**SOCIAL ENGINEERING SIMULATION FOR CYBERSECURITY AWARENESS**

*Internship Project Report submitted to***INLIGHN TECH**

**Submitted by:**

**Sabnam Banu  
B.Tech, Computer Science and Engineering  
UPES, Dehradun  
Email: sabnam11sab@gmail.com**

**Under the Guidance of:**

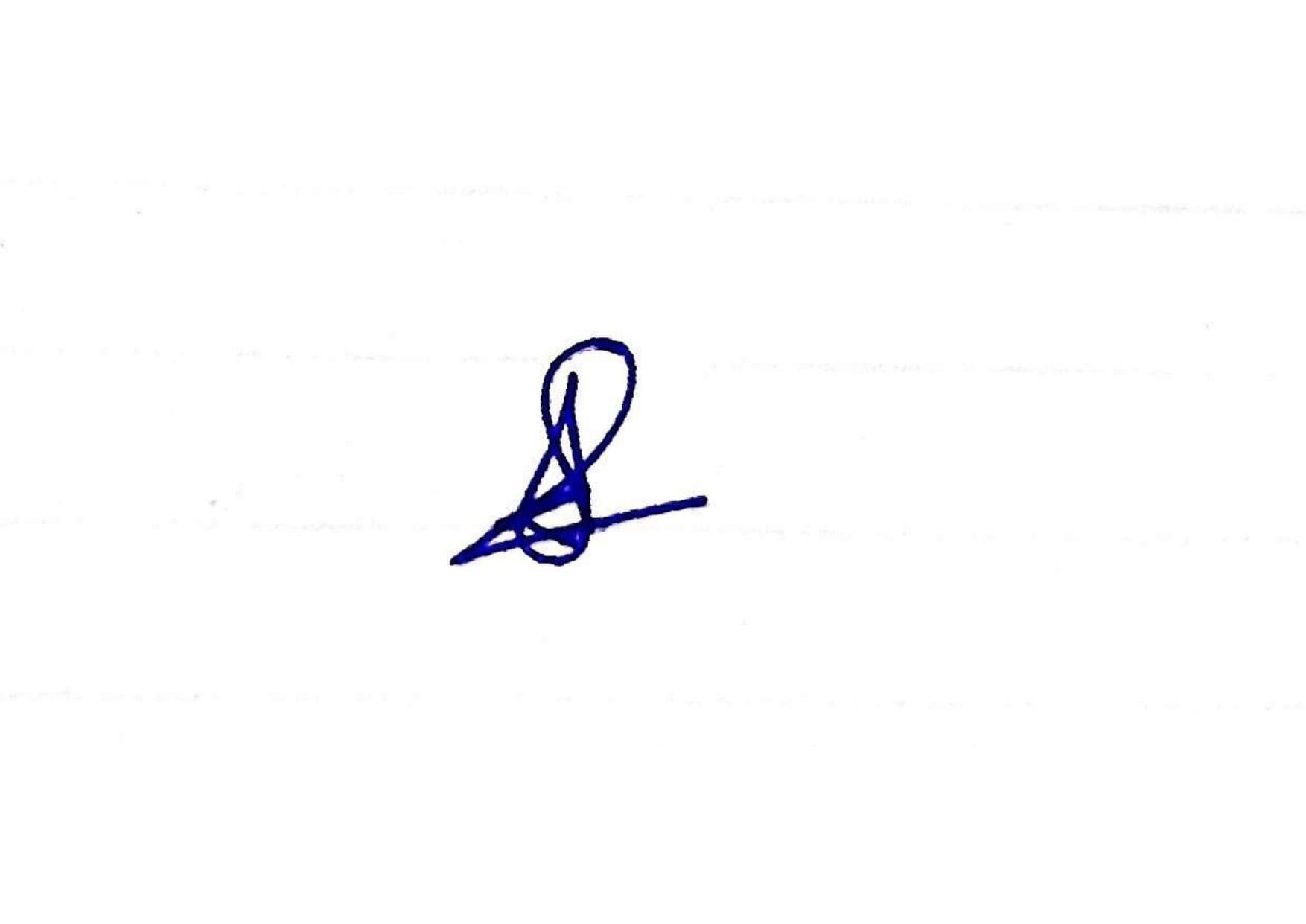
**Mr. Rishav Patel  
Mentor, Inlighn Tech**

**Duration:**

**10th September 2025 – 10th November 2025**

# ***ACKNOWLEDGMENT***

I would like to express my sincere gratitude to Inlighn Tech, my mentor Mr. Raghav Patel, and all participants for their cooperation and feedback. I also extend my heartfelt thanks to UPES, Dehradun – Department of Computer Science & Engineering, for their guidance and support during my internship journey.



