Major Project

"Phishing Awareness Simulation Using Social Engineering Techniques"

---

1. Introduction

Phishing attacks are among the most widespread cybersecurity threats today, targeting human psychology rather than system vulnerabilities. Attackers impersonate trusted entities (banks, IT departments, delivery services, etc.) to trick users into revealing credentials, financial information, or personal data. This project simulates a phishing campaign in a **controlled, ethical, consent-based environment** to study:

- How phishing attacks are structured
- How users respond to them
- How awareness can be improved

The project avoids any harmful activity and focuses on **education and behavioural analysis**.

---

2. Problem Statement

Humans remain the weakest link in cyber defense. Many users still fall for phishing emails because they lack awareness of social engineering techniques. This project aims to **simulate a phishing scenario**, collect safe response metrics, and provide recommendations to help users differentiate between legitimate and malicious communications.

---

3. Project Objectives

1. **Understand common phishing techniques** (email spoofing, fake login pages, malicious links).

2. **Design a realistic but harmless phishing email template** (e.g., fake password reset).
3. **Create a demonstration login page** using HTML/CSS (no data stored).
4. **Conduct a controlled phishing simulation** on a small group with informed consent.
5. **Measure user behavior**—click rates, report rates, suspicious link recognition.
6. **Develop countermeasures and awareness guidelines** to reduce susceptibility to future attacks.

---

4. Research on Common Phishing Techniques

A. Email-Based Phishing

- Spoofed “From” addresses
- Urgency or fear messages (“Your account will be locked”)
- Fake links (URL masking, lookalike domains)
- Suspicious attachments

B. Spear Phishing

- Personalized attacks targeting specific individuals
- Uses name, role, company information

C. Whaling

- Targets high-level executives
- Involves fake invoices, business email compromise (BEC)

D. Fake Websites / Clone Pages

- Exact replicas of login portals (Google, Office 365, banking sites)
- Use lookalike domain names

E. Social Engineering Techniques Used

- Authority pressure (“Admin Notice”)

- Scarcity (“Reset password in 4 hours”)
- Trust exploitation (fake notifications from known brands)
- Curiosity (“You have 5 unread messages”)

---

5. Designing the Phishing Simulation

A. Ethical Guidelines

Before conducting the simulation:

- Obtained **informed consent** from participants.
- Informed them it is a **controlled educational exercise**.
- No personal data was collected or stored.

---

6. Fake Email Template (Harmless Simulation)

Subject: ***Urgent Verification Required for Your Account***

Body:

Dear User,

Our security system detected unusual activity on your account.

For your safety, please verify your account immediately.

Click here to verify your account:

https://sansy-k27.github.io/Index/

This request will expire in 4 hours.

