Phishing Simulation & Awareness Report

(Internship Task – Internee.pk)

1. Introduction

Phishing is one of the most popular cyber-attacks used to steal user credentials and sensitive information. The attackers typically use fake emails that resemble legitimate emails from trusted brands to trick users into submitting their login credentials to fake websites.
This assignment is based on the simulation of a phishing attack using GoPhish. The primary objective of this simulation was to learn how phishing attacks work and how users can be trained to resist such attacks.

2. Objective

The objectives of this task were:

- To simulate a phishing attack for security awareness training
- To demonstrate how attackers design fake emails and login pages
- To analyse user interaction with phishing emails
- To improve awareness about phishing indicators
- To generate a security awareness report

3. Overview of Phishing Attacks

Phishing is a social engineering attack where attackers impersonate trusted organizations to deceive users into providing confidential information such as usernames and passwords.

Common types of phishing include:

- Email phishing
- Spear phishing
- Fake login pages
- Password reset scams.

Attackers usually create urgency in messages such as “Reset your password now” or “Your account will be blocked” to pressure users into clicking malicious links.

4. Tool Used – Go Phish

Go Phish is an open-source phishing simulation tool used for security awareness training. It allows organizations to:

- Create phishing email templates.
- Design fake landing pages
- Launch simulated phishing campaigns.
- Track email opens, link clicks, and form submissions

In this task, Go Phish was used in a local environment for training and learning purposes only.

5. Phishing Simulation Design

5.1 Email Template

A phishing-style email was composed with the subject line “Reset Your Password.”
The email had a custom button that led to a phishing login page.
The email was made to look urgent and realistic, just like a phishing email.

5.2 Landing Page

An example of a phishing login page was created using HTML and CSS. This page accepted user input and then redirected the user to the actual Instagram website.
The purpose of this page was to show how attackers deceive users into entering their credentials.

5.3 Campaign Launch

The phishing link used a local IP address as the phishing URL.
A test email was sent, and user interactions were tracked using Go Phish.
The following activities were monitored:

- Email opened.
- Link clicked.
- Credentials submitted.

6. Results & Analysis

The simulation showed how realistic phishing emails can convince users to click malicious links.
The interaction data helped identify how many users:

- Opened the phishing email.
- Clicked the phishing link.

- Submitted login details.

These results demonstrate the importance of security awareness training and regular phishing simulations.

7. Awareness & Training

After the simulation, awareness was provided to users by explaining common phishing indicators such as:

- Suspicious or shortened URLs.
- Urgent messages like “Reset Now”.
- Brand impersonation
- Spelling or grammar mistakes

Users were trained to:

- Verify sender email addresses.
- Avoid clicking unknown links.
- Report suspicious emails

8. Ethical & Legal Considerations

This phishing simulation was conducted strictly for educational and training purposes.
No real credentials were stored or misused.
No real users were targeted without permission.
The simulation environment was isolated and safe.

9. Recommendations

To reduce phishing risk, the following measures are recommended:

- Regular phishing awareness training
- Strong email filtering and spam detection
- Use of multi-factor authentication (MFA)
- Periodic phishing simulations
- Clear reporting procedures for suspicious emails

10. Conclusion

This assignment showed how phishing attacks are created and how users can be educated to identify them. By employing GoPhish for simulation, it is possible to comprehend attacker methods and user behavior.

This assignment enhanced the practical knowledge of social engineering attacks and the significance of user awareness in defending against cyber attacks.