

PROJECT TITLE:

**PHISHING AWARENESS SIMULATION USING
GOPHISH**

BY:

SHIVANGI TRIVEDI

B.TECH (COMPUTER SCIENCE ENGINEERING)

LOVELY PROFESSIONAL UNIVERSITY

PHISHING ATTACK SIMULATOR PROJECT REPORT

1. Introduction

Phishing is one of the most common social engineering attacks used by cybercriminals to steal sensitive information such as usernames, passwords, and financial data. To understand the effectiveness of phishing and to train users against such attacks, a **Phishing Attack Simulation** was conducted using the open-source tool **GoPhish**.

This project demonstrates how phishing campaigns are created, deployed, and analyzed in a controlled and safe environment for **awareness and defensive learning purposes**.

2. Objectives

- To simulate a real-world phishing attack using GoPhish.
- To analyze user responses to phishing emails.
- To generate awareness about the risks of phishing attacks.
- To prepare defense strategies based on user behavior.

3. Tools & Technologies

- **GoPhish** – Open-source phishing simulation tool.
- **SMTP Configuration** – For sending phishing emails via smtp4dev.

- **HTML/CSS Templates** – For creating fake login pages.
- **CSV Export & Visualization** – For analyzing captured results.
- **Pie Charts & Graphs** – For presenting awareness statistics.

4. Methodology

Step 1: Environment Setup

- Installed **GoPhish** on Windows.
- Configured SMTP for sending test emails via smtp4dev

Step 2: Campaign Creation

- Designed a **fake login page** imitating a LinkedIn security alert.
- Configured the phishing email with a link redirecting to the fake page.
- Created user groups (targets) for testing.

Step 3: Execution

- Launched the phishing campaign.
- Sent phishing emails to the selected group.
- Monitored delivery, clicks, and credential submissions.

Step 4: Data Collection

- Exported results as **CSV files**.
- Visualized responses with **pie charts** showing awareness levels (clicked, submitted data, ignored, etc.).

5. Results & Findings

Email Templates, Landing Page, Sending Profiles(Gophish)

New Template

X

Name:

Urgent Password Reset Warning

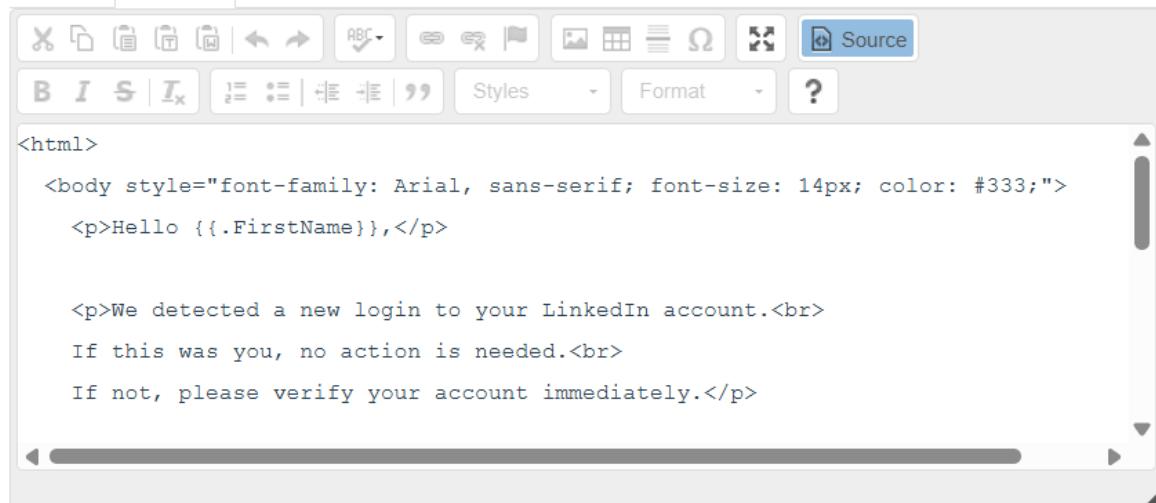
 Import Email

Subject:

Urgent!! Verify account immediately

Text

HTML



The image shows a screenshot of an email editor interface. At the top, there are two tabs: "Text" and "HTML". The "Text" tab is selected. Below the tabs is a toolbar with various icons for file operations (New, Open, Save, Print, etc.), text styling (Bold, Italic, Strike, Font, Alignment, Font Size, Color), and other formatting options. On the far right of the toolbar is a "Source" button. The main area is a code editor containing the following HTML code:

```
<html>
<body style="font-family: Arial, sans-serif; font-size: 14px; color: #333;">
<p>Hello {{.FirstName}},</p>

<p>We detected a new login to your LinkedIn account.<br>
If this was you, no action is needed.<br>
If not, please verify your account immediately.</p>
```

Add Tracking Image

New Sending Profile

X

Name:

Local SMTP

Interface Type:

SMTP

From:

shivangi@company.com

Host:

127.0.0.1

Username:

Username

Password:

Password

Ignore Certificate Errors ?

Email Headers:

X-Custom-Header

{{.URL}}-gophish

+ Add Custom Header

New Landing Page

Name:

Copy of Awareness Page

 Import Site

HTML



```
<!DOCTYPE html><html><head>
<meta charset="UTF-8"/>
<title>Phishing Awareness</title>
<style>
body {
    font-family: Arial, sans-serif;
    background-color: #f9f9f9;
    color: #222;
}
```

Capture Submitted Data 

Cancel

Save Page

New Landing Page

Name:

Copy of Fake linkedin Login

 Import Site

HTML

```
<html><head></head><body style="font-family: Arial, sans-serif; text-align:center;>
  <h2>LinkedIn Login</h2>
  <form action="" method="POST">
    <input type="text" name="username" placeholder="Email or Phone" style="padding: 10px; border-radius: 5px; border: 1px solid #ccc; width: 300px; margin-bottom: 10px;" />
    <input type="password" name="password" placeholder="Password" style="padding: 10px; border-radius: 5px; border: 1px solid #ccc; width: 300px; margin-bottom: 10px;" />
    <input type="submit" value="Sign In" style="padding: 10px 20px; background-color: #007bff; color: white; border: none; border-radius: 5px; font-weight: bold; width: 150px; margin-top: 10px;" />
  </form>
</body></html>
```