IT Support Team

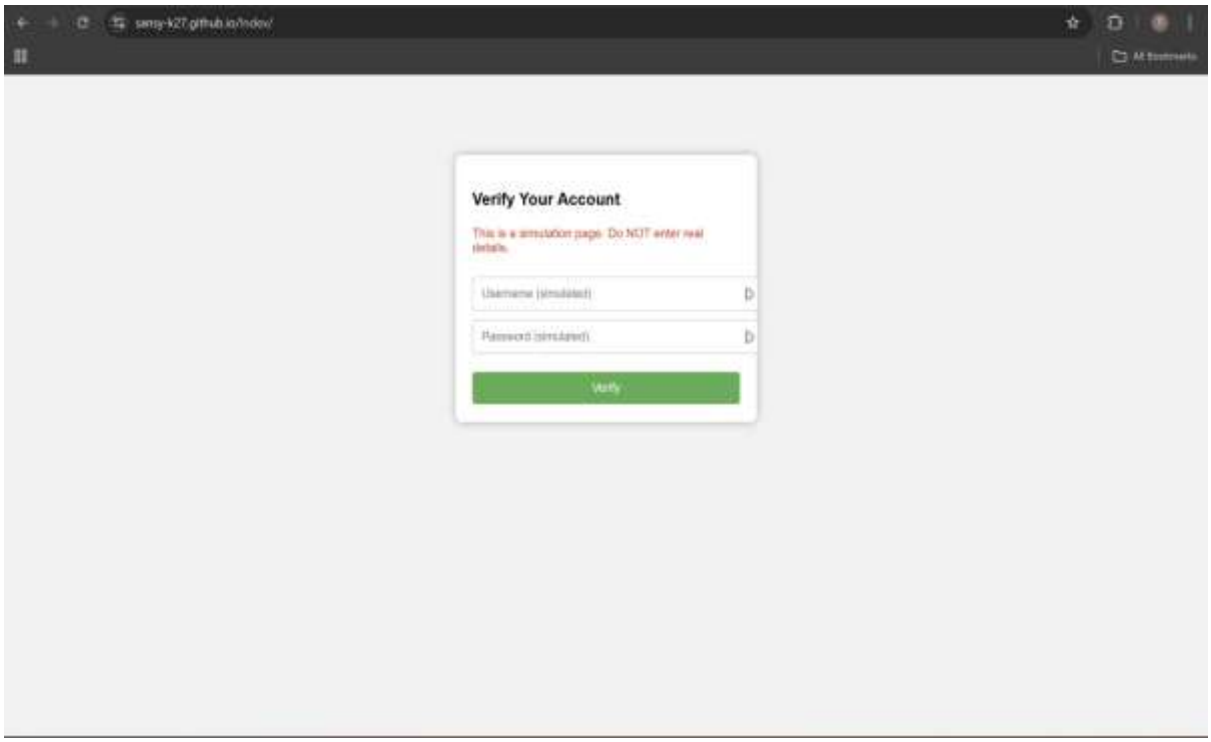
Phishing Markers Included on Purpose

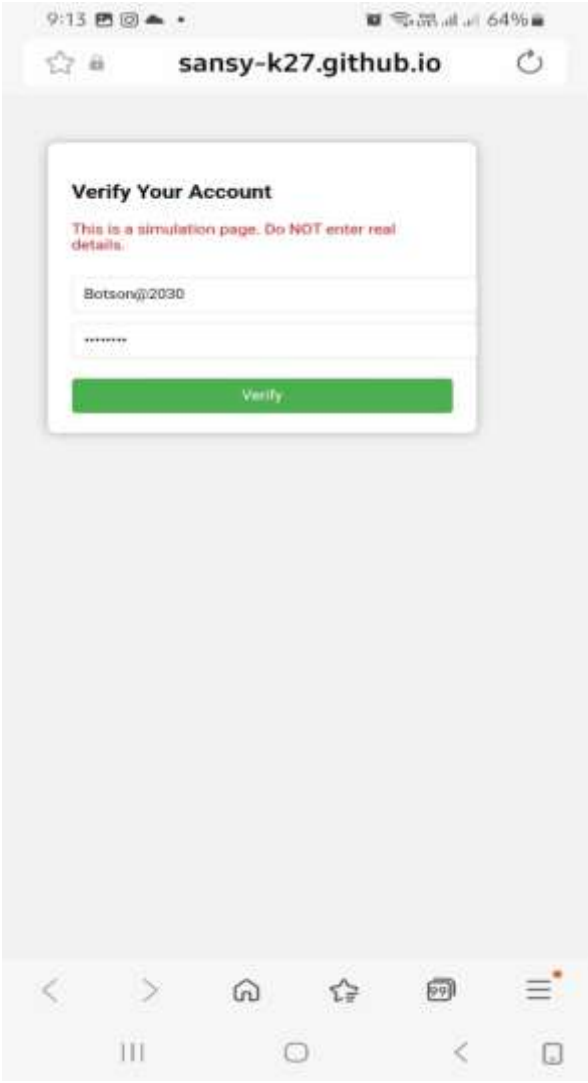