Sabnam Banu

# ***ABSTRACT***

This project explores how social engineering simulations can be used to measure and improve cybersecurity awareness among users. The study involved sending a harmless phishing-style email to informed participants and analyzing their reactions. The results highlight that while awareness levels were generally high, emotional and urgency-based triggers still led some participants to unsafe actions, emphasizing the importance of continuous awareness training.

# TABLE OF CONTENTS

Contents

[***ACKNOWLEDGMENT*** 2](#_Toc211990817)

[***ABSTRACT*** 2](#_Toc211990818)

[TABLE OF CONTENTS 3](#_Toc211990819)

[1. INTRODUCTION 4](#_Toc211990820)

[3. TOOLS & TECHNOLOGIES USED 4](#_Toc211990821)

[4. METHODOLOGY 5](#_Toc211990822)

[5. RESULTS AND ANALYSIS 8](#_Toc211990823)

[6. FINDINGS 9](#_Toc211990824)

[7. RECOMMENDATIONS 9](#_Toc211990825)

[8. CONCLUSION 10](#_Toc211990826)

[9. REFERENCES 10](#_Toc211990827)

[10. APPENDIX 10](#_Toc211990828)

# 1. INTRODUCTION

In the modern digital era, cybersecurity threats are not just technical — they often exploit human psychology.  
**Social engineering** is the art of manipulating people into revealing sensitive information or performing unsafe actions.  
This project demonstrates a **phishing-style awareness simulation** designed to educate and assess users’ responses.  
 **Key Idea:**  
Realistic, harmless simulations help users recognize phishing red flags in a safe environment.

2. OBJECTIVES  
**Primary Goals:**

* To design an ethical phishing-style email for awareness testing.
* To simulate a real-world social engineering scenario.
* To analyze participant behavior and awareness levels.
* To propose practical recommendations for cybersecurity training.

# 3. TOOLS & TECHNOLOGIES USED

| **Tool** | **Purpose** |
| --- | --- |
| Google Forms | Collecting feedback responses |
| Google Sites | Hosting safe landing page |
| Mailmeteor | Sending emails to participants |
| Python (pandas, matplotlib) | Data processing and visualization |
| Canva / MS Word | Documentation & design |

# 4. METHODOLOGY

**Step 1: Email Simulation Design**

* Created a phishing-style email using a professional tone and official-like language.
* The subject line read: *“Account Security Alert – Verification Required”*.
* The email included a link to a harmless landing page (no credentials collected).

**Step 2: Landing Page Setup**

* Hosted on Google Sites:  
  <https://sites.google.com/view/secure-awareness-info/home>
* The page clearly stated the simulation purpose after the user clicked the link.

**Step 3: Participant Awareness**

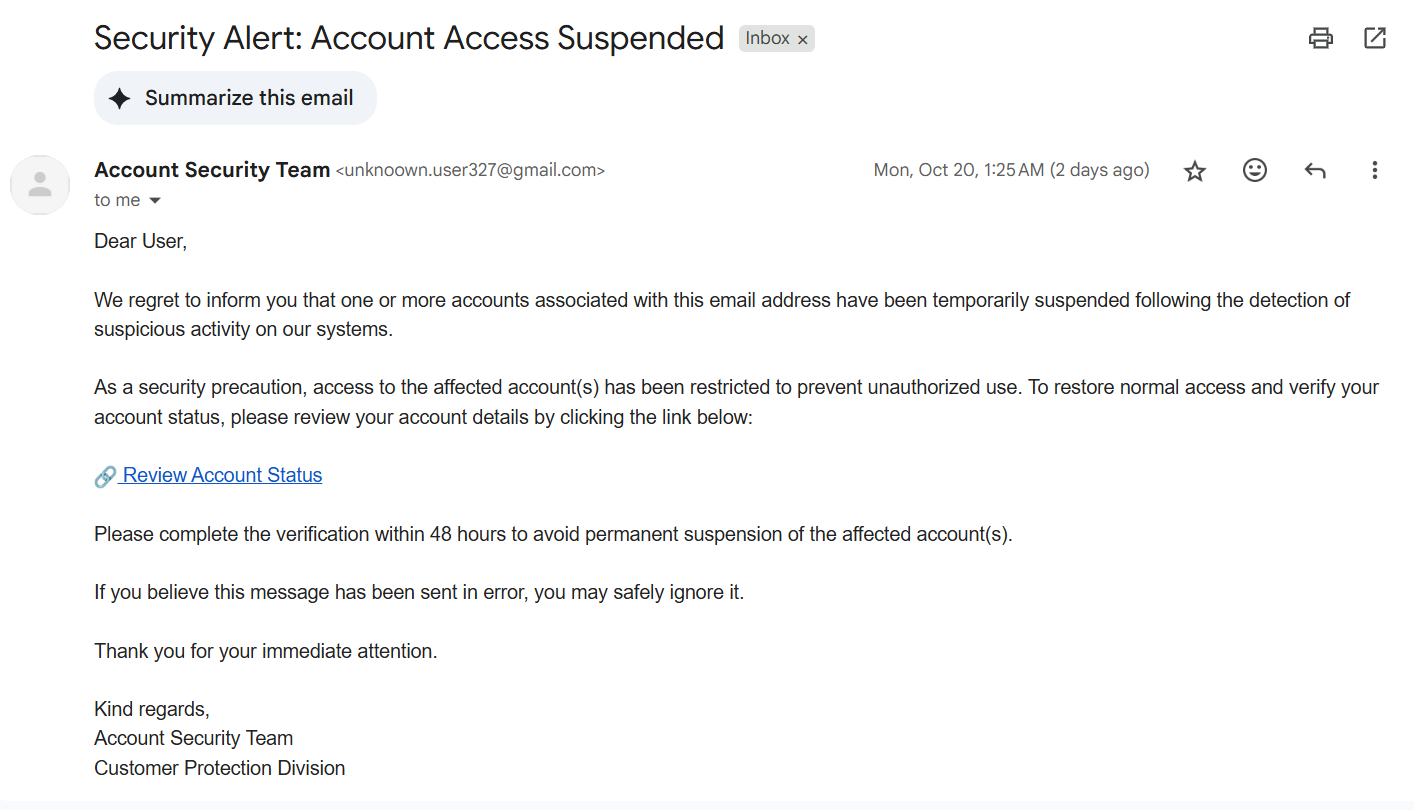
* Participants (family/friends) were pre-informed that the activity was for research and educational purposes.

