

# Security Awareness Report

---

Phishing Simulation and User Interaction Analysis

Tool Used: GoPhish Open-source Phishing Simulation Framework

Date: 24-7-2025

Task 7: Phishing Simulation

Prepared By: Ammarah Taj

Report to Internee.pk on behalf of Cyber Security Internship

## Objective

The purpose of this project was to assess the security awareness of users within an organization by simulating a realistic phishing attack using GoPhish. The goal was to identify potential vulnerabilities in user behavior and generate insights to improve cybersecurity training efforts.

## Tools and Technologies Used

- GoPhish – An open-source phishing framework used for creating and managing phishing campaigns.
- Google Email Templates – To simulate real-world phishing emails.
- Custom Landing Page – Fake login page mimicking legitimate services to track credential submission behavior.

## Simulation Setup

### 1. Campaign Configuration:

- Target Group n .csv file:


	A	B	C	D	E
1	First name	Last name	email	Position	
2	Umeping T	Farwa	umefarwa	student	
3	Hina	Taj	hinataj15	student	
4	Amara	Taj	ammaraTaj	student	
5	Ammarah	Taj	ammaraht	student	

- Email Template: Fake security alert
- Landing Page: Fake login page designed to mimic Google
- URL Redirection: Embedded tracking URL


### 2. Email Delivery Method:

- SMTP server setup (or local delivery)
- Tracking for: Email opened, Link clicked, Credentials submitted

## Email Template and Landing page used



### Change your Password Now

 [ammarah43@gmail.com](mailto:ammarah43@gmail.com)

---

We noticed some suspicious behaviour on your Google account. If you would like to change your password, click below:

[Change Password Now](#)

You can also see security activity at:  
<https://myaccount.google.com/notifications>

You received this email to let you know about important changes to your Google Account and services.  
© 2025 Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

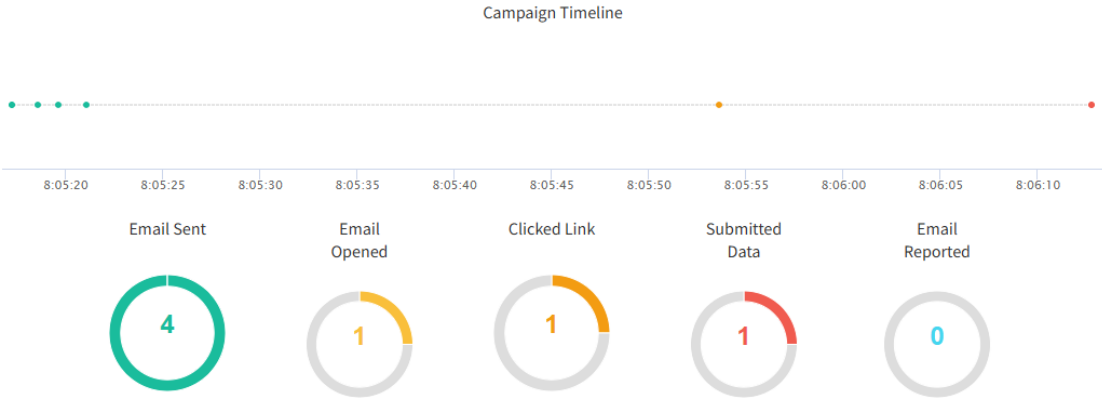
Username:

Password:

## Results Summary

Metric	Result
Emails Sent	4
Emails Delivered	4
Emails Opened	1
Users Clicked the Link	1
Users Submitted Credentials	1
Users Reported the Email	0

Out of 4 users, 1 opened the email, 1 clicked on the phishing link, and 1 submitted credentials.



## Behavioral Analysis

- Common Red Flags Missed:
  - Unfamiliar sender address
  - Suspicious link text
- User Response Observations:
  - Some users clicked links without verifying the email's authenticity.
  - A small number of users submitted their login credentials.
  - No users reported the phishing email to the security team.

## **Recommendations**

1. Security Awareness Training by Conduct regular awareness sessions and emphasize identification of phishing red flags.
2. Technical Controls: Implement email link scanning and URL filtering. Enable multi-factor authentication to reduce impact of credential leaks.
3. Policy Enforcement: Encourage users to report suspicious emails immediately.

## **Conclusion**

The phishing simulation using GoPhish provided valuable insights into user behavior in response to social engineering attacks. While most users showed awareness, some still fell victim to the phishing attempt, indicating the need for enhanced training and improved incident response awareness.