- Urgent tone

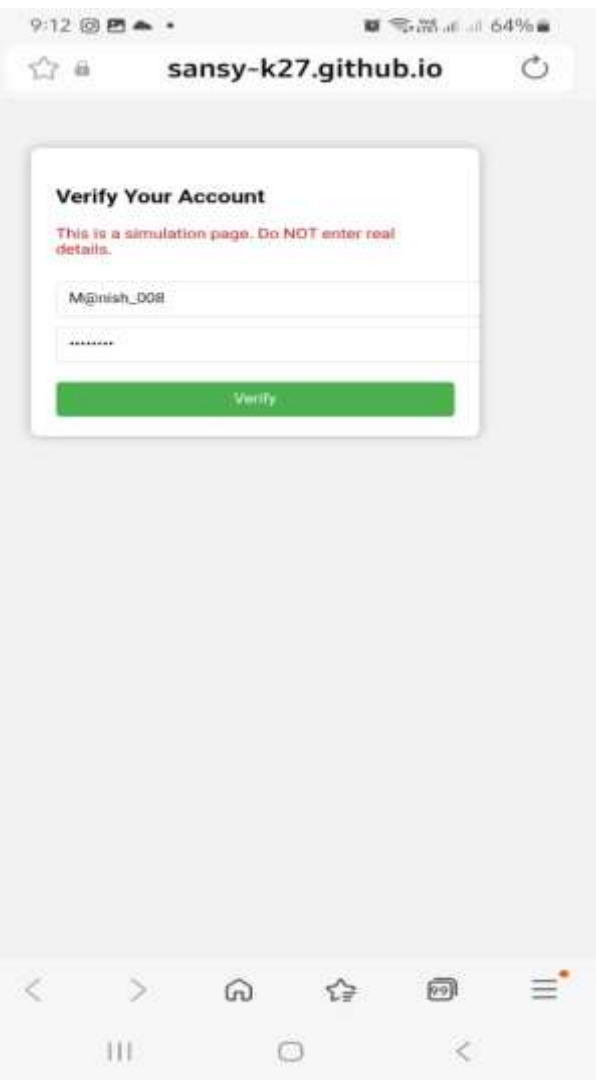
- Fake but believable brand language
- Link to demonstration page

