._.

GoPhish Phishing Simulation – Report

._.

Deansingh Ramphul

2/14/2025

.

Table of Contents

Introduction

a. Purpose of the project

Phishing is one of the most common and dangerous forms of cyberattacks. It involves the use of fraudulent emails or messages to trick individuals into revealing sensitive information such as usernames, passwords, or credit card details.

The purpose of this project was to simulate a phishing attack using GoPhish, in order to evaluate the security awareness of my Friends. Specifically, I wanted to test:

- How users respond to realistic phishing emails
- Whether they can distinguish between legitimate and fraudulent messages
- If they would click suspicious links or enter sensitive data
- How many users are aware enough to report phishing attempts

This ethical phishing simulation helps assess human vulnerability in cybersecurity and aims to highlight the importance of user awareness training as a first line of defense against social engineering attackss.

b. Relevance of phishing simulations in cybersecurity

Phishing simulations are important in cybersecurity because they help people learn how to spot and avoid real phishing attacks. By sending fake but realistic emails, we can test how users respond, find weak points, and raise awareness. This helps build a stronger security culture and lowers the risk of serious problems like data breaches or financial loss.

2. Objectives

The main objectives of this project were:

- Simulate a Realistic Phishing Attack
  To design and launch convincing phishing emails and landing pages that mimic real-world scenarios (e.g., Microsoft 365 password expiry, Facebook login alerts).
- Assess User awareness
  To observe how users interact with the phishing emails ,whether they click the links, enter credentials, or report the email .In order to measure their vulnerability.
- Promote Awareness and Education
  To use the results of the simulation to increase awareness among participants, helping them understand the signs of phishing and how to respond safely in the future.

3. Tools and Technologies Used

- GoPhish
  An open-source phishing simulation framework used to create, send, and track phishing campaigns. It allows for building email templates, landing pages, and viewing detailed user interaction metrics (clicked, submitted, reported, etc.).

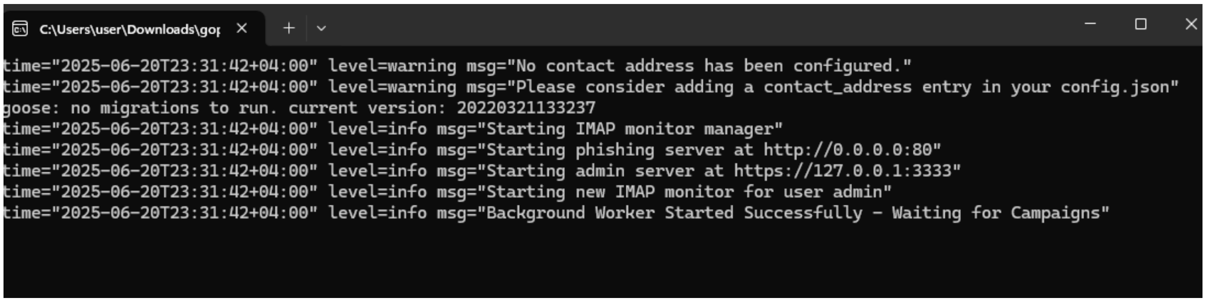
- Ngrok
  Used to expose the local GoPhish server and phishing landing pages to the internet via a secure public URL. This was necessary to reach users outside the local network.

- Gmail
  Gmail were used to test and interact with the phishing pages. Gmail was used as the email platform to receive and view phishing emails during the simulation.

4. Project Setup

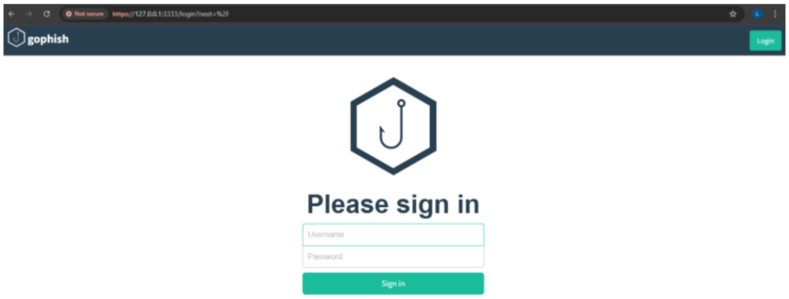
Environment Configuration

- GoPhish Installation:
  GoPhish was installed and run on a local machine (Windows/Linux). After launching the binary, the GoPhish dashboard was accessible via https://localhost:3333.



