

**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



Name:

Urgent Password Reset Warning



 Import Email

Subject:

Urgent!! Verify account immediately

Text

HTML

```
<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



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

 Source

**B** *I* S I<sub>x</sub>        Styles    Format    ?

```
<!DOCTYPE html><html><head>
  <meta charset="UTF-8"/>
  <title>Phishing Awareness</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #f9f9f9;
      color: #222;
    }
  </style>
</head>
<body>
  <div>
    <h1>Phishing Awareness</h1>
    <p>Phishing is a type of cyber attack where someone impersonates a trusted entity to steal sensitive information like passwords, credit card numbers, or other personal data. It often involves creating fake websites, emails, or messages that look legitimate.
  </div>
  <div>
    <h2>How to Protect Yourself</h2>
    <ol>
      <li>Be cautious of unsolicited emails or messages, especially those asking for personal information or money.
      <li>Verify the sender's email address and contact them through a trusted channel if you're unsure.
      <li>Never click on suspicious links or download attachments from unknown sources.
      <li>Use strong, unique passwords and enable two-factor authentication (2FA) on your accounts.
      <li>Keep your software, including operating systems and browsers, up to date with security patches.
      <li>Be wary of offers that seem too good to be true or create a sense of urgency.
      <li>Regularly back up your important data.
    </ol>
  </div>
  <div>
    <h2>Reporting Phishing</h2>
    <p>If you've received a phishing attempt, report it to the appropriate authorities, such as your organization's IT department or local law enforcement. You can also report phishing emails to the Federal Bureau of Investigation (FBI) or the Internet Crime Complaint Center (IC3).
  </div>
  <div>
    <h2>Conclusion</h2>