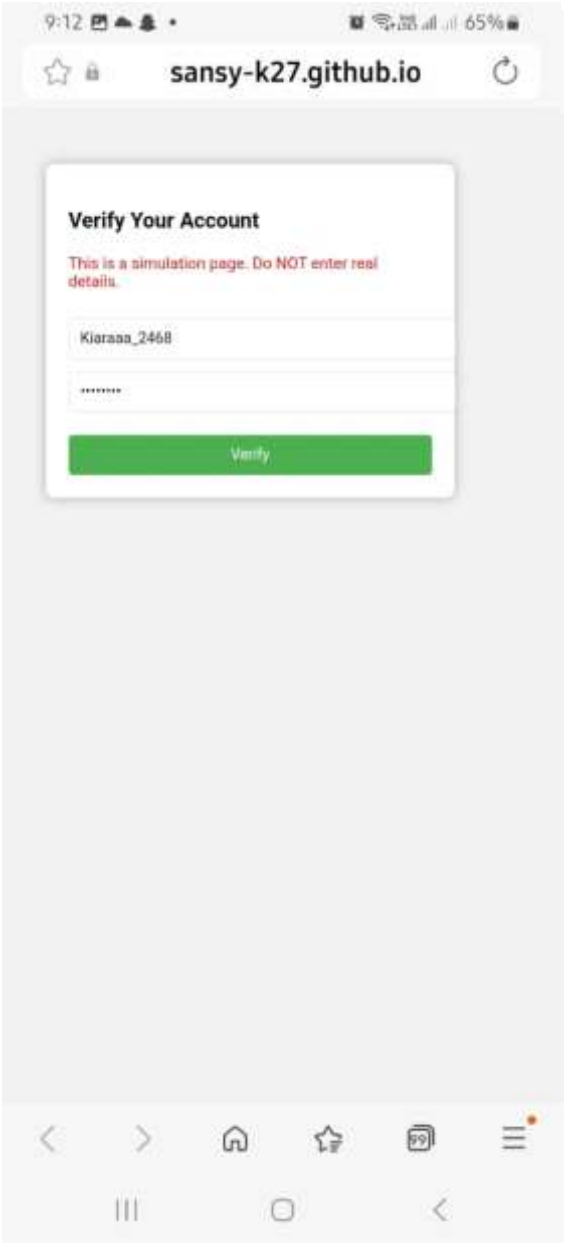
---

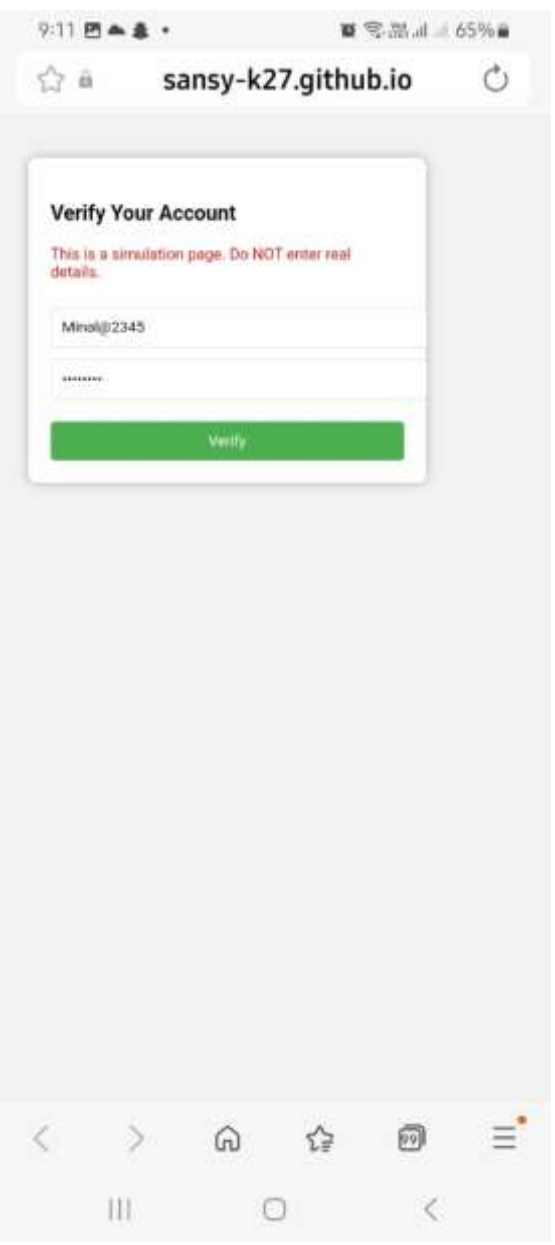
7. Creating a Fake Login Page

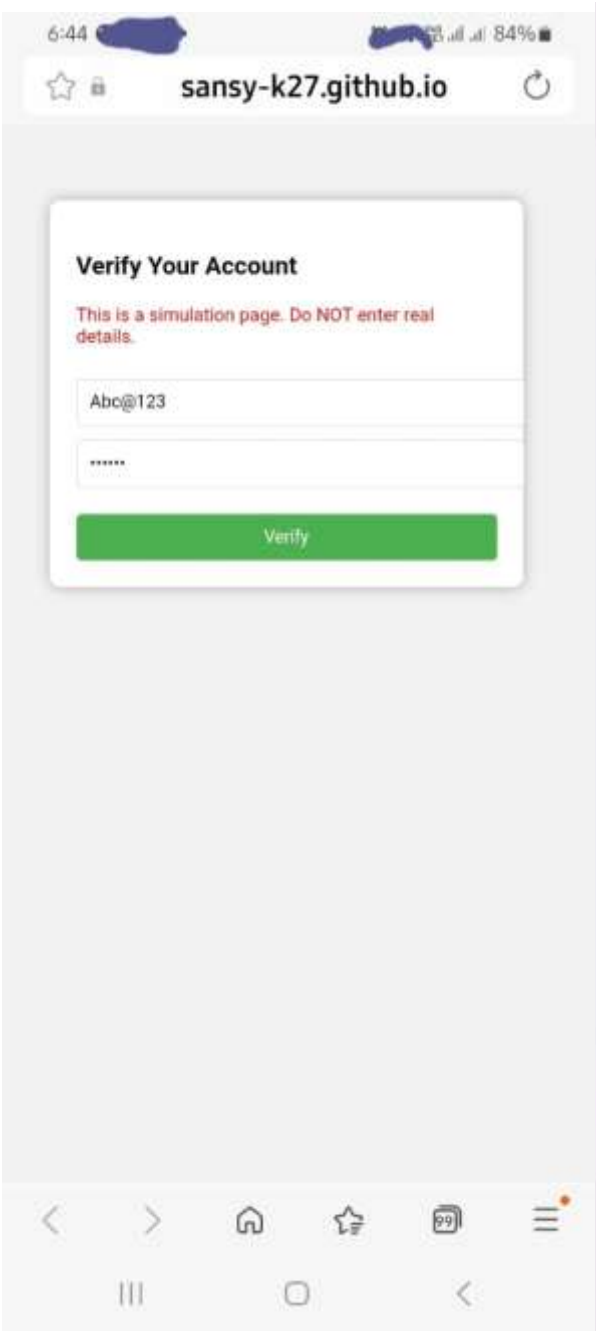


