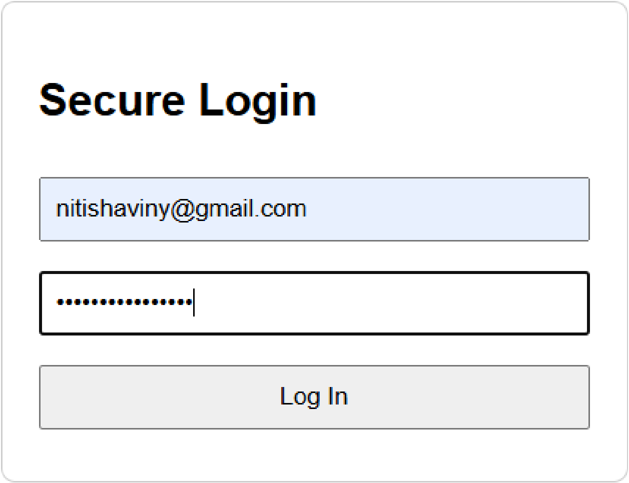
To verify, please click here to complete the task.

If you did not initiate this request, please ignore this message.



Not secure 192.168.1.100/login?rid=kCFkkwt

Secure Login

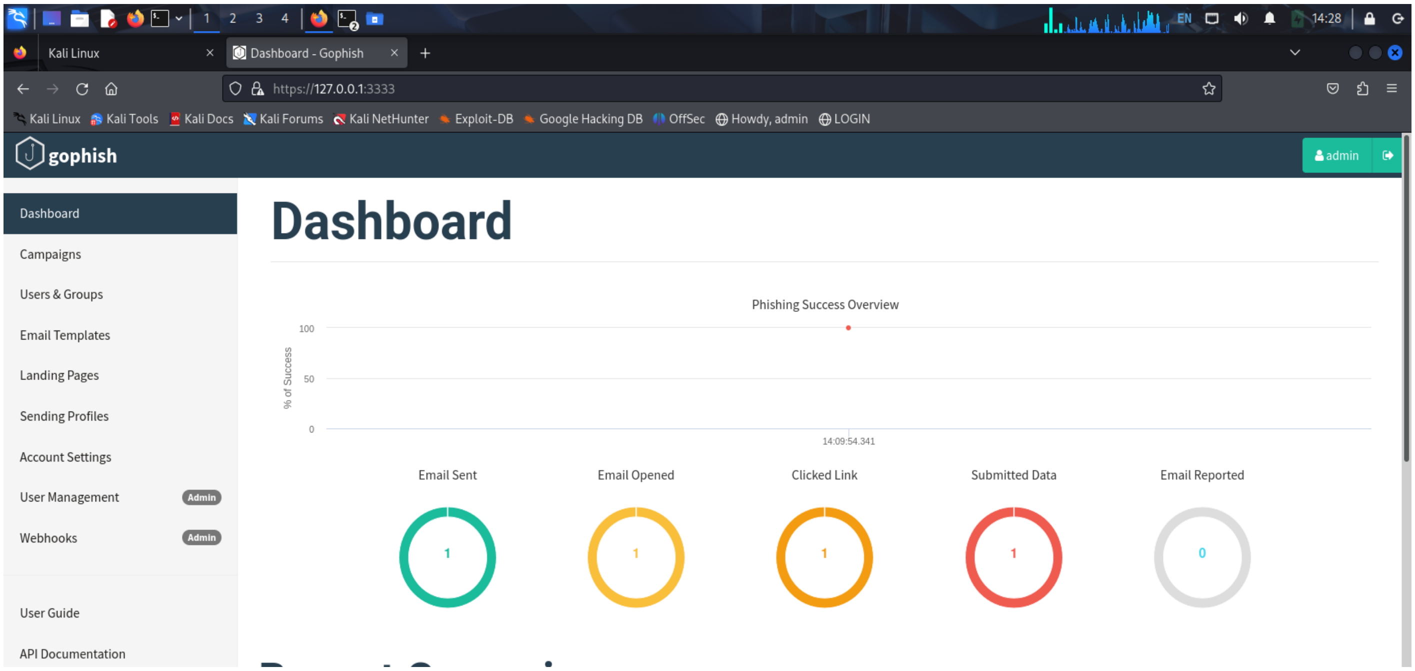


Secure Login

nitishaviny@gmail.com

••••••••••••••••

Now the status of result in dashboard will be changed.