**Step 4: Feedback Form**

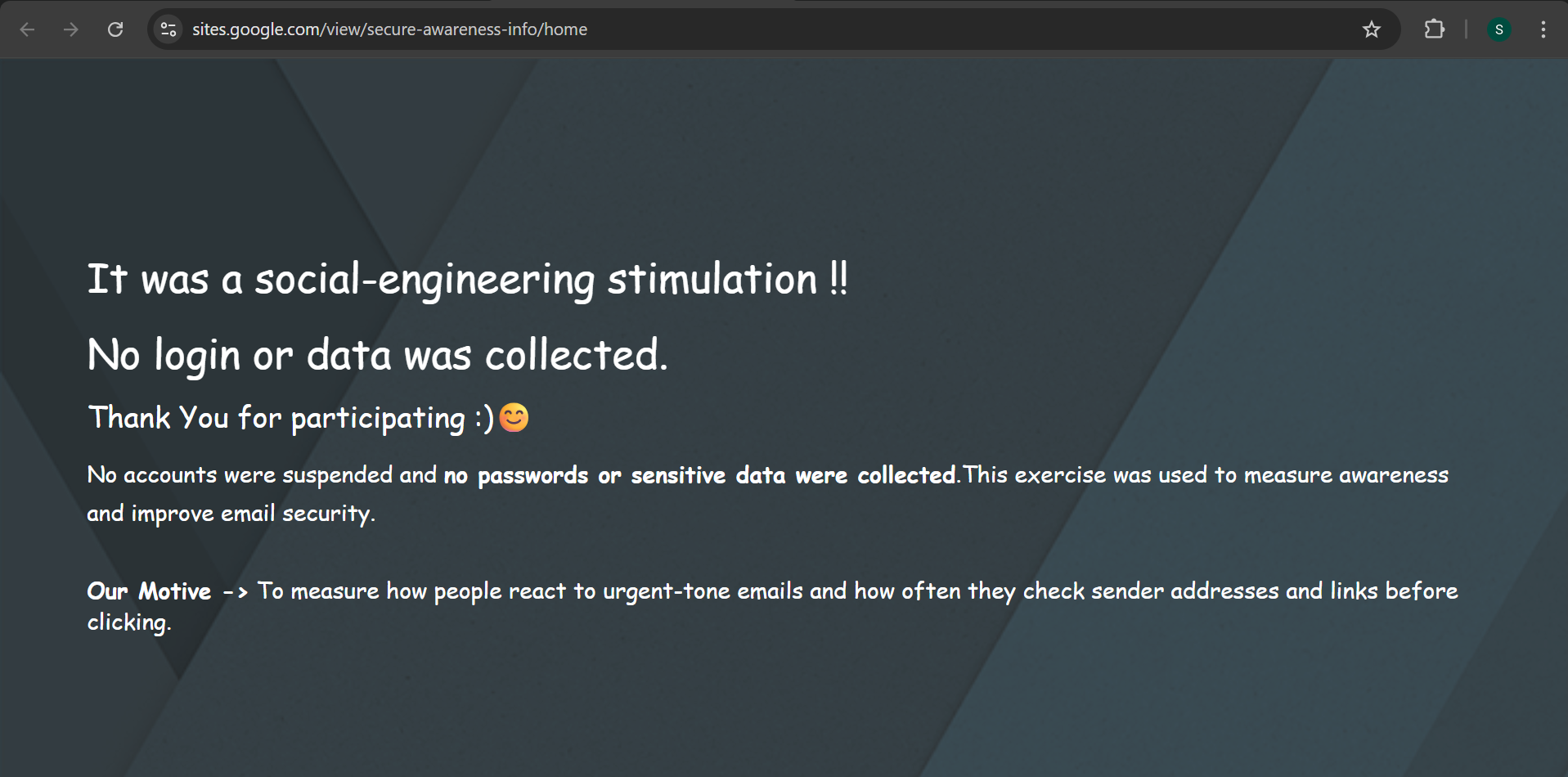
* A Google Form was shared to record user behavior and perceptions:  
  <https://forms.gle/kEp61zcU9wqVBipP8>