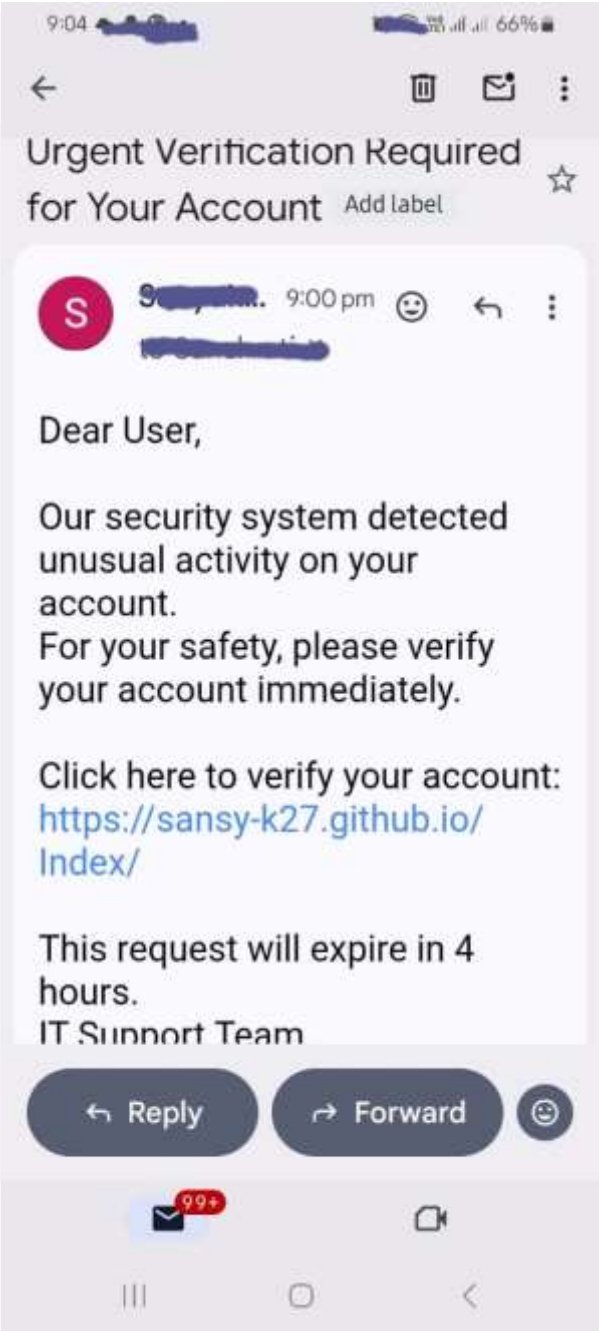

9:13
64%
sansy-k27.github.io
Verify Your Account
This is a simulation page. Do NOT enter real details.
Botson@2030
Verify

