PHISHING SIMULATION REPORT

1. Introduction

Phishing is a cyber attack in which attackers trick users into revealing sensitive information such as usernames, passwords, and banking details by pretending to be a trusted source. A phishing simulation is conducted to test user awareness and improve cyber security practices.

2. Objective

- To understand phishing attacks

- To test user awareness of fake emails and links

- To improve cyber security practices

- To identify security weaknesses

3. Tools Used

- Email client (Gmail/Outlook)

- Phishing awareness templates

- Web browser

- Security monitoring tools

4. Methodology

Step 1: A sample phishing email was created pretending to be from a bank or social media platform.

Step 2: The email contained a fake login link requesting user credentials.

Step 3: Users were asked to identify whether the email was real or fake.

Step 4: Responses were observed and recorded.

5. Sample Phishing Indicators

- Suspicious sender email address

- Urgent message like 'Your account will be blocked'

- Fake login links

- Spelling and grammar mistakes

- Unknown attachments

6. Observations

- Some users clicked on the fake link

- Some users identified phishing correctly

- Many users were unaware of phishing signs
- Awareness level needs improvement

7. Risks Identified

- Password theft
- Data breach
- Financial fraud
- Malware installation

8. Recommendations

- Do not click on unknown links
- Check sender email carefully
- Use strong passwords
- Enable two-factor authentication
- Attend cyber security awareness training

9. Conclusion

Phishing simulation helps in understanding how users respond to fake emails and attacks. Regular awareness and training can prevent phishing attacks and protect sensitive information.