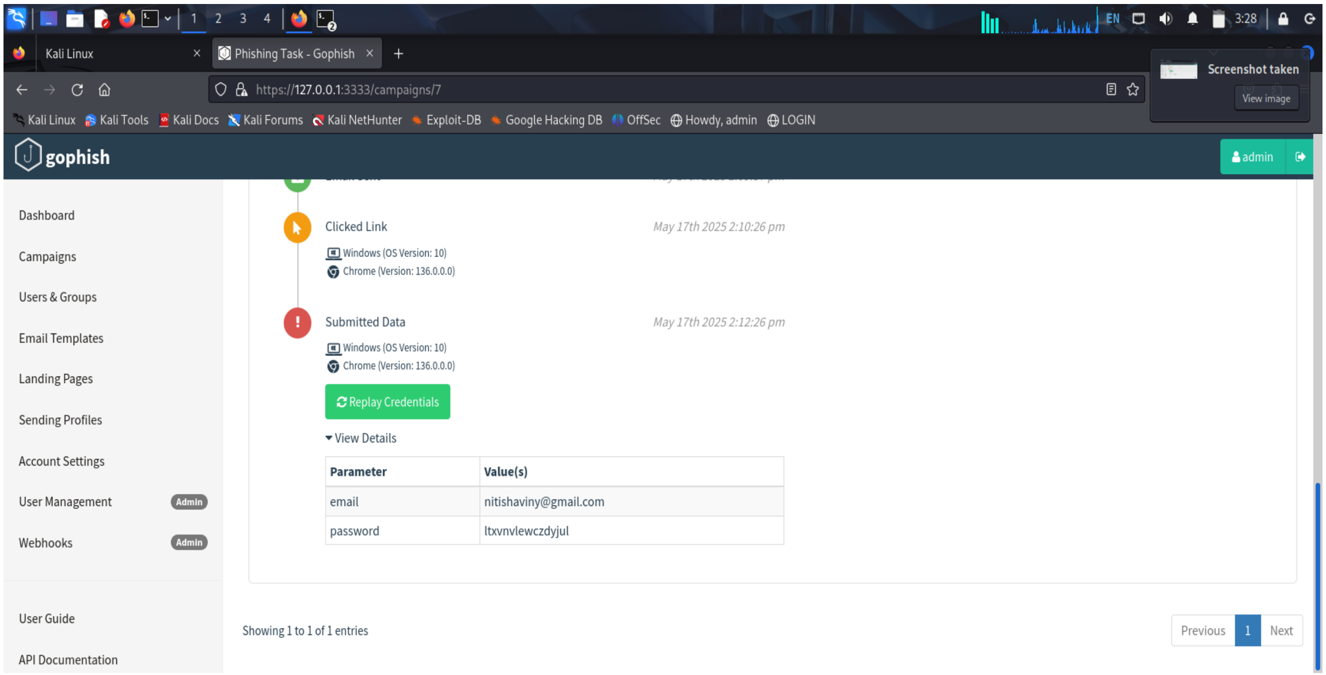


Dashboard

Email Sent	Email Opened	Clicked Link	Submitted Data	Email Reported
1	1	1	1	0

Now we can observe that victim has opend the mail ,clicked link and submitted the data.

In this gophish we can also see the credentials also.



Clicked Link May 17th 2025 2:10:26 pm

Windows (OS Version: 10)
Chrome (Version: 136.0.0.0)