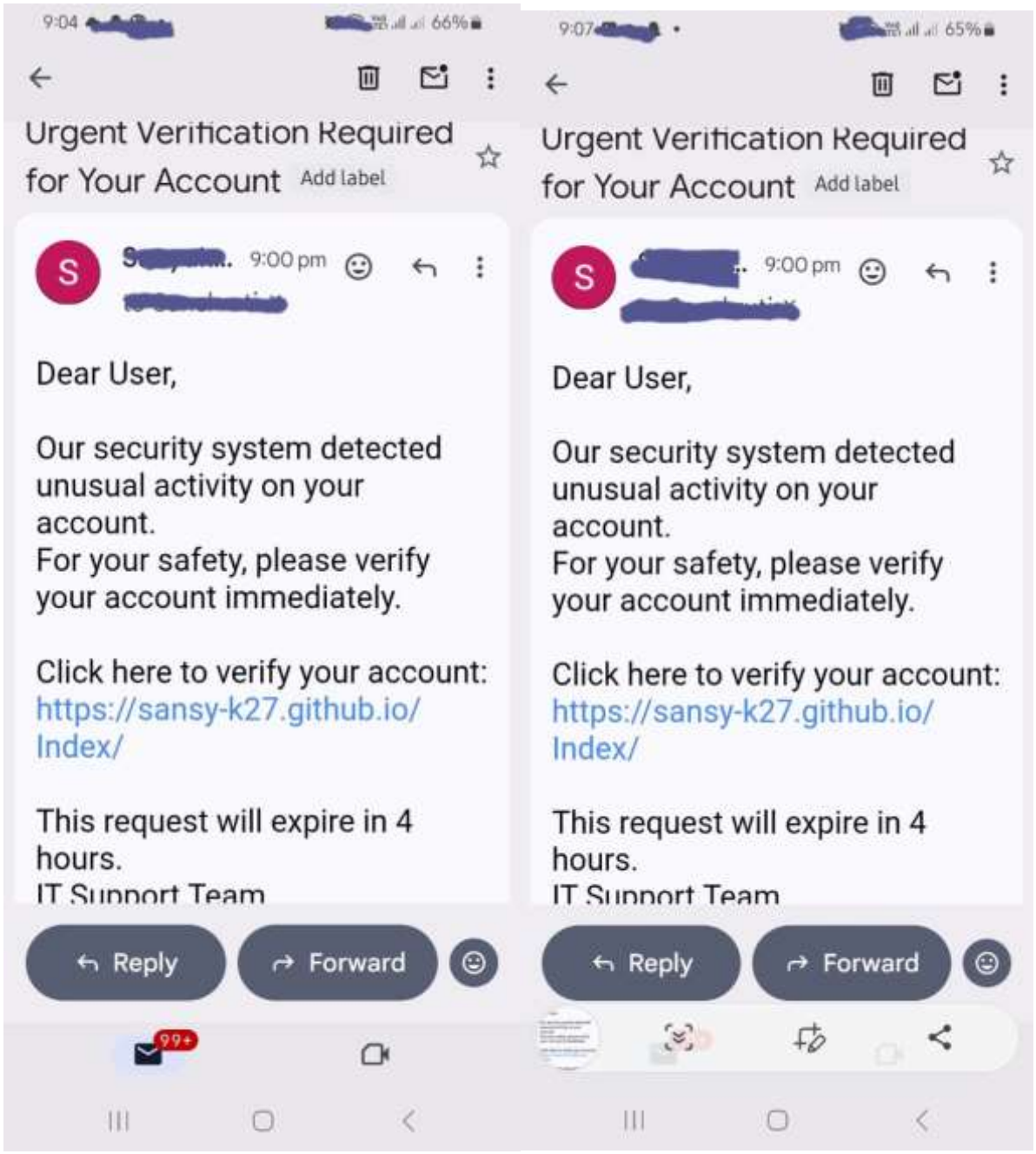

9:12
64%
sansy-k27.github.io
Verify Your Account
This is a simulation page. Do NOT enter real details.
M@nish_008
Verify