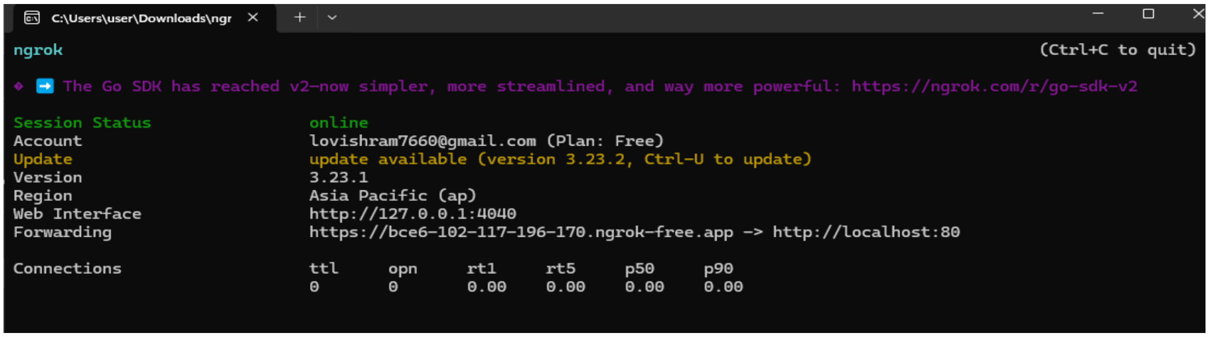
```
time="2025-06-20T23:31:42+04:00" level=warning msg="No contact address has been configured."
time="2025-06-20T23:31:42+04:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: no migrations to run. current version: 20220321133237
time="2025-06-20T23:31:42+04:00" level=info msg="Starting IMAP monitor manager"
time="2025-06-20T23:31:42+04:00" level=info msg="Starting phishing server at http://0.0.0.0:80"
time="2025-06-20T23:31:42+04:00" level=info msg="Starting admin server at https://127.0.0.1:3333"
time="2025-06-20T23:31:42+04:00" level=info msg="Starting new IMAP monitor for user admin"
time="2025-06-20T23:31:42+04:00" level=info msg="Background Worker Started Successfully - Waiting for Campaigns"
```

This is when the server Gophish is running on port 3333.



Ngrok Setup:

Ngrok was used to tunnel the local server (http://localhost:80) to a public URL like https://bcr6-102-117-196-170.ngrok-free.app, making it accessible to target outside the local network.