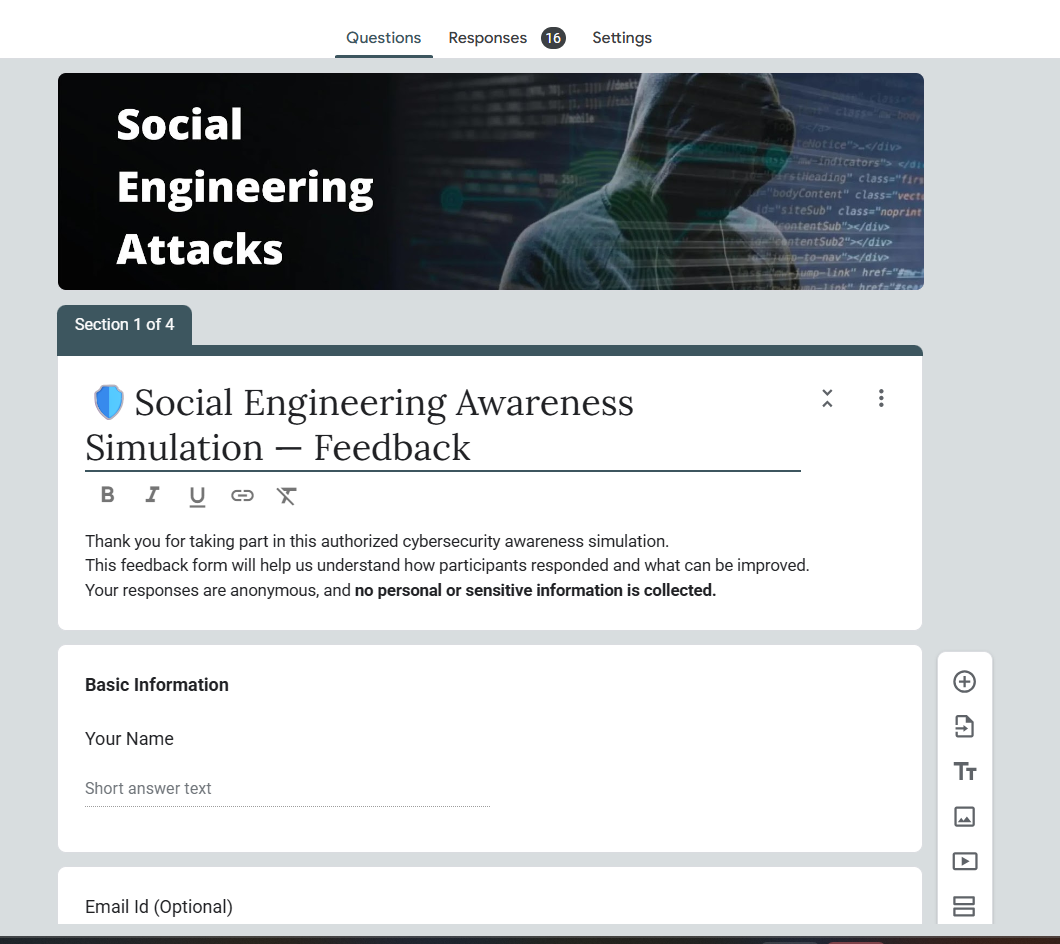
**Step 5: Data Analysis**

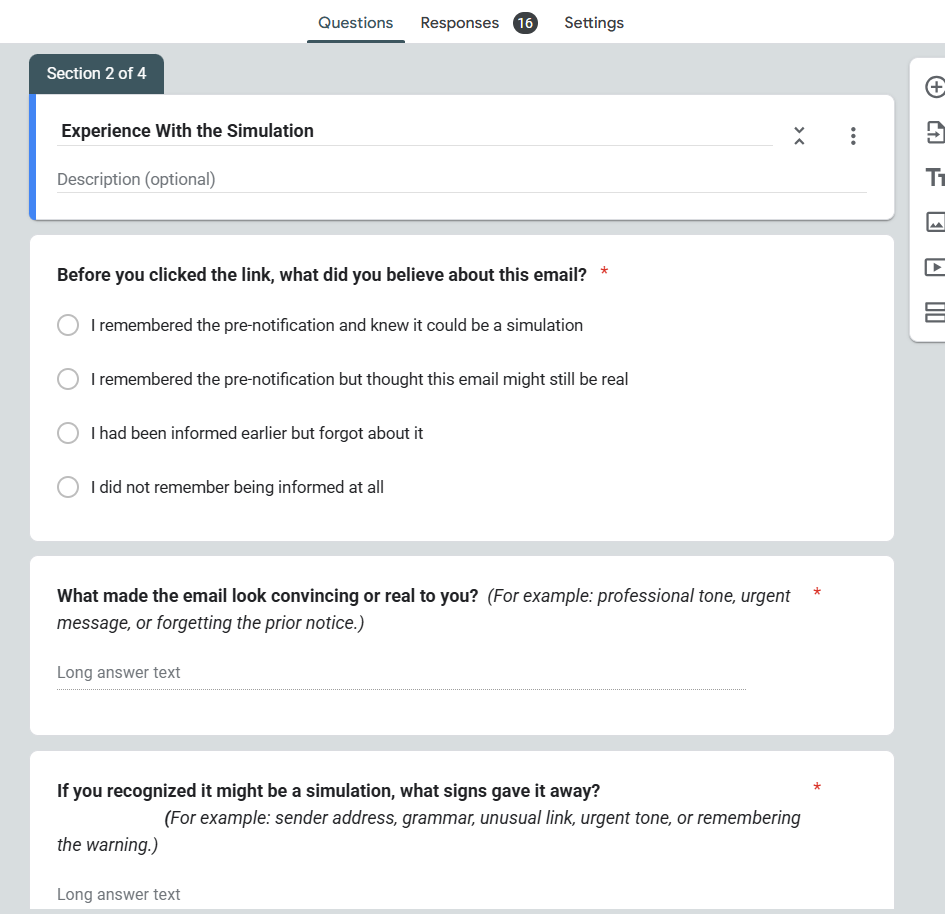
* Responses were analyzed in Google Sheets and Python.
* Metrics: awareness level, realism rating, and recognition of red flags.