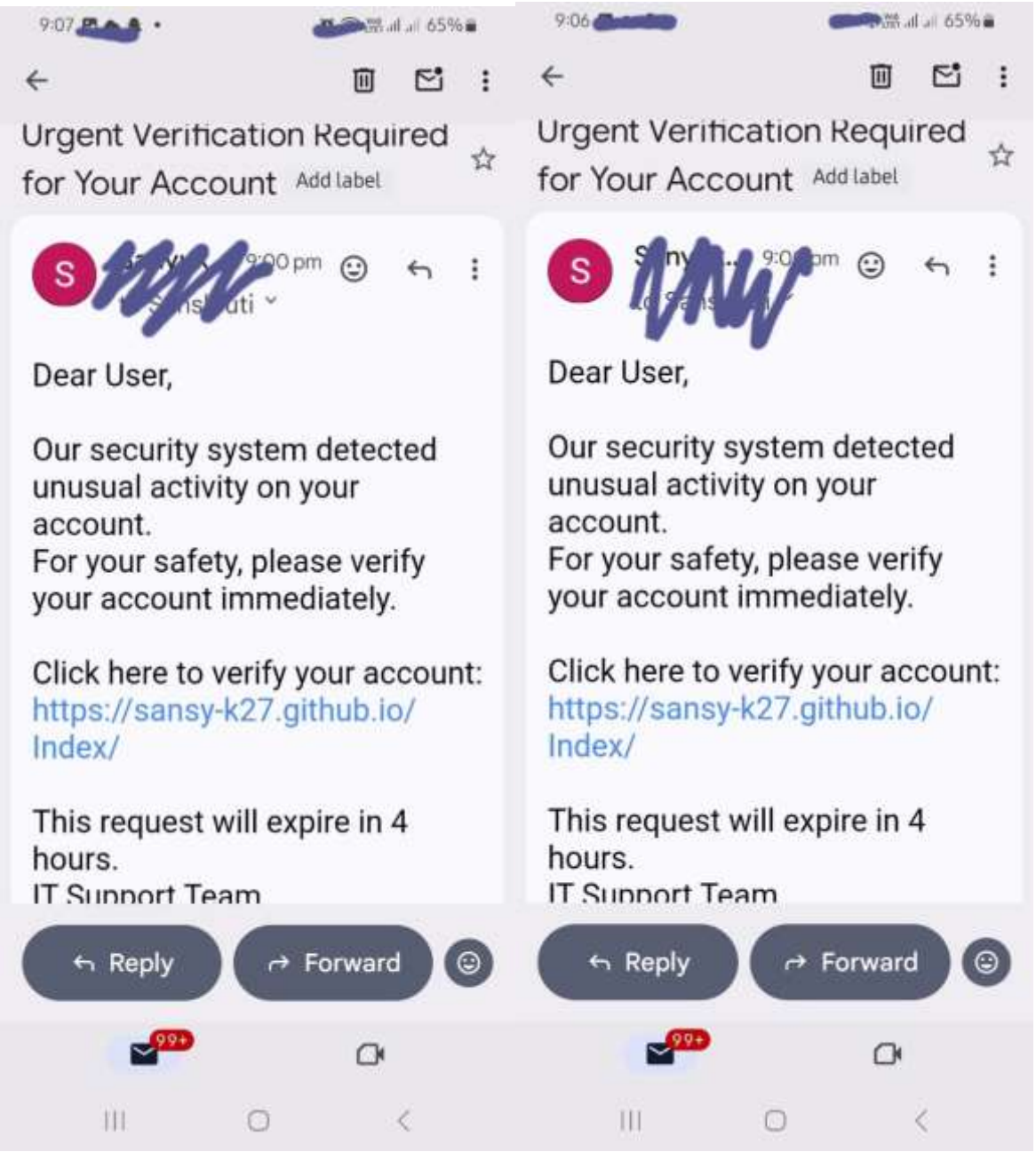

9:12
65%
sansy-k27.github.io
Verify Your Account
This is a simulation page. Do NOT enter real details.
Kiaraaa_2468
Verify