Capture Submitted Data 

Cancel

Save Page

CSV Data

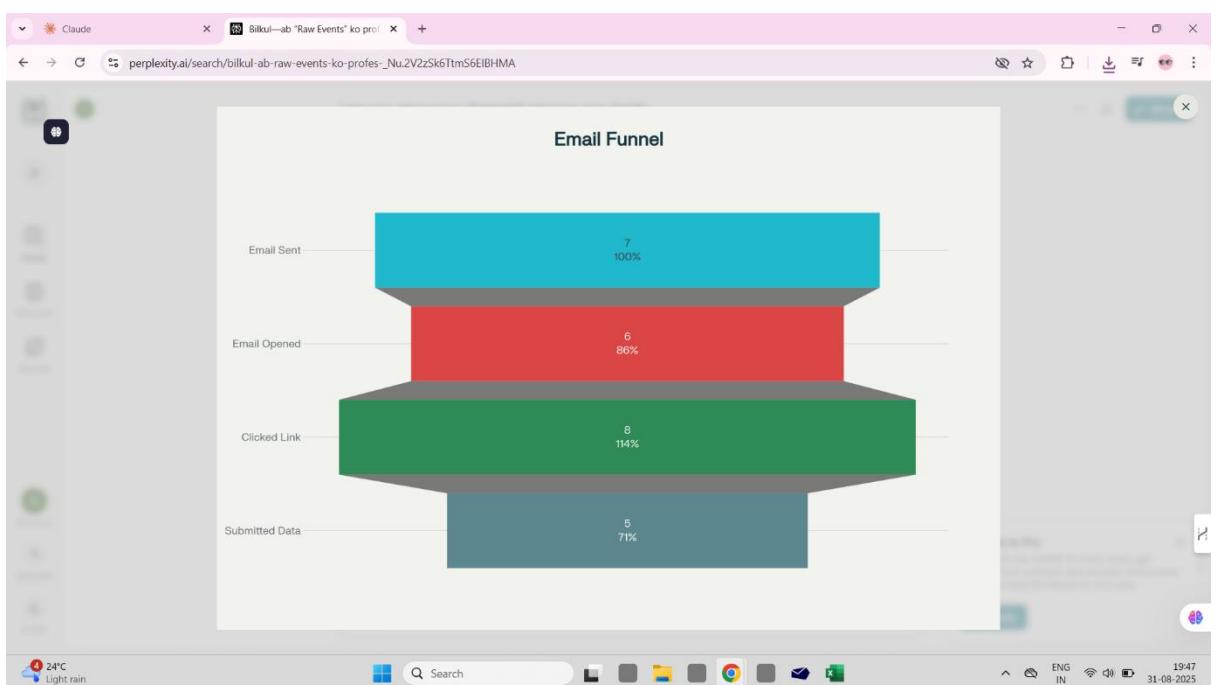
• CSV chart of AWARENESS CAMPAIGN

POSSIBLE DATA LOSS		Some features might be lost if you save this workbook in the comma-delimited (.csv) format. To preserve these features, save it in an Excel file format.														Don't show again		Save As...			
A1	email	Sent Time	Opened	Tir	Clicked	Tir	Submitted	Time													
1	dubeys@12	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	
2	dubeys@12	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	
3	lpu@79861	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	
4	sandeep3@	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	
5	shivangi@i	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	
6	shyamli@12	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	
7	trivedi@co	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	
8	vedangi@i	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	2025-08-3 2025-08-3	
9																					
10																					
11																					
12																					
13																					

CSV chart of Copy of Pseudo Login

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	email	time	message	details	time_IST											
2	dubey@12	2025-08-3	Clicked Link	{"payload": "2025-08-31 01:14:53.119367800+00:00"}												
3	dubey@12	2025-08-3	Email Opened	{"payload": "2025-08-31 01:14:51.829553800+00:00"}												
4	dubey@12	2025-08-3	Email Sent	2025-08-31 01:12:59.975604900+00:00												
5	dubey@12	2025-08-3	Submitted	{"payload": "2025-08-31 01:17:57.793146600+00:00"}												
6	lpu@79861	2025-08-3	Clicked Link	{"payload": "2025-08-31 01:13:33.910231500+00:00"}												
7	lpu@79861	2025-08-3	Email Opened	{"payload": "2025-08-31 01:13:32.128266+00:00"}												
8	lpu@79861	2025-08-3	Email Sent	2025-08-31 01:13:00.038038600+00:00												
9	lpu@79861	2025-08-3	Submitted	{"payload": "2025-08-31 01:14:31.650796300+00:00"}												
10	sandeep3c	2025-08-3	Email Sent	2025-08-31 01:12:59.860457600+00:00												
11	shivangi@i	2025-08-3	Clicked Link	{"payload": "2025-08-31 19:18:24.495743800+00:00"}												
12	shivangi@i	2025-08-3	Email Opened	{"payload": "2025-08-31 19:18:23.008869700+00:00"}												
13	shivangi@i	2025-08-3	Email Sent	2025-08-31 01:12:59.510305900+00:00												
14	shivangi@i	2025-08-3	Submitted	{"payload": "2025-08-31 19:18:42.436116600+00:00"}												
15	shyamli@i	2025-08-3	Clicked Link	{"payload": "2025-08-31 01:27:18.871000100+00:00"}												
16	shyamli@i	2025-08-3	Email Opened	{"payload": "2025-08-31 01:27:17.123752200+00:00"}												
17	shyamli@i	2025-08-3	Email Sent	2025-08-31 01:12:59.921718800+00:00												
18	shyamli@i	2025-08-3	Submitted	{"payload": "2025-08-31 01:27:52.275780400+00:00"}												
19	trivedi@co	2025-08-3	Email Sent	2025-08-31 01:12:59.734587700+00:00												
20	vedang@i	2025-08-3	Email Sent	2025-08-31 01:12:59.796857+00:00												
21			Campaign Created	2025-08-31 01:10:33.984523300+00:00												
22																
23																
24																
25																
26																