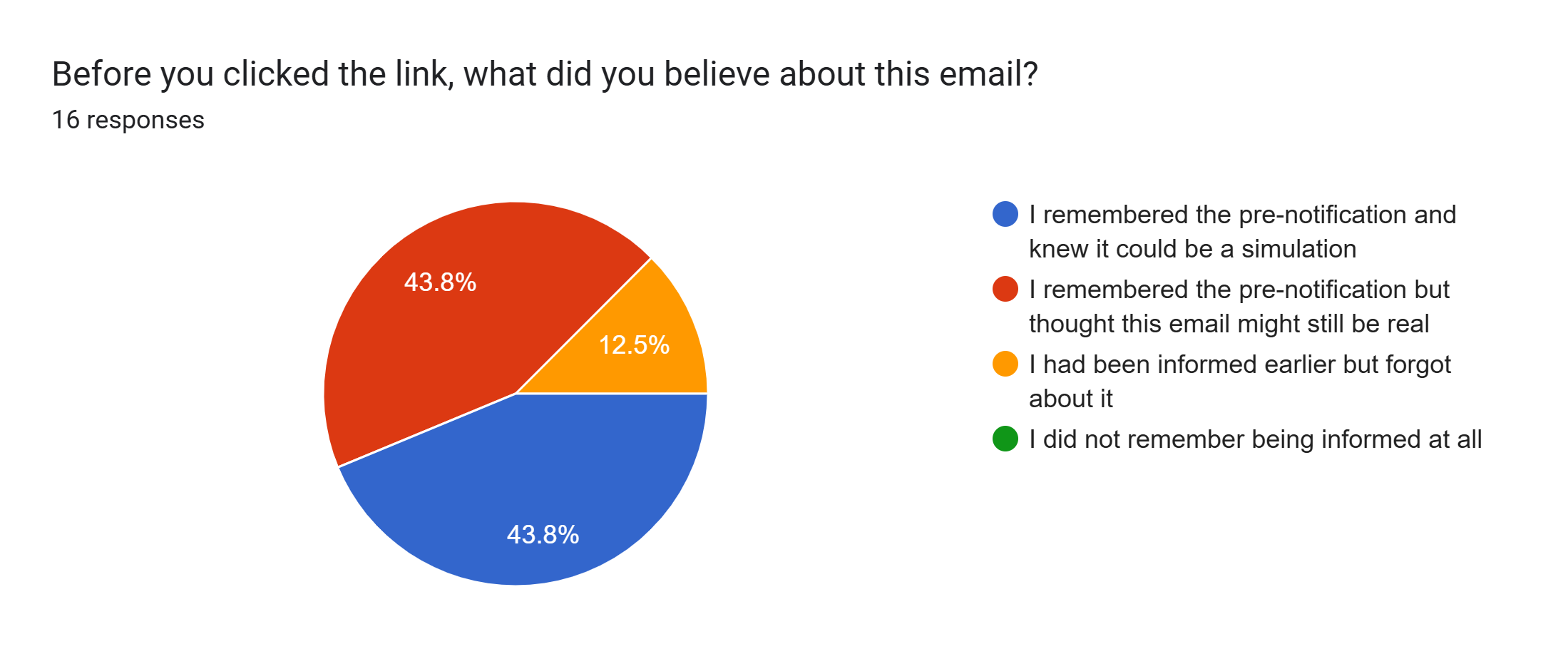
**Fake Email Simulation =>**

**Landing Page =>**

****

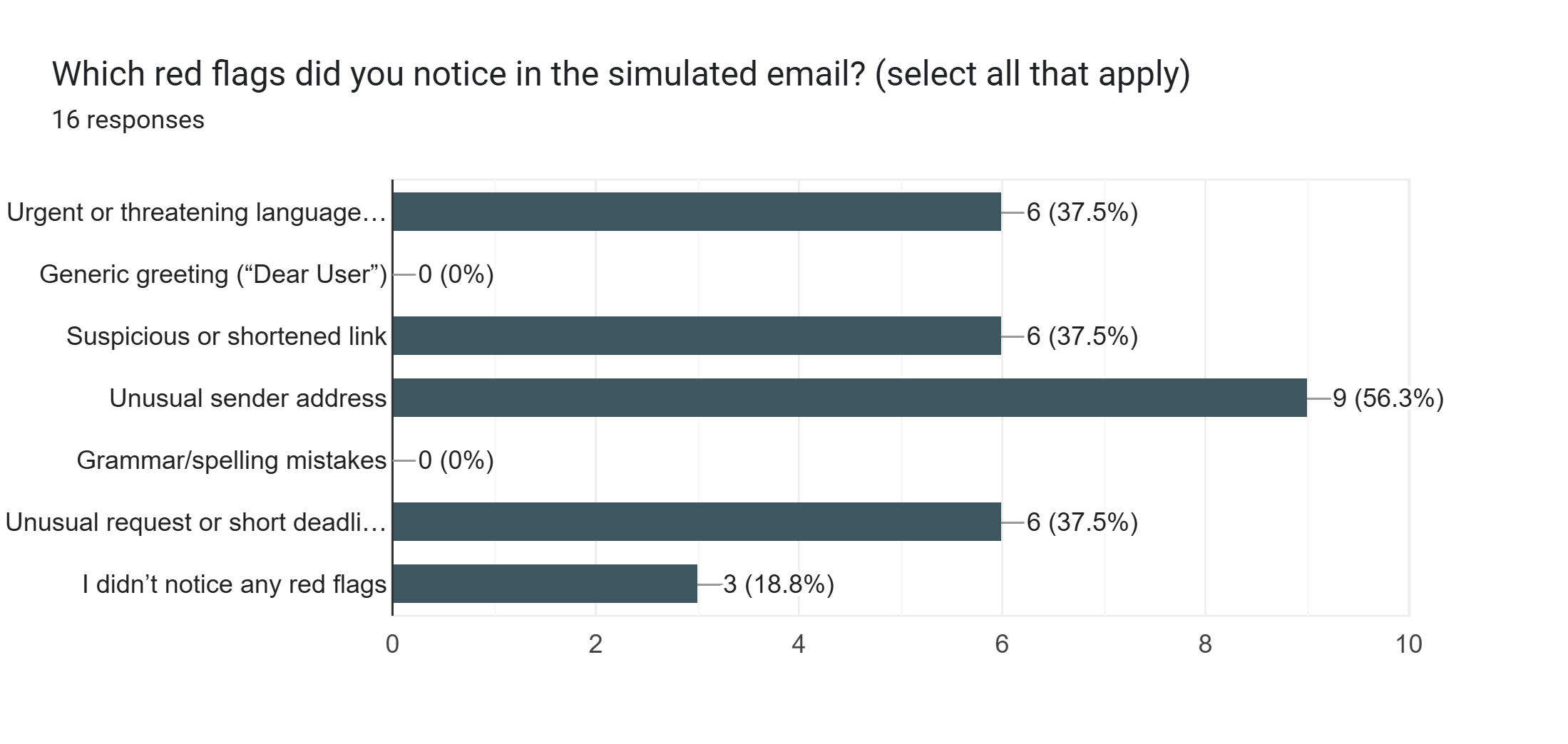
**Feedback Form Interface :**

****

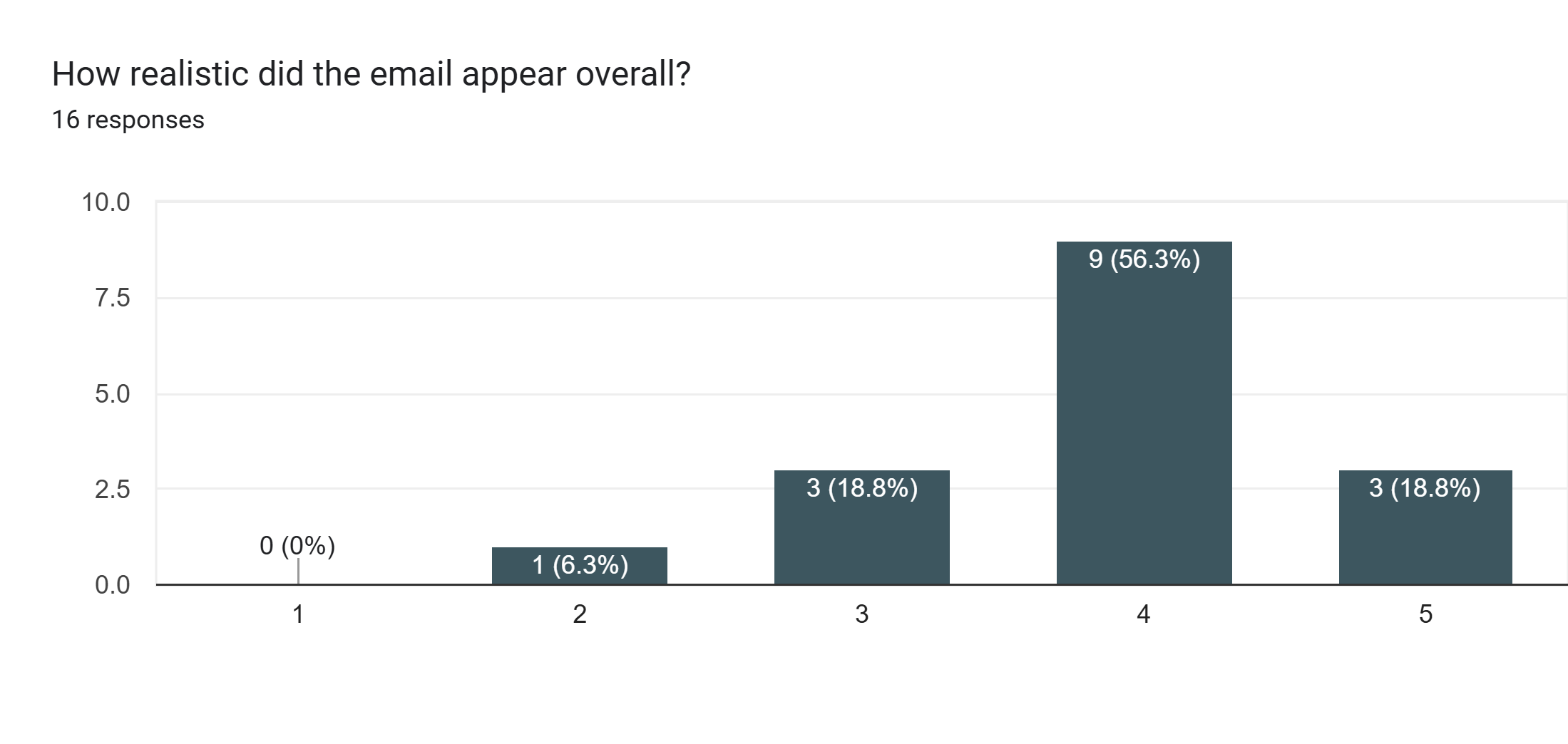
**– Summary of Awareness Level :**  


# 5. RESULTS AND ANALYSIS

* **Total Participants:** 16
* **70%** checked sender details before clicking.
* **25%** clicked the link without verifying.
* **Common red flags noticed:** fake sender, suspicious link, urgency tone.
* **Average realism score:** 4.1 / 5
* **General awareness level:** High.



**Red Flags Noticed by Participants**



**Email Realism Rating Results**

# 6. FINDINGS

* Participants demonstrated good theoretical awareness.
* Some users still responded impulsively under time pressure.
* Awareness alone doesn’t prevent risky clicks — *habitual verification* is key.
* Social simulations are an effective awareness reinforcement strategy.