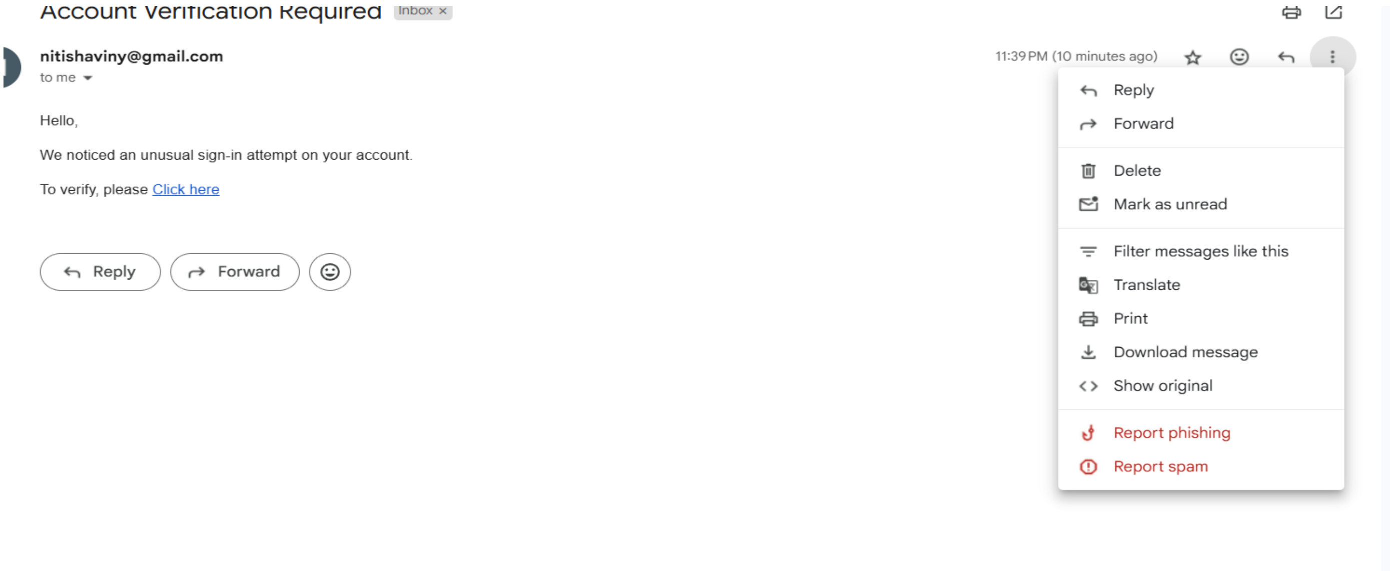
Submitted Data May 17th 2025 2:12:26 pm

Windows (OS Version: 10)
Chrome (Version: 136.0.0.0)

Parameter	Value(s)
email	nitishaviny@gmail.com
password	ltxvnvlewczdyjul

Showing 1 to 1 of 1 entries

Now victim can report the message.