1. Diagram representation of results of Copy of pseudo login:-



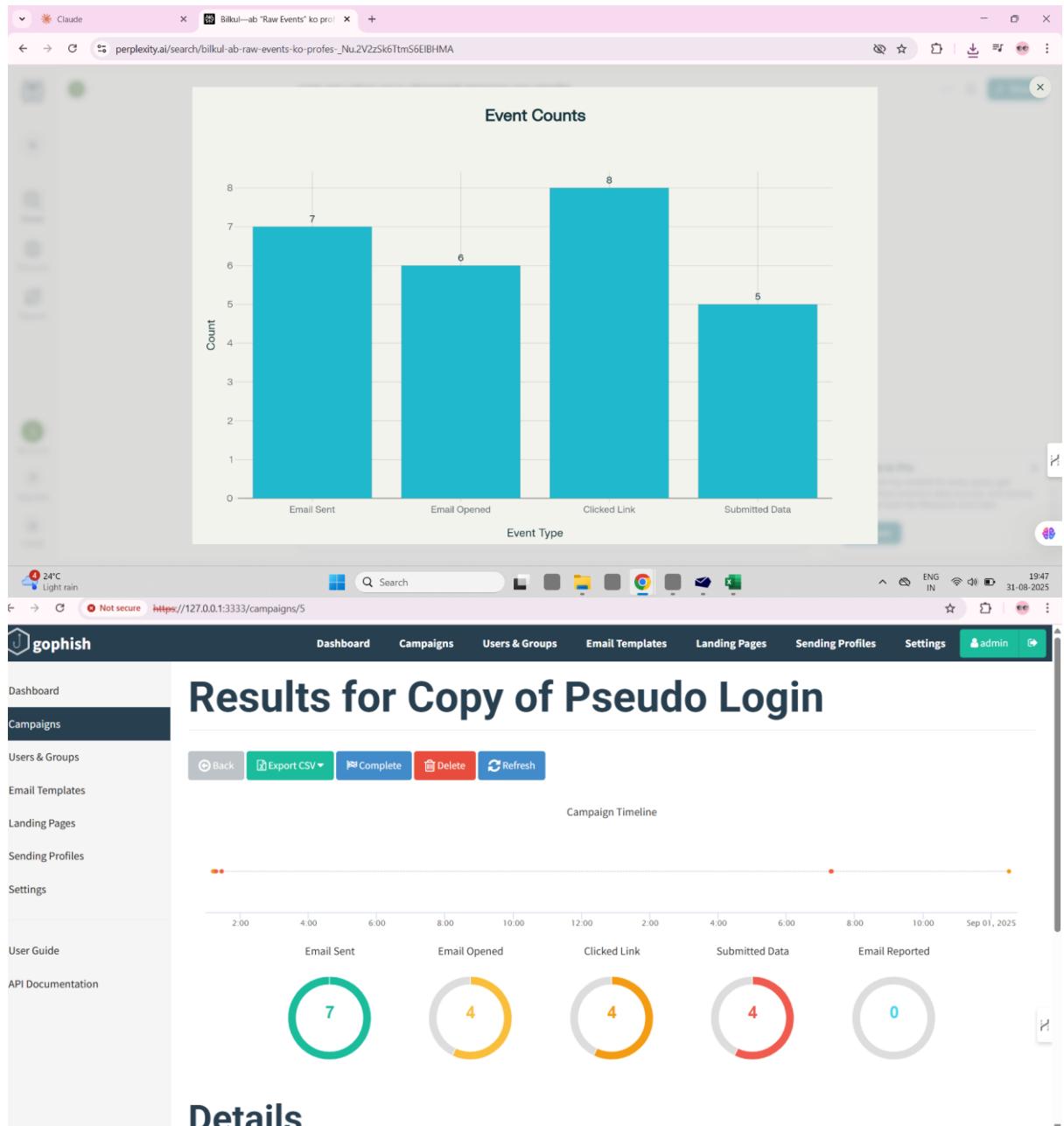