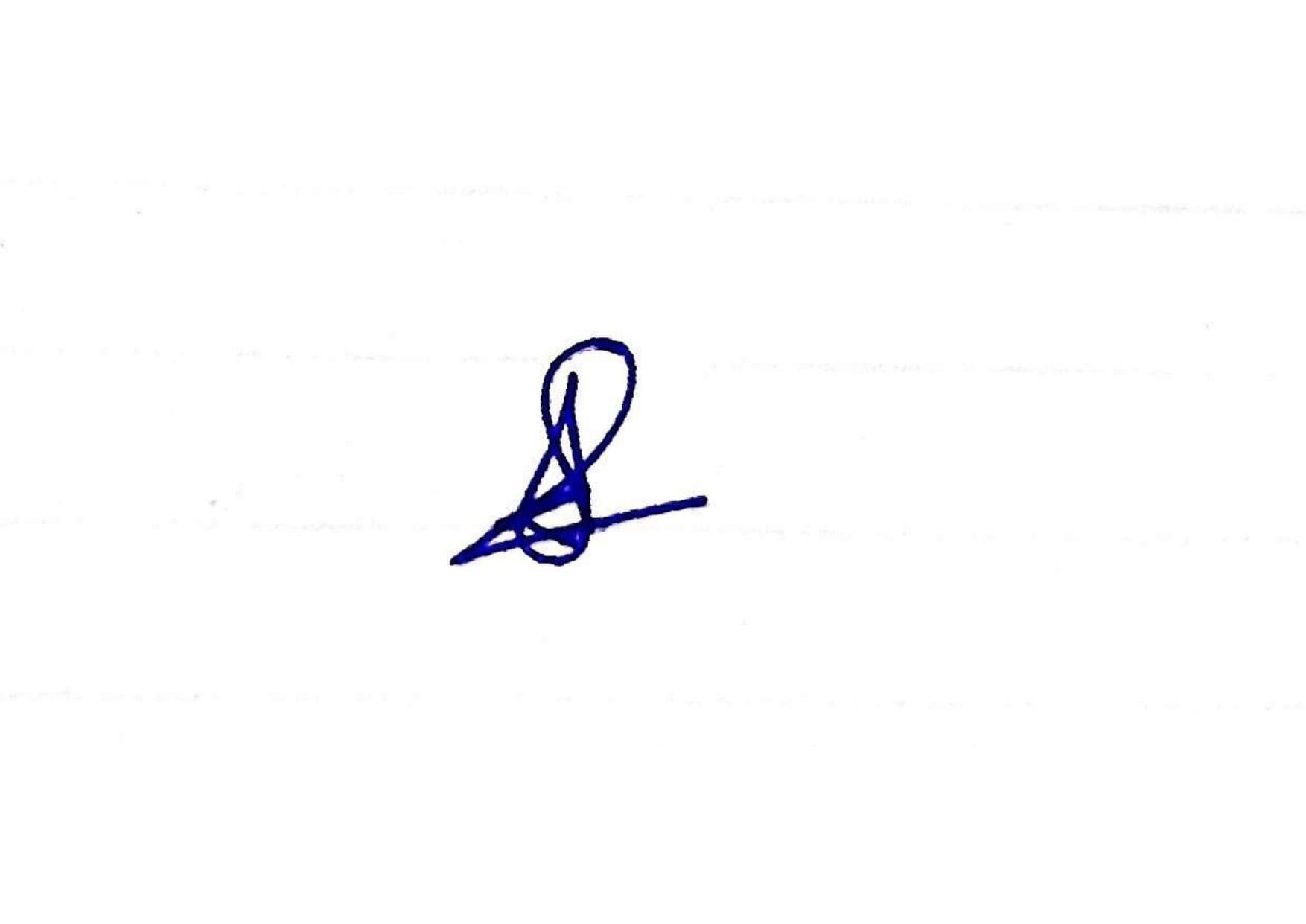
# 7. RECOMMENDATIONS

* Conduct periodic phishing simulation exercises.
* Introduce short cybersecurity awareness modules.
* Encourage “Think Before You Click” training.
* Promote clear communication from IT/security teams.

# 8. CONCLUSION

The **Social Engineering Simulation for Cybersecurity Awareness** successfully demonstrated how simulated phishing can help identify human vulnerabilities and strengthen user awareness.  
Participants became more alert and cautious after realizing how realistic phishing emails can appear.  
Continuous simulations and training are crucial to build lasting cybersecurity awareness.

**Sabnam Banu**



# 9. REFERENCES

* OWASP Foundation – Phishing Awareness Guide
* Mailmeteor Official Documentation
* Google Forms & Google Sites User Guides
* Python (pandas, matplotlib) Documentation
* Academic Research: Human Factors in Cybersecurity

# 10. APPENDIX

**Links:**

* **Feedback Form:** <https://forms.gle/kEp61zcU9wqVBipP8>
* **Landing Page:** <https://sites.google.com/view/secure-awareness-info/home>

**Attachments:**

* Screenshots of Email, Landing Page, Google Form Summary, Charts.
* CSV data file (feedback responses summary).

[Social Engineering Simulation Feedback (Responses) - Form Responses 1 (1).csv.xlsx](https://1drv.ms/x/c/fb28405ced462bfb/EURusc6m025Pp31448w6jkQB0-nZr8LZwHEaT0irdhR_9g?e=WgzcyA)