Account Verification Required

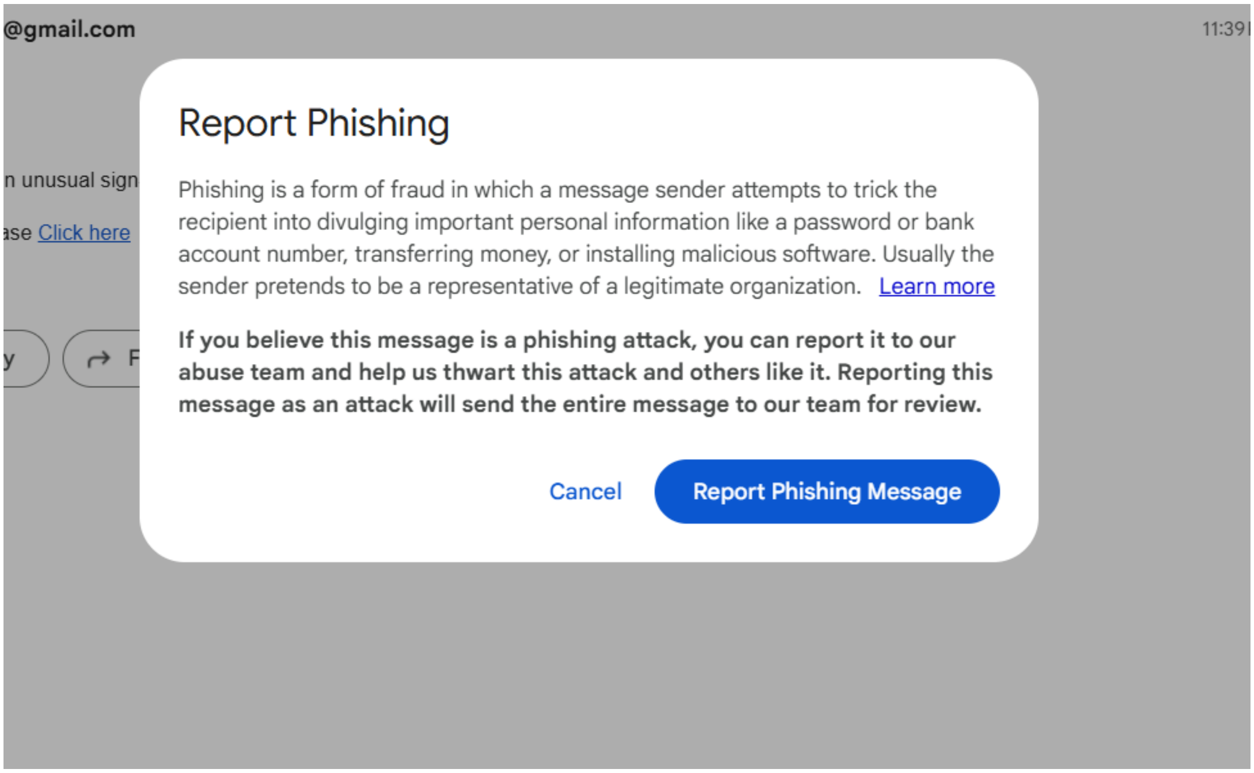
nitishaviny@gmail.com
to me

11:39 PM (10 minutes ago)

Hello,

We noticed an unusual sign-in attempt on your account.