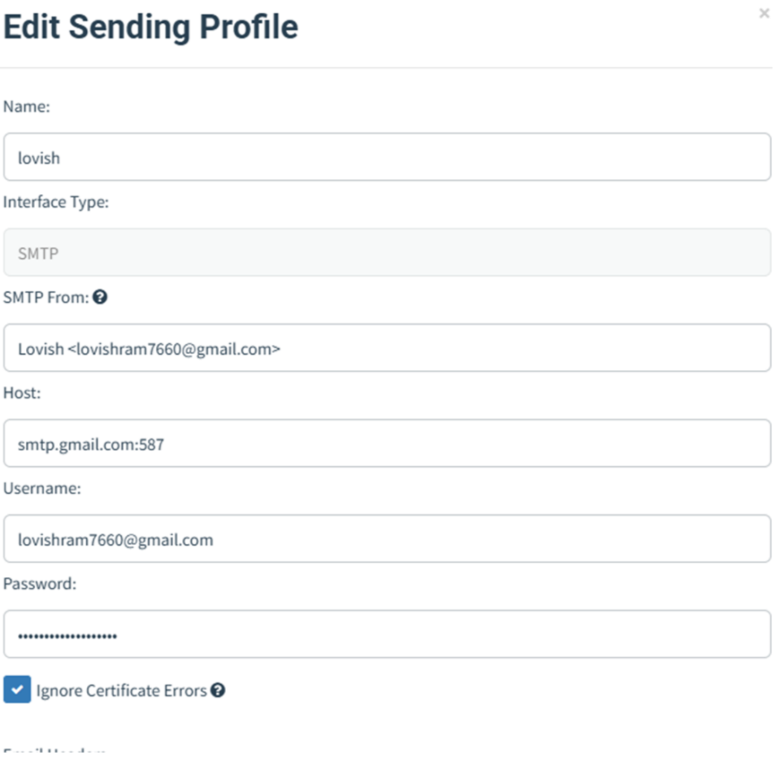
```
C:\Users\user\Downloads\ngr

ngrok                                                                                   (Ctrl+C to quit)

❖ ➡ The Go SDK has reached v2—now simpler, more streamlined, and way more powerful: https://ngrok.com/r/go-sdk-v2

Session Status                online
Account                       lovishram7660@gmail.com (Plan: Free)
Update                        update available (version 3.23.2, Ctrl-U to update)
Version                       3.23.1
Region                        Asia Pacific (ap)
Web Interface                 http://127.0.0.1:4040
Forwarding                    https://bce6-102-117-196-170.ngrok-free.app -> http://localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

Landing Page Hosting

- Phishing landing pages were created using GoPhish's built-in landing page editor.
- Each page was set to capture credentials and redirect users to legitimate websites (e.g,LinkedIn) after submission.

Email Server / Sender Configuration

- Emails were sent using GoPhish's default sending profile or a configured SMTP server.