9:11
65%
sansy-k27.github.io
Verify Your Account
This is a simulation page. Do NOT enter real details.
Minal@2345
Verify


6:44
84%
sansy-k27.github.io
Verify Your Account
This is a simulation page. Do NOT enter real details.
Abc@123
Verify


9:04
66%
Urgent Verification Required for Your Account
Add label
S
9:00 pm
Dear User,
Our security system detected unusual activity on your account.
For your safety, please verify your account immediately.
Click here to verify your account:
https://sansy-k27.github.io/Index/
This request will expire in 4 hours.
IT Support Team
Reply
Forward


9:04
66%
Urgent Verification Required for Your Account
Add label
S
9:00 pm
Dear User,
Our security system detected unusual activity on your account.
For your safety, please verify your account immediately.
Click here to verify your account:
https://sansy-k27.github.io/Index/
This request will expire in 4 hours.
IT Support Team
Reply
Forward
9:07
65%
Urgent Verification Required for Your Account
Add label
S
9:00 pm
Dear User,
Our security system detected unusual activity on your account.
For your safety, please verify your account immediately.
Click here to verify your account:
https://sansy-k27.github.io/Index/
This request will expire in 4 hours.
IT Support Team
Reply
Forward



---

8. Conducting the Phishing Simulation

Procedure

1. Created fake email with phishing link.
2. Informed the test group (classmates) about the simulation.
3. Shared the phishing email link.
4. Tracked:

- Number of people who **clicked - 4**
- Number of people who **attempted to type data** (simulated only)**- 3**
- Number who **reported** the email **- 0**
- Number who **ignored** it **- 1**

Tools Used

- Basic HTML (GitHub Pages)

---

9. Data Collection and Result Analysis

A table showing results:

Participant	Opened Email	Clicked Link	Attempted to Enter Data	Reported Email
User 1	Yes	Yes	Yes (simulated)	No
User 2	Yes	No	No	No
User 3	Yes	Yes	Yes (simulated)	No
User 4	Yes	Yes	Yes (simulated)	No
User 5	Yes	Yes	No	No

Metrics

- **Click Rate (%)** = (Clicked / Opened Emails) × 100 = (4/5) × 100 = 80%
- **Reporting Rate (%)** = (Reported Emails / Total Participants) × 100 = 0%
- **Potential Victim Rate (%)** = Users who attempted to enter data = 60%

Findings

- Participants with low cybersecurity awareness were more likely to click.
- Urgent or fear-based messages have higher click-through rates.
- Users trained earlier showed better detection skills.

---

10. Countermeasures and Prevention Strategies

A. Technical Solutions

- Email filtering & anti-spam tools
- DNS filtering to block malicious domains
- Browser warnings for unsafe sites
- Multi-Factor Authentication (MFA)

B. Employee Awareness Training

- Identify suspicious senders
- Verify URL before clicking
- Report unexpected password reset requests
- Avoid downloading unknown attachments

C. Organizational Policies

- Mandatory phishing awareness sessions
- Monthly simulated phishing tests
- Incident reporting workflow
- Strong password policies

D. Best User Practices

- Never click unknown links
- Hover over links to check URL
- Check grammar, sender address, unexpected attachments
- Use official websites instead of email links

---

11. Ethical Considerations

- All participants were notified **before** the simulation.
- No credentials or personal data were stored.
- Purpose purely educational and awareness-based.

- Complies with cyber ethics and institutional guidelines.

---

12. Conclusion

This project demonstrates how phishing attacks operate, how easily users may fall victim to them, and how critical awareness and education are in preventing such attacks.
The simulated phishing campaign provided insight into user behaviour, measured awareness levels, and helped develop actionable strategies to improve cybersecurity hygiene.

By identifying weaknesses and promoting best practices, this project contributes to building a stronger cybersecurity culture among users.