    <p>Phishing is a serious threat to your online security. By staying vigilant and following these best practices, you can significantly reduce your risk of falling victim to a phishing attack. Remember, if in doubt, don't click.
  </div>
  <div>
    <h2>Additional Resources</h2>
    <p>For more information on phishing and other cybersecurity topics, visit our blog or contact our support team.
  </div>
  <div>
    <h2>Contact Us</h2>
    <p>If you have any questions or need assistance, please reach out to our support team at support@phishingawareness.com.
  </div>
  <div>
    <h2>Footer</h2>
    <p>© 2023 Phishing Awareness. All rights reserved.
  </div>
</body>
</html>
```

☐ Capture Submitted Data ?

Cancel

Save Page

×

### Copy of Fake linkedin Login

HTML

☐ Capture Submitted Data ?

Save Page

**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.

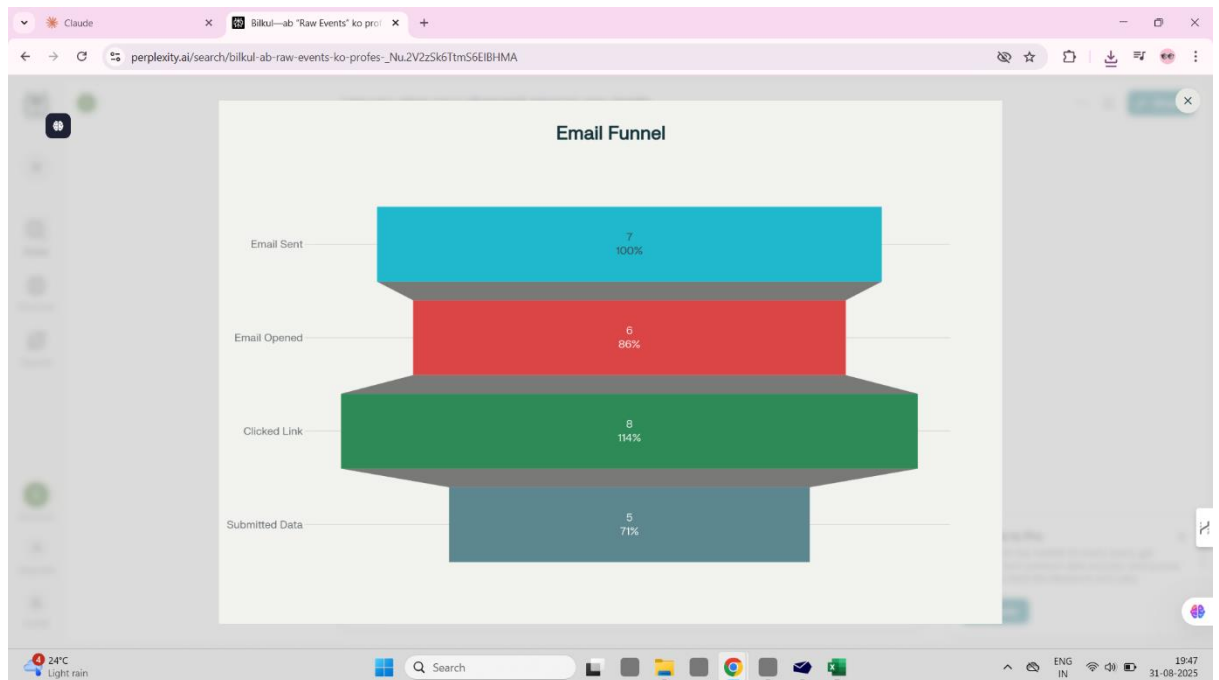
Don't show again

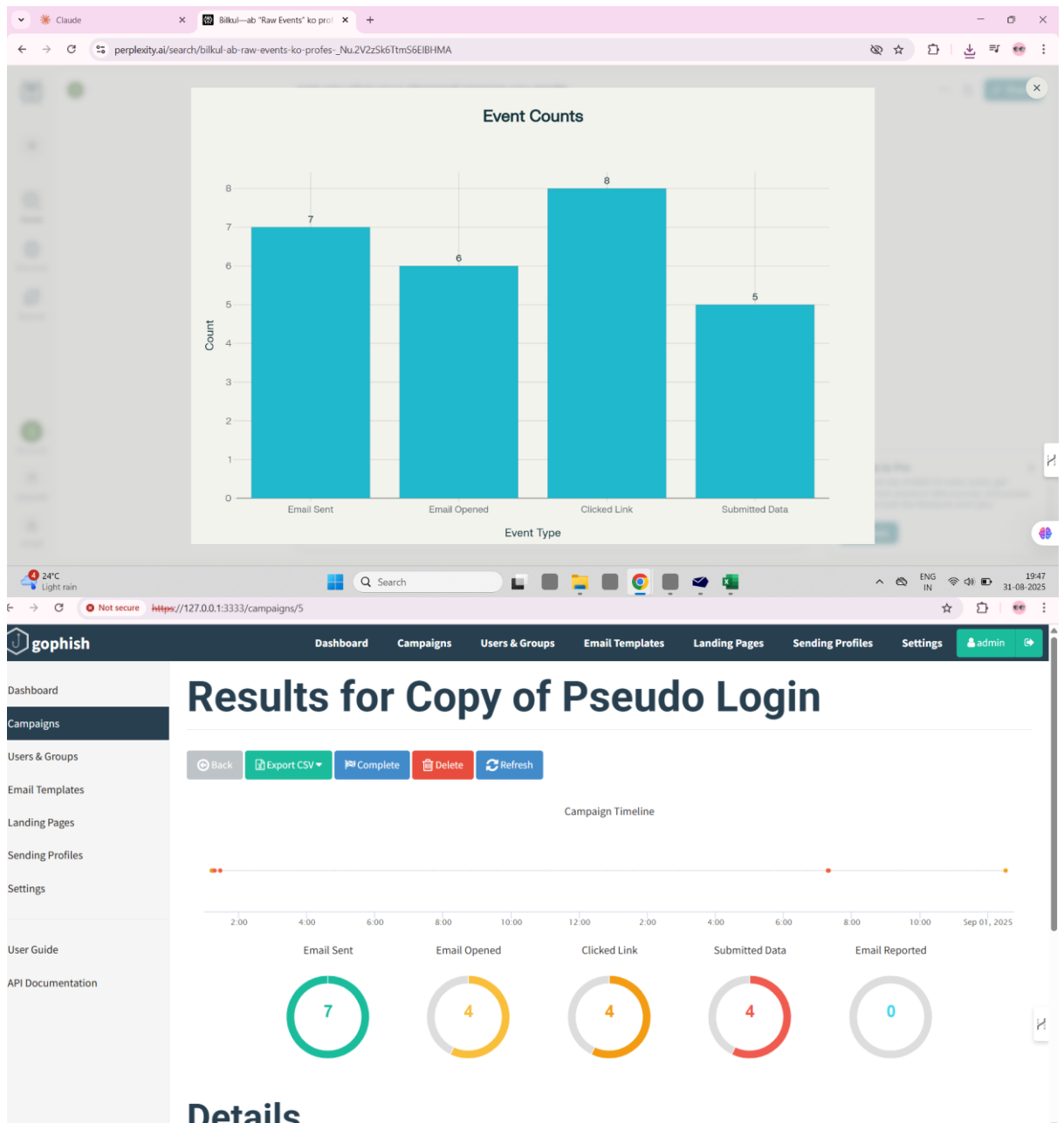