Edit Sending Profile

Name:

lovish

Interface Type:

SMTP

SMTP From:

Lovish <lovishram7660@gmail.com>

Host:

smtp.gmail.com:587

Username:

lovishram7660@gmail.com

Password:

•••••••••••••••••••

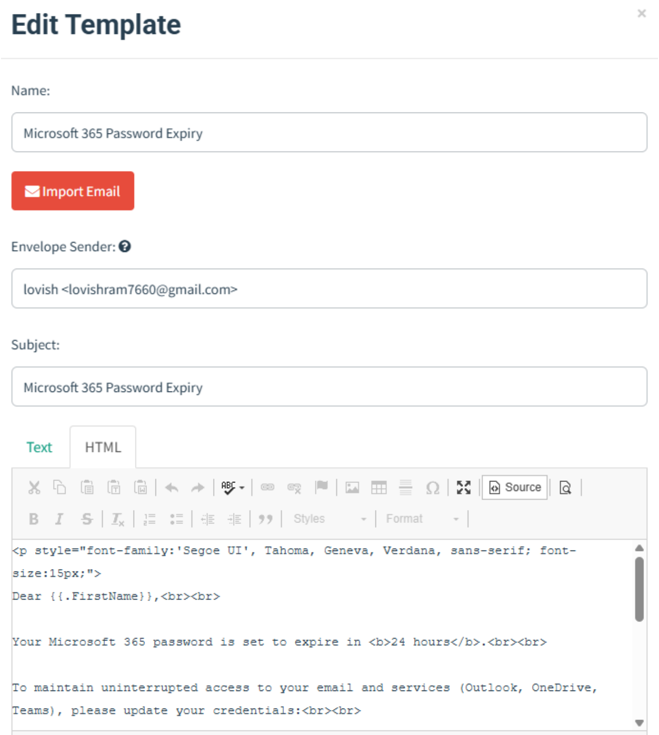
☑ Ignore Certificate Errors

5. Phishing Campaigns

As part of the simulation, three separate phishing campaigns were created to reflect common attack scenarios. Each campaign included a unique email template, a custom landing page, and a redirect to a real website after data submission to make the experience more realistic.

Campaign #1: Microsoft 365 Password Expiry

- Scenario: A fake alert notifying the user that their Microsoft 365 password is expiring within 24 hours, urging them to update it immediately.
- Email Template Highlights: Used branding colors, formal tone, and a prominent “Update Password” button linking to a phishing landing page.



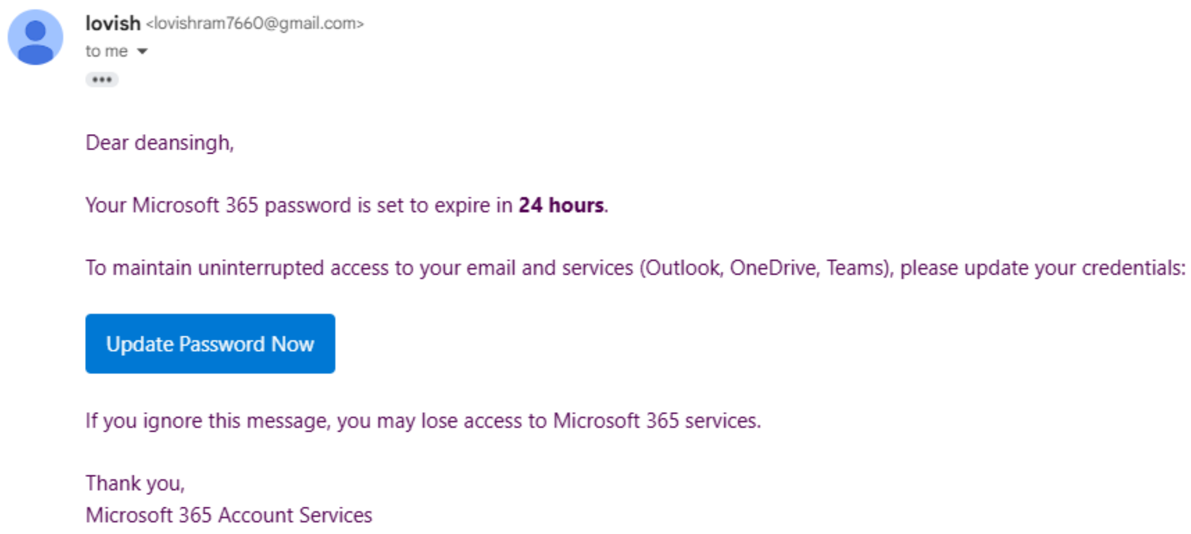
Edit Template

Name: Microsoft 365 Password Expiry

Envelope Sender: lovish <lovishram7660@gmail.com>

Subject: Microsoft 365 Password Expiry

