MAJOR PROJECT REPORT

Phishing Awareness Simulation Using Social Engineering Techniques

---

1. Introduction

Cybersecurity threats have increased rapidly with the expansion of digital communication and online services. Among these threats, **phishing attacks** remain one of the most common and effective cyber-attacks used by attackers to steal sensitive information such as usernames, passwords, banking details, and personal data. Phishing is a type of **social engineering attack** that exploits human psychology rather than technical vulnerabilities.

Attackers often impersonate trusted organizations and create a sense of urgency or fear to trick users into clicking malicious links or providing confidential information. Despite the availability of advanced security technologies, phishing continues to succeed due to a lack of user awareness.

This project focuses on conducting a **phishing awareness simulation in a controlled and ethical environment** to understand how phishing attacks operate, analyze user behavior, and suggest preventive measures. The project is strictly educational, and informed consent was obtained from all participants.

---

2. Problem Statement

Phishing attacks continue to be successful because many users are unable to identify fraudulent emails and fake websites. Organizations and individuals suffer data breaches, financial losses, and privacy violations due to a single successful phishing attempt. Technical security solutions alone are insufficient to stop phishing attacks, as the primary target is human behavior.

Therefore, there is a strong need to educate users through practical demonstrations and simulations to improve phishing awareness and cyber hygiene.

---

3. Objectives

The objectives of this project are:

- To study common phishing and social engineering techniques
- To design and simulate a realistic phishing email (for demonstration only)
- To analyze user responses and awareness levels
- To identify the effectiveness of phishing attacks

• To suggest preventive measures and awareness strategies

---

4. Scope of the Project

• The project is limited to **email-based phishing simulation**
• No real credentials or sensitive information are collected
• The simulation is conducted only for educational purposes
• Participants are informed about the simulation
• Results are analyzed anonymously

---

5. Literature Review / Background Study

Phishing attacks have evolved significantly over time. Early phishing emails were poorly written and easy to identify, but modern phishing attacks use professional language, official logos, and realistic website designs. According to cybersecurity studies, more than 90% of cyber-attacks begin with phishing emails.

Common phishing indicators include suspicious sender addresses, urgent language, unexpected attachments, and mismatched URLs. However, many users fail to verify these indicators due to lack of awareness or time pressure.

---

6. Methodology

6.1 Ethical Considerations

• All participants were informed in advance
• The activity was clearly labeled as a simulation
• Dummy credentials were used
• No data was stored or misused

6.2 Designing the Phishing Email

A fake password reset email was designed to resemble a legitimate security alert. The email included urgency-based language and a call-to-action link directing users to a demo login page.

6.3 Creating the Fake Login Page

A simple login page was created using **HTML and CSS** (or Google Form) to mimic a real login interface. The page clearly mentioned that it was a simulation for educational purposes.

6.4 Distribution

The phishing email was shared with a small group of participants (classmates). Participants interacted voluntarily.

6.5 Data Collection

The following user actions were observed:

- Number of users who opened the email
- Number of users who clicked the link
- Number of users who attempted to enter dummy data
- Number of users who reported the email as suspicious

---

7. Tools and Technologies Used

- HTML and CSS
- Google Forms
- Email client (Gmail)
- Screenshot documentation
- Optional theoretical study of Kali Linux – SET

---

8. Results and Observations

User Action	Number of Participants
Email Received	20
Clicked Link	12
Entered Dummy Data	7
Reported as Phishing	5

Observations:

- Urgency-based messages were highly effective
- Some users did not verify sender information
- A few participants correctly identified phishing indicators
- Awareness level was moderate

---

9. Lessons Learned

- Humans are the weakest link in cybersecurity
- Phishing relies more on psychology than technology
- Visual similarity increases trust
- Awareness training can significantly reduce phishing success

---

10. Preventive Measures

10.1 User Awareness

- Regular phishing awareness training
- Real-world phishing simulations
- Cybersecurity workshops and campaigns

10.2 Technical Controls

- Email spam filtering
- URL reputation checks
- DMARC, SPF, and DKIM implementation
- Multi-Factor Authentication (MFA)

10.3 Organizational Policies

- Mandatory cybersecurity training
- Easy reporting mechanisms
- Incident response planning

---

11. Ethical and Legal Considerations

- Simulation conducted with informed consent
- No real data collected
- No malicious intent or misuse of tools
- Educational purpose only

---

12. Conclusion

This project successfully demonstrated how phishing attacks exploit human psychology to steal sensitive information. The simulation helped participants understand common phishing techniques and improved awareness about cybersecurity threats. Combining technical security controls with continuous user education is essential to prevent phishing attacks effectively.

---

13. Future Scope

- SMS and voice phishing (smishing and vishing) simulations
- AI-based phishing detection systems
- Organization-wide phishing awareness programs

---

14. References

1. APWG – Phishing Activity Trends Reports
2. NIST Cybersecurity Framework
3. OWASP Phishing Guidelines
4. Cisco Cybersecurity Reports