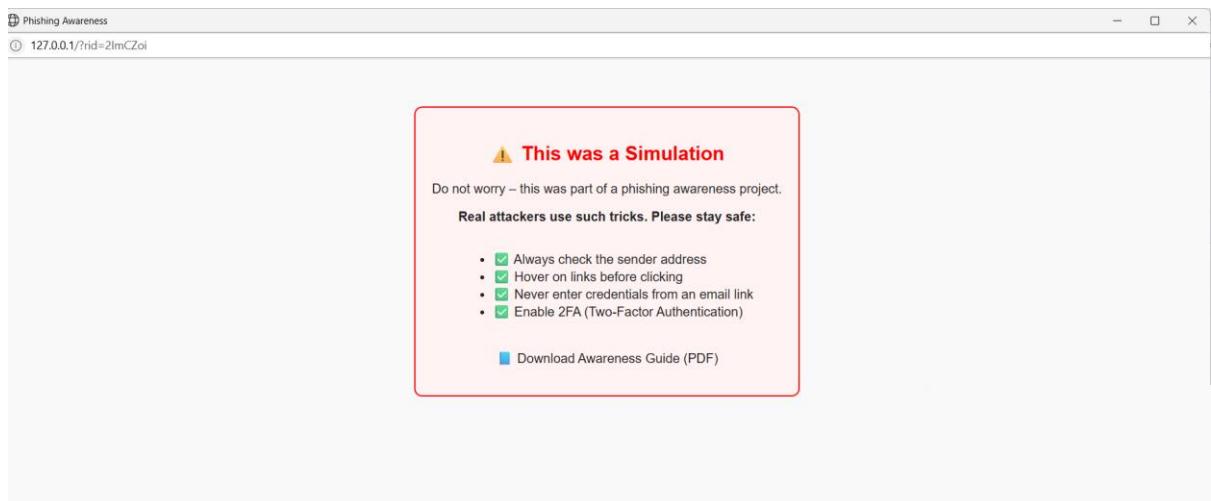
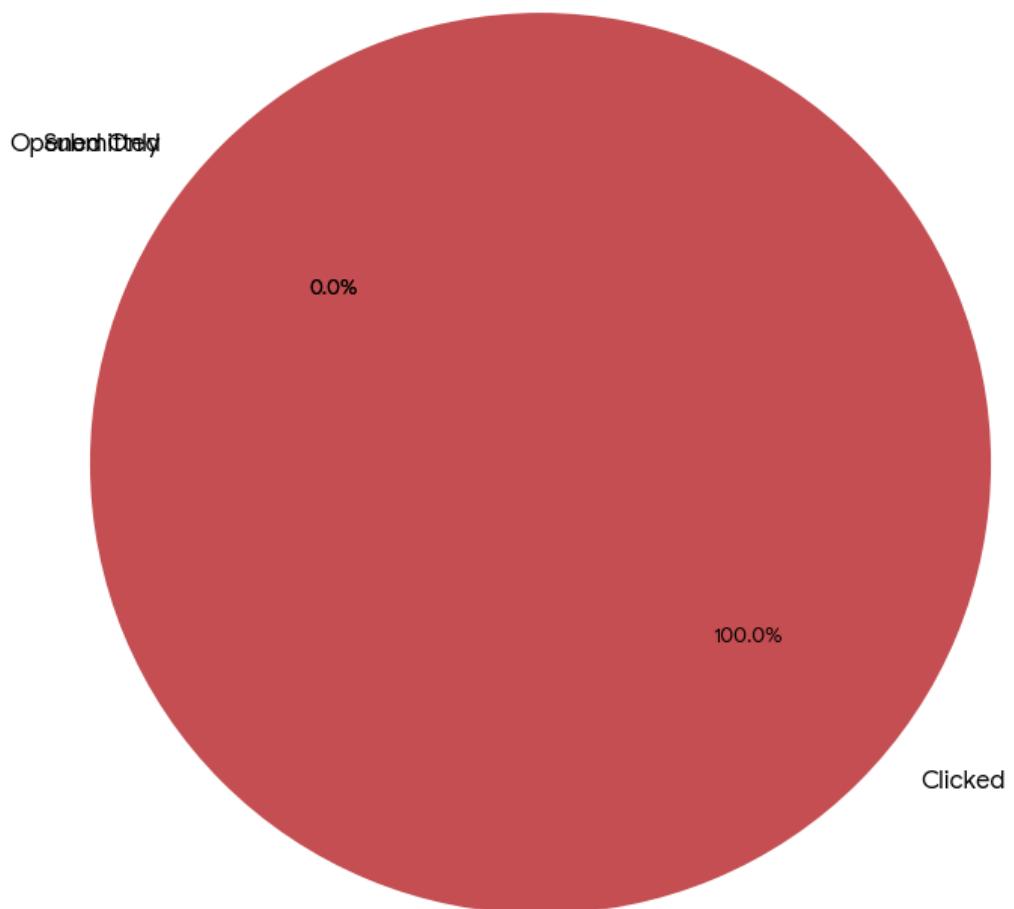