```
<p style="font-family:'Segoe UI', Tahoma, Geneva, Verdana, sans-serif; font-
size:15px;">
Dear {{.FirstName}},<br><br>

Your Microsoft 365 password is set to expire in <b>24 hours</b>.<br><br>

To maintain uninterrupted access to your email and services (Outlook, OneDrive,
Teams), please update your credentials:<br><br>
```



lovish <lovishram7660@gmail.com>
to me

Dear deansingh,

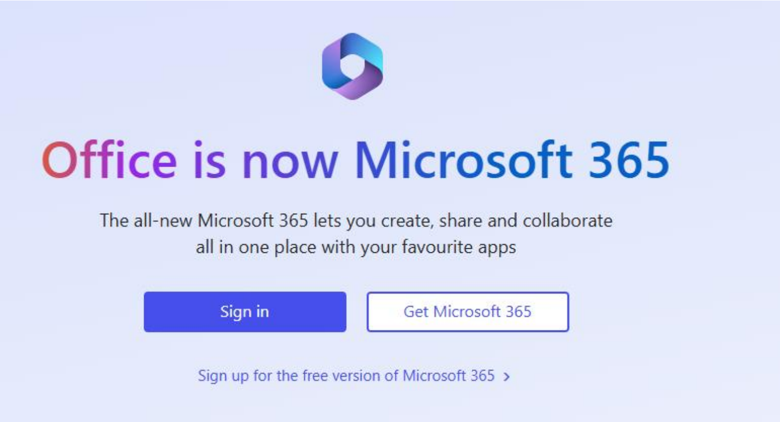
Your Microsoft 365 password is set to expire in **24 hours**.

To maintain uninterrupted access to your email and services (Outlook, OneDrive, Teams), please update your credentials:

If you ignore this message, you may lose access to Microsoft 365 services.

Thank you,
Microsoft 365 Account Services

- Landing Page: A fake Microsoft login form requesting the user's email and password.



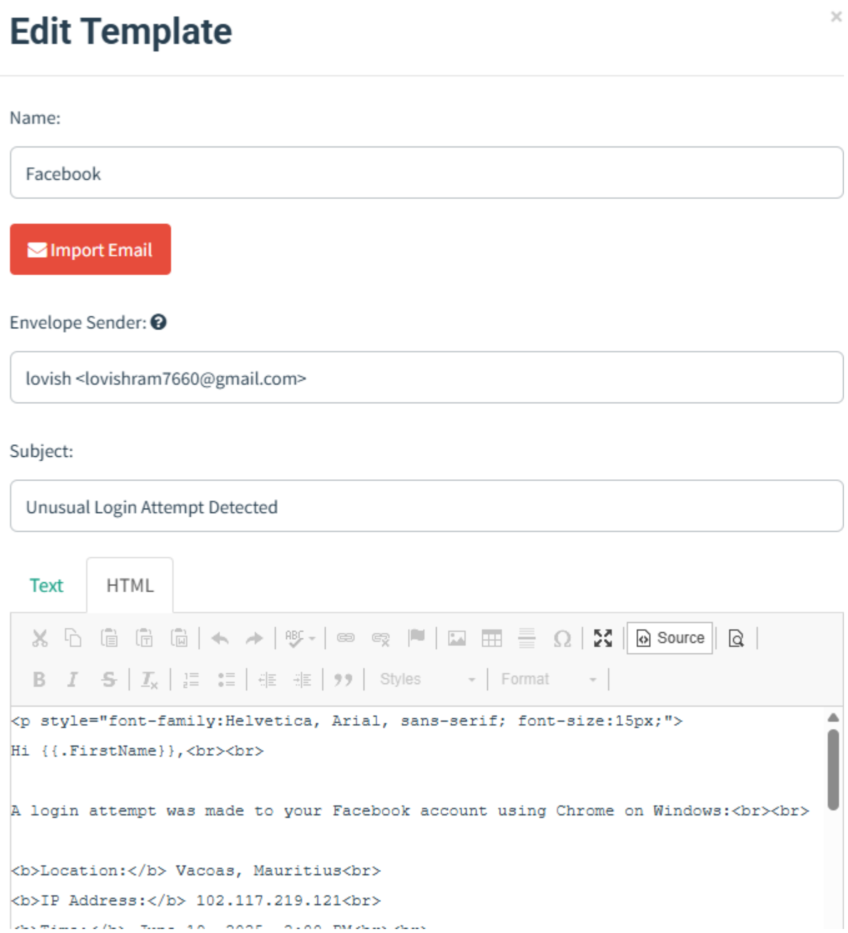
Office is now Microsoft 365

The all-new Microsoft 365 lets you create, share and collaborate all in one place with your favourite apps

- Redirect URL: https://outlook.office.com/mail/

Campaign #2: Facebook Login Attempt

- Scenario: A security alert email stating that a login attempt was detected from a new device, prompting the user to verify their account.
- Email Template Highlights: Included IP, location, device type, and a "Review Activity" button.



Edit Template

Name:

Facebook

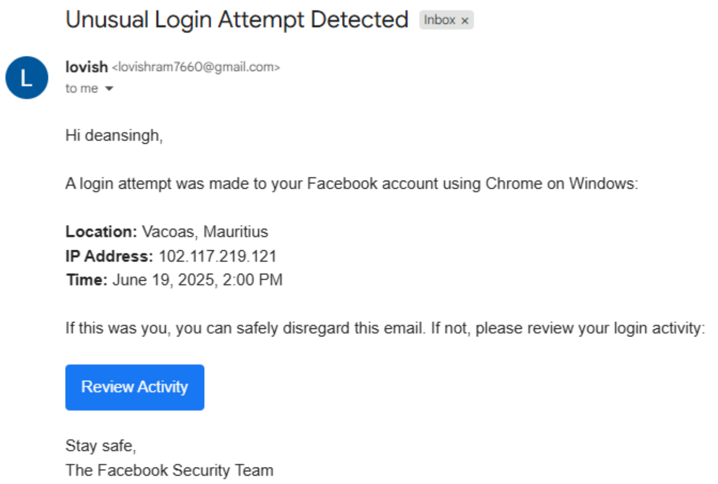
Envelope Sender:

lovish <lovishram7660@gmail.com>

Subject:

Unusual Login Attempt Detected