Save As...

### CSV chart of Copy of Pseudo Login

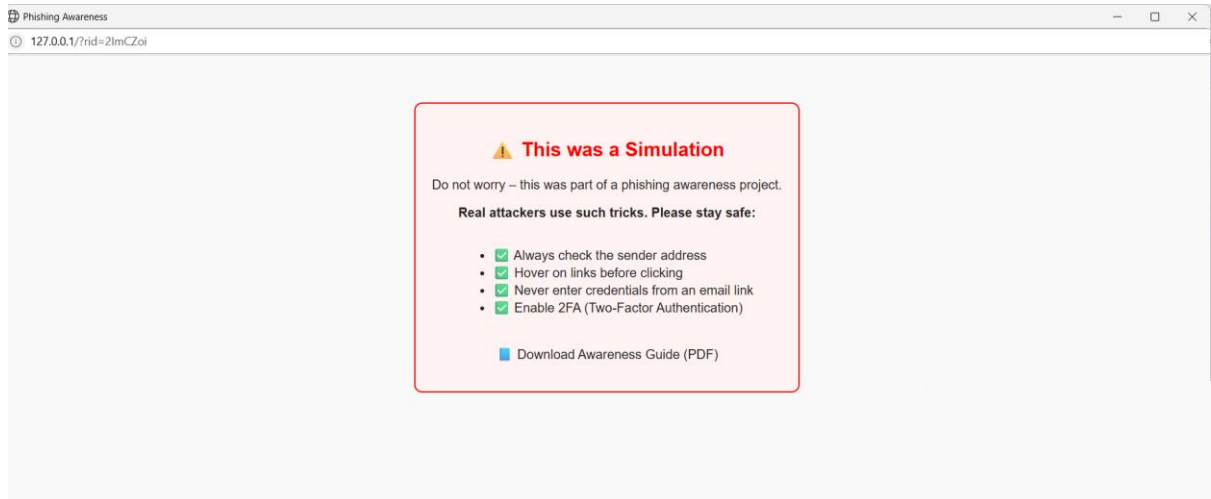
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	email	time	message	details	time IST												
2	dubey@12	2025-08-3	Clicked Lin	("payload":	2025-08-31 01:14:53.119367800+00:00												
3	dubey@12	2025-08-3	Email Oper	("payload":	2025-08-31 01:14:51.829553800+00:00												
4	dubey@12	2025-08-3	Email Sent		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@7986	2025-08-3	Clicked Lin	("payload":	2025-08-31 01:13:33.910231500+00:00												
7	lpu@7986	2025-08-3	Email Oper	("payload":	2025-08-31 01:13:32.128266+00:00												
8	lpu@7986	2025-08-3	Email Sent		2025-08-31 01:13:00.038038600+00:00												
9	lpu@7986	2025-08-3	Submitted	("payload":	2025-08-31 01:14:31.650796300+00:00												
10	sandeep3	2025-08-3	Email Sent		2025-08-31 01:12:59.860457600+00:00												
11	shivangi@	2025-08-3	Clicked Lin	("payload":	2025-08-31 19:18:24.495743800+00:00												