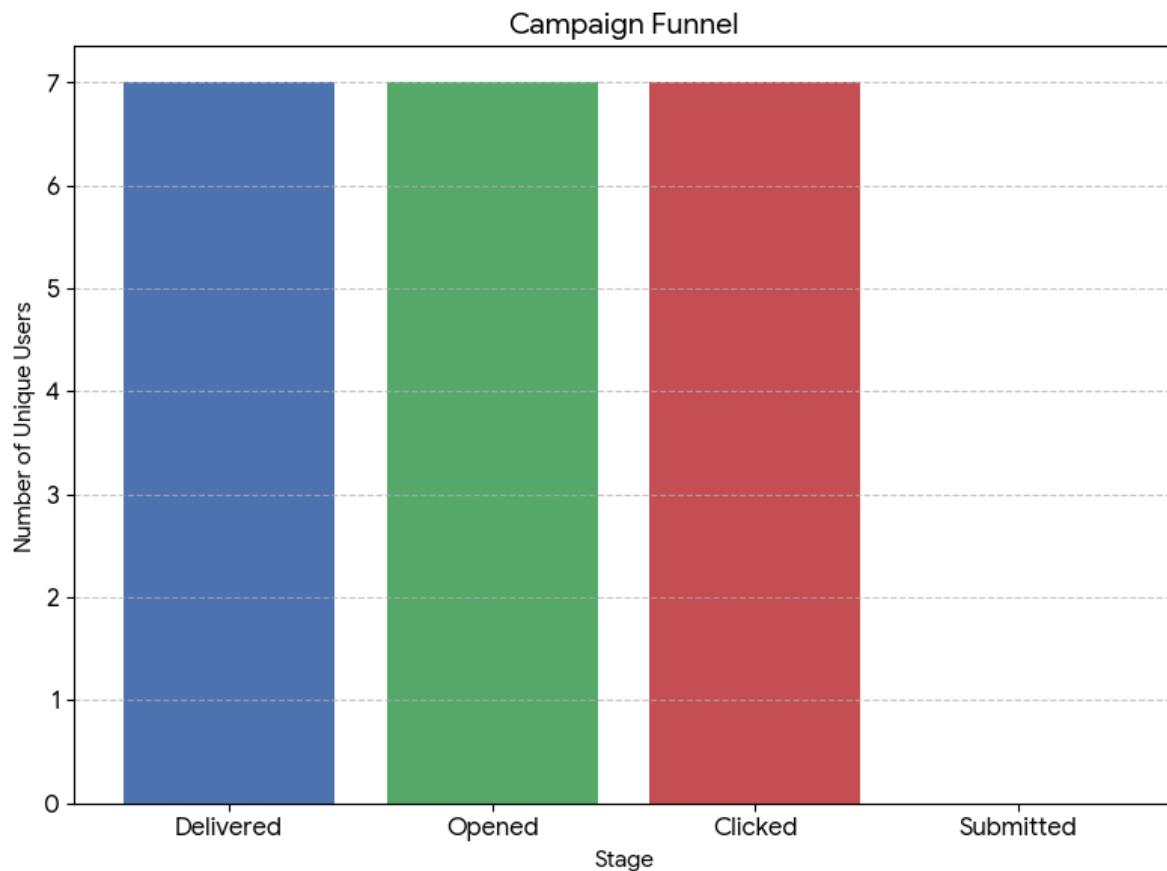
Diagram Representation of results of Awareness Campaign