```
<p style="font-family:Helvetica, Arial, sans-serif; font-size:15px;">
Hi {{.FirstName}},<br><br>

A login attempt was made to your Facebook account using Chrome on Windows:<br><br>

<b>Location:</b> Vacoas, Mauritius<br>
<b>IP Address:</b> 102.117.219.121<br>
<b>Time:</b> June 19, 2025, 2:00 PM<br><br>
```



Unusual Login Attempt Detected

lovish <lovishram7660@gmail.com>
to me

Hi deansingh,

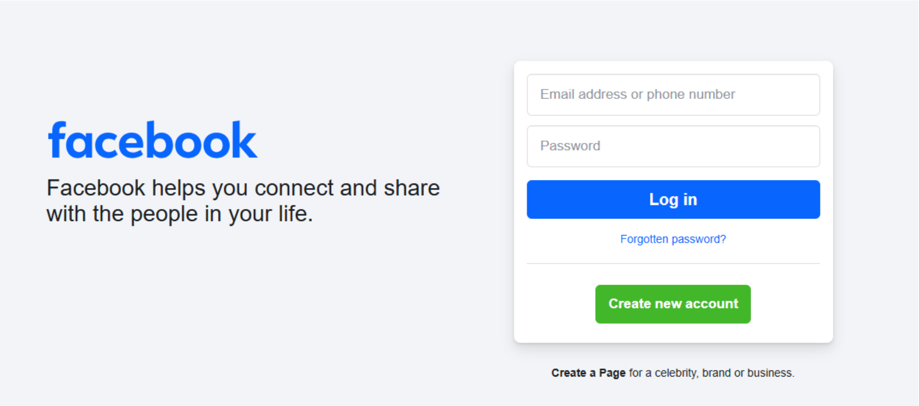
A login attempt was made to your Facebook account using Chrome on Windows:

Location: Vacoas, Mauritius
IP Address: 102.117.219.121
Time: June 19, 2025, 2:00 PM

If this was you, you can safely disregard this email. If not, please review your login activity:

Stay safe,
The Facebook Security Team

- Landing Page: A Facebook-style login form asking for email/phone and password.



Facebook helps you connect and share with the people in your life.

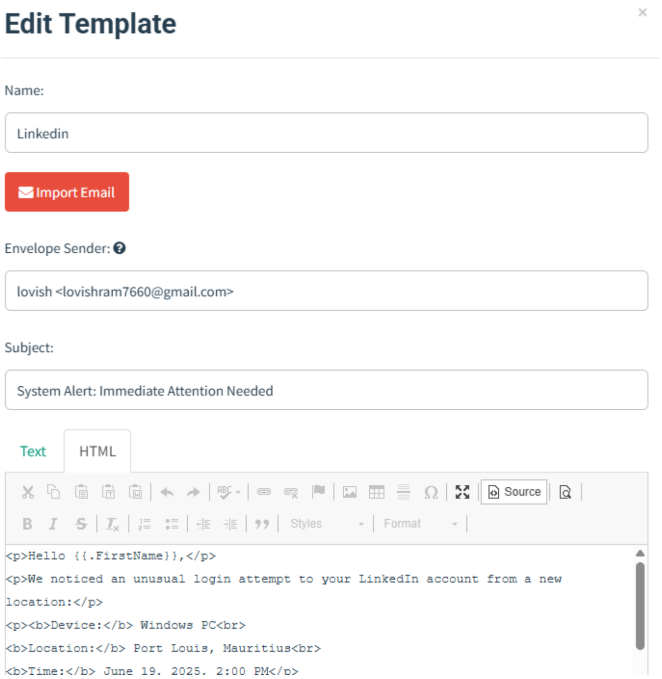
Create a Page for a celebrity, brand or business.

- Redirect URL: https://www.facebook.com/

Campaign #3: LinkedIn Suspicious Activity

- Scenario: A fake LinkedIn email notifying the user of suspicious activity on their account, with a link to "secure" their profile.
- Email Template Highlights: Used LinkedIn color theme and wording to

create urgency.



Edit Template

Name:

Linkedin

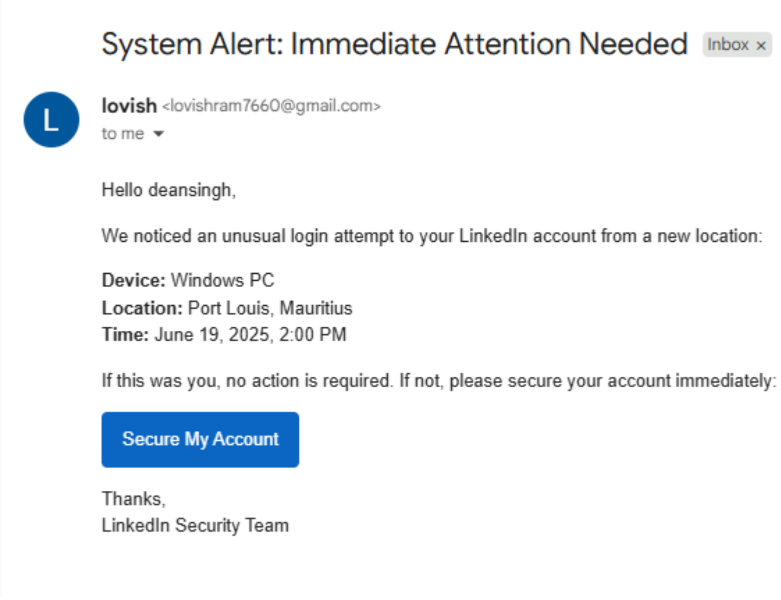
Envelope Sender:

lovish <lovishram7660@gmail.com>

Subject:

System Alert: Immediate Attention Needed