12	shivangi@	2025-08-3	Email Oper	("payload":	2025-08-31 19:18:23.008869700+00:00												
13	shivangi@	2025-08-3	Email Sent		2025-08-31 01:12:59.510305900+00:00												
14	shivangi@	2025-08-3	Submitted	("payload":	2025-08-31 19:18:42.436116600+00:00												
15	shyamli@1	2025-08-3	Clicked Lin	("payload":	2025-08-31 01:27:18.871000100+00:00												
16	shyamli@1	2025-08-3	Email Oper	("payload":	2025-08-31 01:27:17.123752200+00:00												
17	shyamli@1	2025-08-3	Email Sent		2025-08-31 01:12:59.921718800+00:00												
18	shyamli@1	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	vedangi@	2025-08-3	Email Sent		2025-08-31 01:12:59.796857+00:00												
21		2025-08-3	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-:

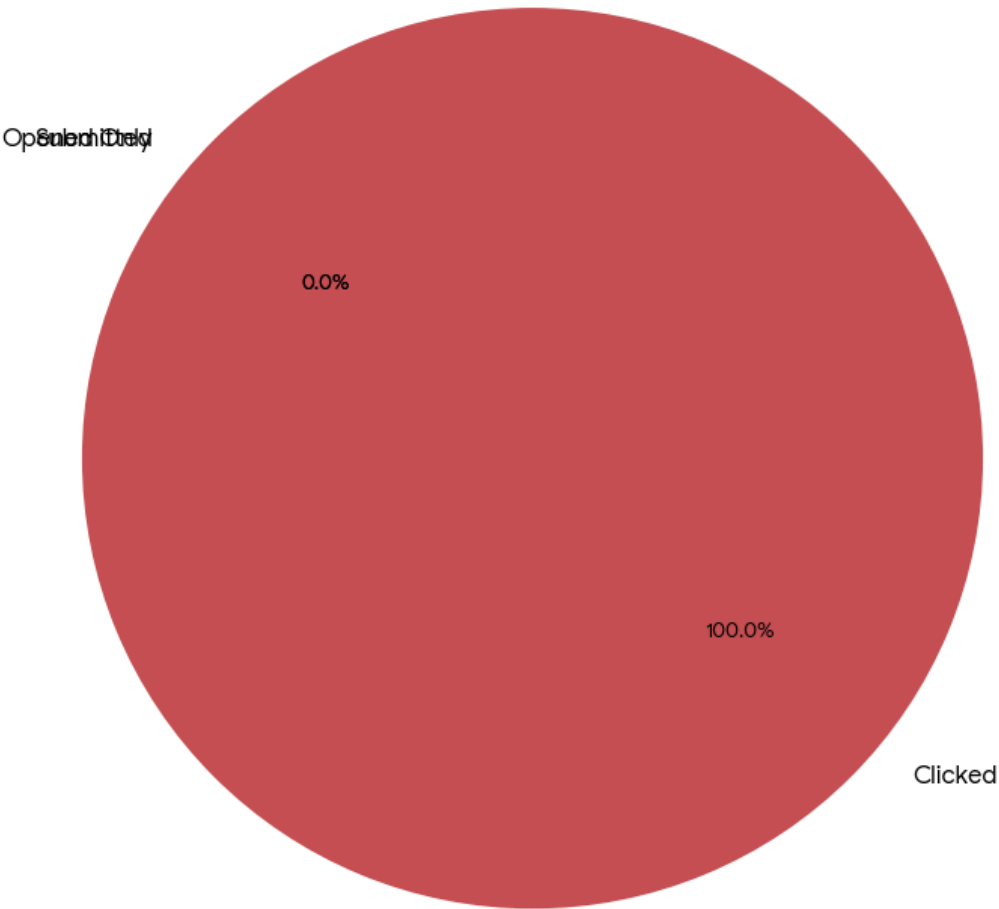


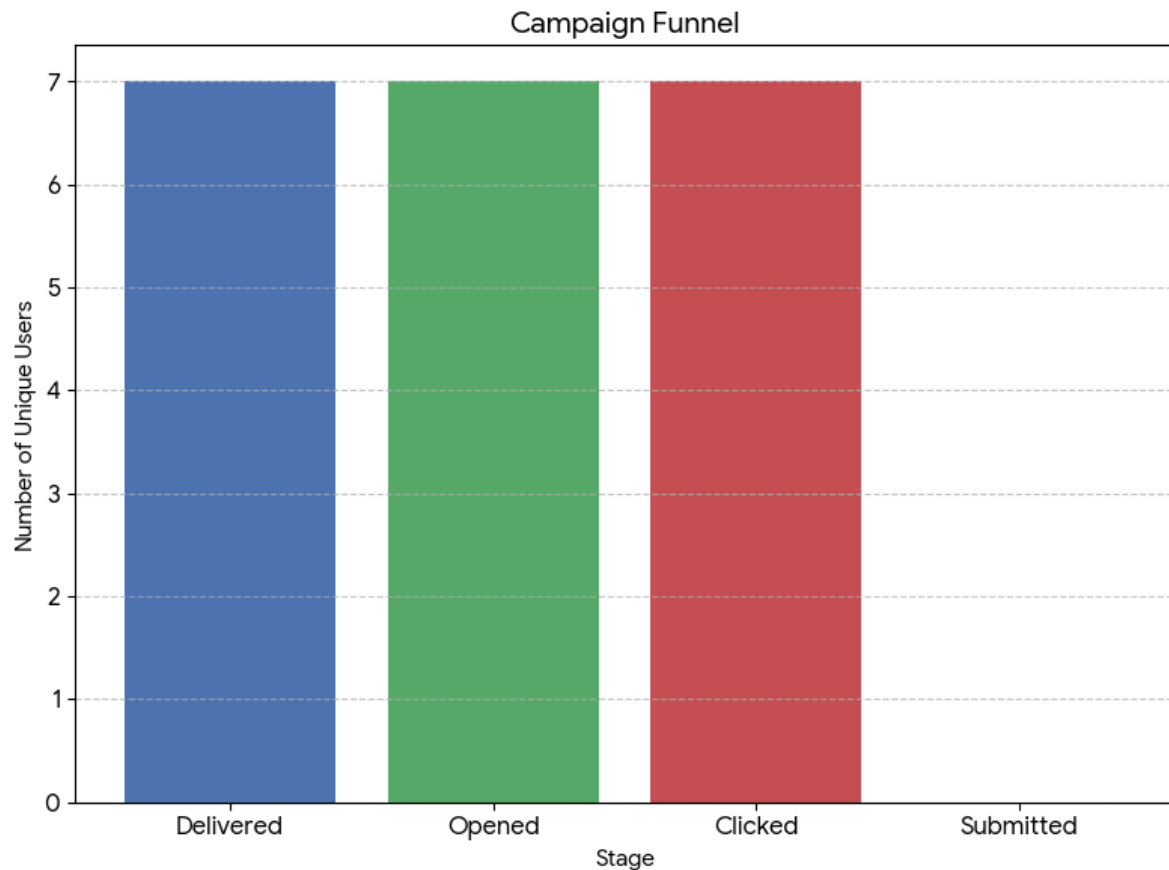


**Diagram Representation of results of Awareness Campaign**



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**.