A screenshot of the gophish application interface. The title bar shows "Not secure https://127.0.0.1:3333/campaigns/8". The top navigation bar includes "Dashboard", "Campaigns", "Users & Groups", "Email Templates", "Landing Pages", "Sending Profiles", "Settings", and a user "admin". The left sidebar has links for "Dashboard", "Campaigns" (which is selected), "Users & Groups", "Email Templates", "Landing Pages", "Sending Profiles", "Settings", "User Guide", and "API Documentation". The main content area is titled "Results for Awareness Campaign". It features a "Campaign Timeline" with markers at 12:20, 12:30, 12:40, 12:50, 1:00, 1:10, 1:20, 1:30, 1:40, 1:50, and 2:00. Below the timeline are five circular metrics: "Email Sent" (7), "Email Opened" (7), "Clicked Link" (7), "Submitted Data" (0), and "Email Reported" (0). Action buttons at the top include "Back", "Export CSV", "Complete", "Delete", and "Refresh".

User Engagement Breakdown





Observations

- A percentage of users clicked on the phishing link, indicating susceptibility.
- A smaller group submitted credentials, highlighting lack of awareness.
- Some users ignored or reported the email, showing strong awareness

Skills My Project Shows

Technical Skills

1. Cybersecurity Fundamentals

- Understanding of phishing, social engineering, and the human factor.

- Knowledge of attack vectors (email spoofing, credential harvesting).

2. Security Tools & Platforms

- Hands-on experience with **GoPhish** (phishing framework).
- Configuring **SMTP servers** for secure mail delivery.
- Creating **fake login pages** (LinkedIn, Outlook, etc.).

3. Networking & Email Security

- Concepts of **TLS/SSL, SMTP authentication, and app passwords**.
- Understanding email delivery challenges (spam filters, spoofing protections like SPF/DKIM/DMARC).

4. Data Handling & Analysis

- Exporting campaign data as **CSV**.
- Interpreting results (open rate, click rate, credential submissions).
- Creating **awareness pie charts** & reports.

5. Incident Simulation & Reporting

- Simulating a **real-world phishing attack scenario**.
- Writing **structured professional reports** with screenshots, charts, and metrics.

Soft / Professional Skills

1. Project Management

- Structured execution: Setup → Campaign → Results → Awareness.
- Completing **multi-phase projects independently**.

2. Analytical Thinking

- Evaluating user behavior & attack effectiveness.
- Translating raw logs into meaningful security insights.

3. Communication Skills

- Explaining complex technical results in a **clear report format**.
- Awareness training focus → **bridging tech & non-tech audiences**.

4. Problem-Solving

- Overcame issues with email delivery, TLS, app passwords.
- Debugged SMTP/Gmail/Outlook(not used) instead downloaded local smtp4dev.

5. Cybersecurity Mindset

- Thinking both like an **attacker (red team)** and a **defender (blue team)**.

6. Conclusion

This project successfully demonstrated the **creation, deployment, and analysis of a phishing attack simulation**. The results highlight the importance of **phishing awareness training** in organizations.

Key takeaways:

- Even a basic phishing campaign can trick a significant portion of users.
- Awareness programs and continuous simulations are necessary to reduce risks.
- Defensive measures like email filters, multi-factor authentication, and regular employee training can greatly minimize the impact of phishing.

7. Future Scope

- Integration of **automated awareness training** after simulation.
- Using **machine learning** to detect phishing patterns.
- Extending the project to simulate **spear phishing** and **business email compromise**.