```
<p>Hello {{.FirstName}},</p>
<p>We noticed an unusual login attempt to your LinkedIn account from a new
location:</p>
<p><b>Device:</b> Windows PC<br>
<b>Location:</b> Port Louis, Mauritius<br>
<b>Time:</b> June 19, 2025, 2:00 PM</p>
```



System Alert: Immediate Attention Needed

lovish <lovishram7660@gmail.com>
to me

Hello deansingh,

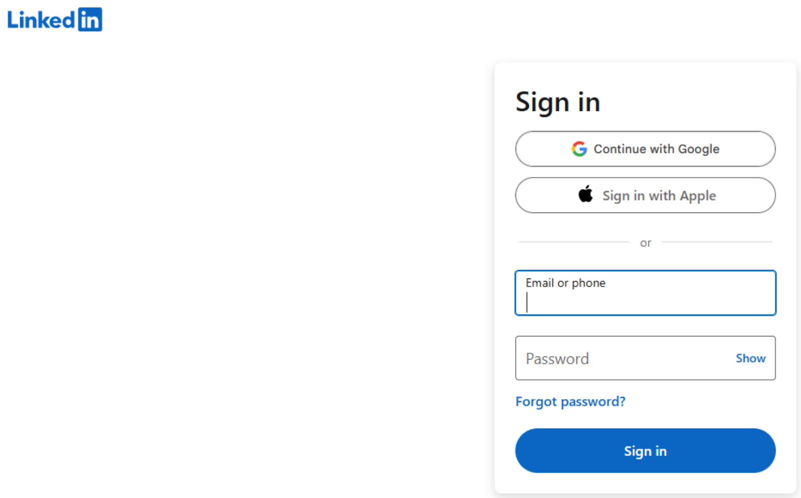
We noticed an unusual login attempt to your LinkedIn account from a new location:

Device: Windows PC
Location: Port Louis, Mauritius
Time: June 19, 2025, 2:00 PM

If this was you, no action is required. If not, please secure your account immediately:

Thanks,
LinkedIn Security Team

- Landing Page: A simple login form styled to look like the LinkedIn sign-in page.



- Redirect URL: https://www.linkedin.com/feed/

6. Target Groups

The phishing simulation was conducted on a small, controlled group of users for ethical testing and awareness purposes.

Number of Targets

A total of 7 users were included in this simulation across all campaigns.

Types of Users

The selected targets were:

- Friends and classmates from Polytechnic Mauritius
- Individuals with basic to intermediate knowledge of cybersecurity

This mix helped ensure the scenarios were realistic and relatable to the test group.

Consent Obtained

- Informed consent was obtained from all participants prior to the test.
- Participants were notified that this was a controlled ethical phishing simulation for educational and awareness purposes.
- No real credentials were collected or stored outside the GoPhish environment, and no harm was caused.

Note: If you did not obtain formal consent and only tested on yourself or close friends, you can rephrase as:

“All users were close friends who gave verbal consent to participate in this simulation. The activity was conducted strictly for academic purposes, with no malicious intent or data misuse.”

7. Tracking and Reporting

GoPhish provides powerful built-in tracking features that allow campaign managers to monitor how users interact with phishing emails and landing pages. In this project, several key metrics were captured to assess user behavior and awareness.

Metrics Captured

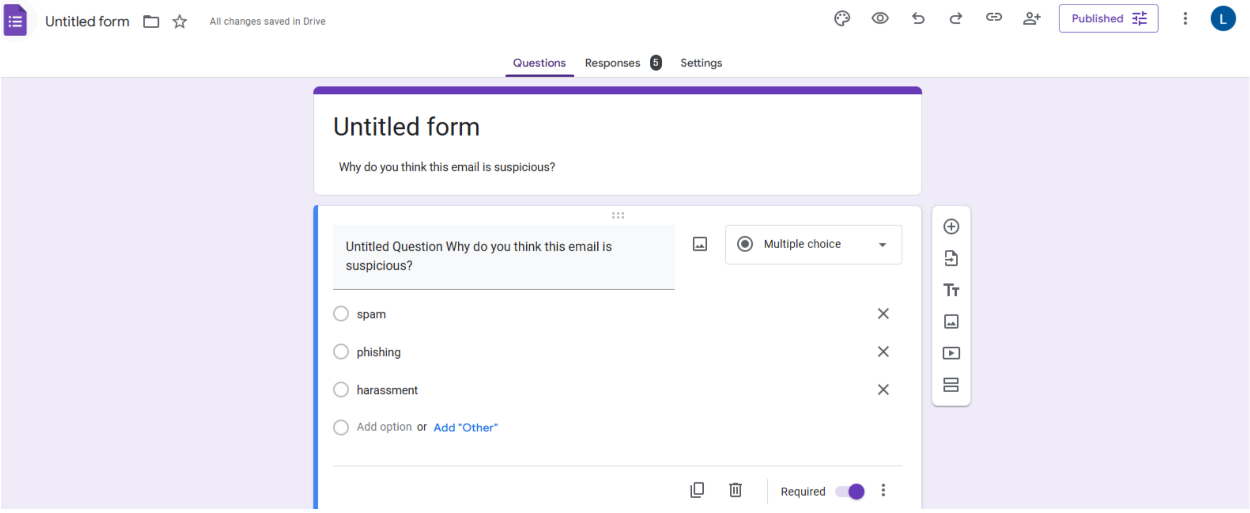
The following user interaction metrics were tracked for each phishing campaign:

Metric	Description
Email Opened	Indicates that the target opened the phishing email.
Link Clicked	Indicates that the target clicked the phishing link ({{.URL}}) in the email.
Credentials Submitted	Shows that the user filled out and submitted information on the fake login page.
Email Reported	Simulated via a Google Form where users could report suspicious emails. Reporting status was manually updated in GoPhish based on form submissions.

Reporting Simulation

Since GoPhish does not automatically detect reports from Gmail, a custom "Report Phishing" link was added at the bottom of each email template. This link redirected users to a Google Form, allowing them to report the email if they suspected phishing.

- Each form response was logged with the target's name or email
- Reports were cross-referenced with GoPhish results
- GoPhish entries were manually marked as "Reported" for users who filled out the form



Untitled form

Why do you think this email is suspicious?

Untitled Question Why do you think this email is suspicious?

○ spam

○ phishing

○ harassment

8. Results and Statistics

The phishing simulation results were analyzed based on email opens, link clicks, credential submissions, and phishing reports. These metrics help assess the security awareness of the participants and their ability to identify and respond to phishing threats.