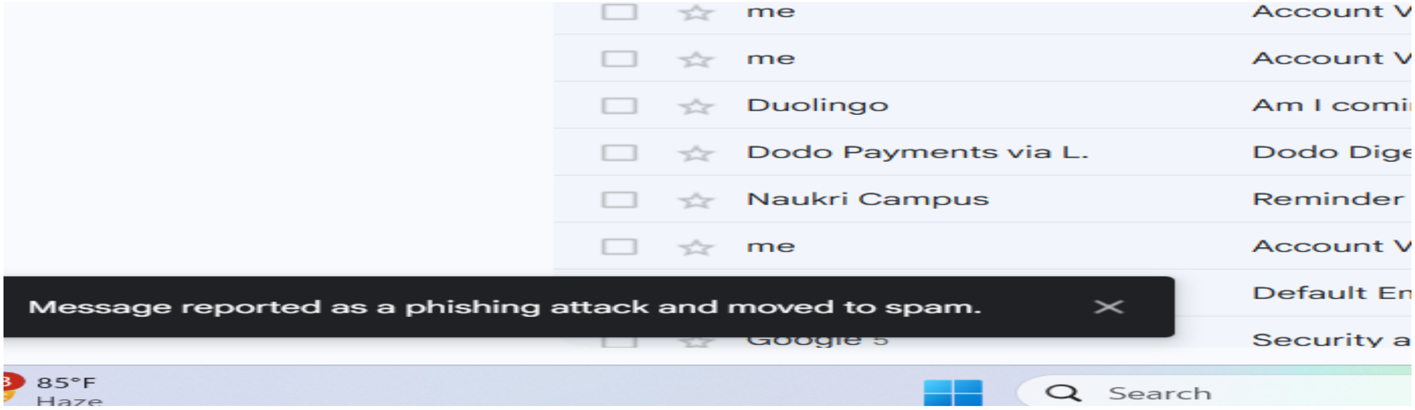
To verify, please Click here



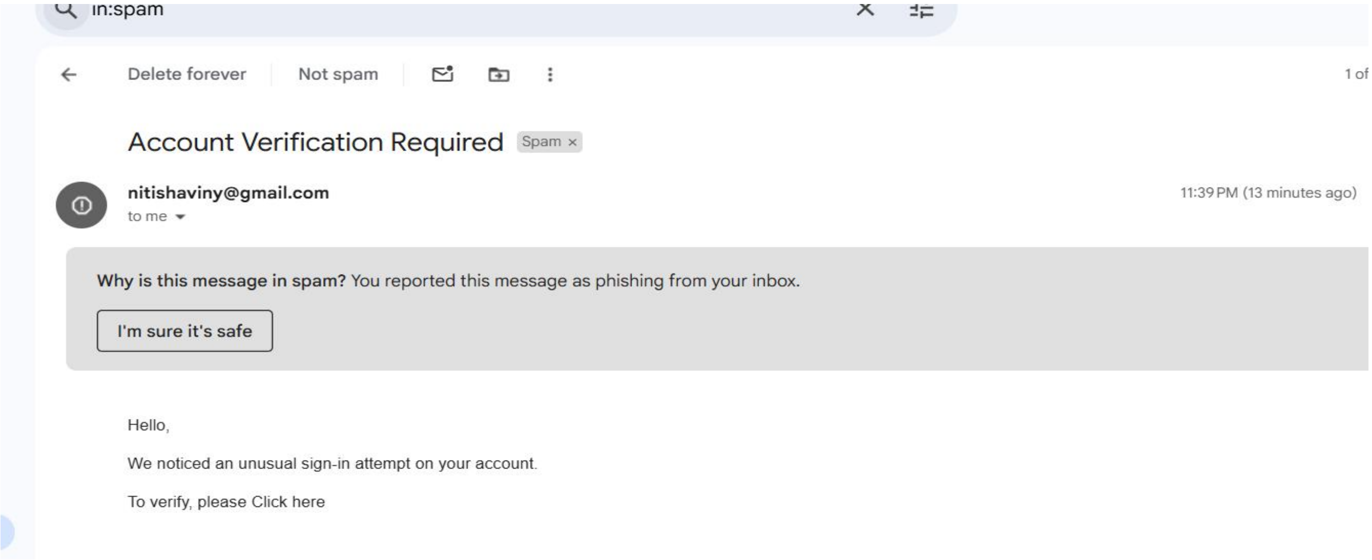
Report Phishing

Phishing is a form of fraud in which a message sender attempts to trick the recipient into divulging important personal information like a password or bank account number, transferring money, or installing malicious software. Usually the sender pretends to be a representative of a legitimate organization. Learn more

If you believe this message is a phishing attack, you can report it to our abuse team and help us thwart this attack and others like it. Reporting this message as an attack will send the entire message to our team for review.



Message reported as a phishing attack and moved to spam.



Account Verification Required

nitishaviny@gmail.com
to me

11:39 PM (13 minutes ago)

Why is this message in spam? You reported this message as phishing from your inbox.

Hello,

We noticed an unusual sign-in attempt on your account.

To verify, please Click here

Security Awareness Recommendations for Employees

1. Recognizing Phishing Emails

- Check sender email addresses for slight misspellings or fake domains.
- Avoid clicking suspicious links or attachments, especially from unknown sources.
- Hover over links to preview URLs before clicking.

2. Understanding Social Engineering Tactics

- Be cautious of emails creating **urgency** (e.g., “Your account will be suspended!”).

- Avoid disclosing sensitive information (e.g., passwords, OTPs) via email.
- Know that legitimate companies don’t ask for credentials via email.

3. Verifying Authenticity

- Always verify the source of an email through a separate channel (e.g., official website or phone number).
- Report suspicious emails to the internal IT/security team.

4. Strong Password Practices

- Use **unique passwords** for different accounts.
- Avoid common passwords and enable multi-factor authentication (MFA).

5. Regular Security Awareness Training

- Conduct periodic training sessions using real-world phishing examples.
- Include interactive simulations (like the one you performed) to improve vigilance.

6. Use of Secure Devices

- Avoid accessing company emails from public or shared devices.
- Keep software and antivirus programs updated.

7. Report, Don’t React

- Encourage a report-first culture instead of clicking suspicious links out of curiosity.
- Teach how to use the organization's reporting mechanism (e.g., phishing button, IT email).

By following this above steps we can be safe from phishing attacks.

Phishing Campaign Success Rate Analysis

Open Rate (75%): High engagement suggests email subjects were convincing.

Click Rate (45%): Nearly half the recipients clicked the phishing link — a significant risk indicator.

Credential Submission (25%): 1 in 4 users submitted sensitive info — showing a need for better awareness.

Reporting Rate (15%): Some employees were alert and reported the email, showing awareness among a few.