Table: Campaign Results Summary

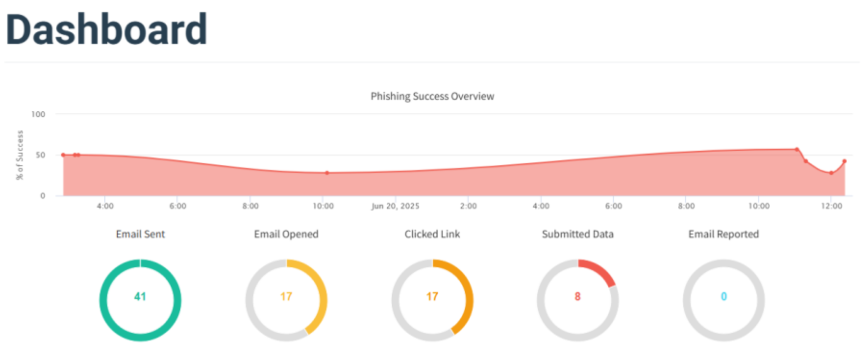
User	Opened	Clicked	Submitted	Reported
deansinghramphul@gmail.com	⍰	⍰	⍰	⍰
neeleshramphul2010@gmail.com	⍰	⍰	⍰	⍰
deenkybedasee0@gmail.com	⍰	⍰	⍰	⍰

fmahomudally1604@gmail.com	⍰	⍰	⍰	⍰
neyhaula@gmail.com	⍰	⍰	⍰	⍰
abhishbhantooa60@gmail.com	⍰	⍰	⍰	⍰

⍰ = Yes ⍰ = No

Chart: Click-Through and Submission Rates

Metric	Count	Percentage
Emails Sent	41	100%
Emails Opened	17	41%
Links Clicked	17	41%
Credentials Submitted	8	19%
Emails Reported (via Form)	5	12.1%



9. Analysis

Behavior Pattern	Observation
Users who clicked but didn’t submit	Likely became suspicious after landing page load
Users who submitted but didn’t report	Possibly unaware of reporting practices
Users who reported without clicking or submitting	Strong awareness — recognized it as phishing

Repeat clickers across campaigns	More susceptible — should receive awareness training

10. Recommendations

Based on the results of this phishing simulation, the following recommendations are suggested to improve user awareness and reduce the risk of real-world phishing attacks:

How to Reduce Phishing Risk

- Use strong spam filters to detect and block suspicious emails before they reach users.
- Implement multi-factor authentication (MFA) so that even if credentials are compromised, access to systems is not easily granted.
- Keep browsers and systems up to date to protect users from malicious links and credential-stealing scripts.

Suggestions for Awareness Training

- Conduct regular cybersecurity awareness sessions to teach users how to identify phishing indicators such as suspicious sender names, spelling errors, or misleading URLs.
- Use simulated phishing tests periodically, like this project, to keep users alert.

How This Simulation Helped

- Made participants aware of how realistic phishing emails can be.
- Helped demonstrate common phishing techniques, such as urgency and impersonation.
- Identified which users need further training and support.

11. Limitations

Despite the success of the project, several limitations were noted:

Free Ngrok Limitations

- Ngrok’s free plan uses a temporary, randomly generated URL that changes each time, making it less reliable for long-term campaigns.
- It also has limited speed and connection time, which can affect accessibility.

No Automatic Email Reporting Integration

- GoPhish does not automatically detect when an email is reported using Gmail, Outlook, or other clients.
- A Google Form was used instead, and results had to be manually cross-checked and updated in GoPhish.

Small Target Group

- The number of participants was limited to a few classmates and friends.
- While useful for a proof-of-concept, the results may not reflect a broader population with varied awareness levels.

---

12. Conclusion

This phishing simulation using GoPhish successfully demonstrated the effectiveness of phishing tactics and the importance of cybersecurity awareness.

What Was Achieved

- Designed and launched three realistic phishing campaigns using GoPhish.
- Captured user interactions including opens, clicks, submissions, and reports.
- Assessed the awareness level of users in identifying and responding to phishing emails.

Skills Learned

- Setting up GoPhish and Ngrok for phishing simulations.
- Creating phishing email templates and landing pages.
- Analyzing user behavior and tracking security metrics.
- Understanding the social engineering aspect of cyberattacks.

Future Improvements

- Use a custom domain instead of Ngrok for more realism.
- Integrate an automated reporting system.
- Expand to a larger and more diverse test group.
- Use spear phishing.