Phishing Attack Simulation & Detection - Task 11 Report

NAME : KARTHIK P ***DATE :02-02-2026***

1. Introduction

This report documents a phishing attack simulation conducted as part of my Cyber Security Internship Task 11 "Phishing Attack Simulation & Detection."
The main goal of this task was to understand how phishing works in real life, how attackers design their emails and fake websites, and how users can detect and prevent such attacks through awareness and best practices.

Phishing is a social engineering technique where an attacker pretends to be a trusted entity (such as a bank, email provider, or company) and tricks users into revealing sensitive information like usernames, passwords, OTPs, or card details.
By running this simulation in a controlled and ethical environment, I was able to observe the full flow of a phishing attack from email to landing page and then analyze the red flags and prevention methods.

2. Objective of the Simulation

The main objectives of this task were:

- To design a realistic-looking phishing email and a fake landing page.
- To simulate sending the phishing email to a test user (myself / test account) and observe how a victim might interact with it.
- To track and analyze what happens when the link is clicked and credentials are entered.
- To identify the warning signs (red flags) in the email and page.
- To document prevention methods and improve social engineering awareness.

This entire simulation was done only for learning purposes in a safe environment and not used against any real users.

3. Tools and Environment

For this task, I used:

- Operating System: **Windows / Linux]**
- Phishing Setup Method: **GoPhish / Manual phishing templates]**
- Browser: **Chrome / Firefox / Edge]**
- Text/Code Editor: **VS Code / Notepad++ / etc.]**
- GitHub: **Used for uploading all task files, screenshots, and documentation.**

If using GoPhish, I used it to manage the email template, landing page, and campaign tracking. If using a manual approach, I created the phishing email as an HTML/text file and hosted the fake login page locally in my browser.

4. Phishing Email Design

4.1 Concept

I created a phishing email that pretends to be a security alert from an official-looking service. The email warns the user that their account may be locked or disabled if they do not verify their details immediately. This type of urgent message is very common in real phishing attacks because it creates pressure and fear, making users click without thinking carefully.

4.2 Email Content

- From Name: [IT Support] or [Security Team]
- From Email (spoofed style): support@secure-account[dot]com **(just an example)**
- Subject Line: URGENT:Account Verification Required
- Message Body (summary):
  - **Informs the user that suspicious login activity was detected.**
  - **Says that the account may be locked if they do not verify it.**
  - **Provides a button or link:** "Verify Account Now"**.**
  - **The link points to the fake landing page URL that I created.**

The email is designed to look professional and trustworthy, with a simple layout, a logo (optional), and a formal tone, so that it feels like a real notification from a company.

4.3 Observed Red Flags in the Email

Even though the email looks somewhat realistic, it still contains typical phishing red flags:

- The sender email address is not a genuine company domain.
- The email uses a generic greeting like “Dear User” instead of the real name.
- There is a strong sense of urgency and fear (“your account will be disabled today”).
- The message pushes the user to click a link instead of visiting the official website manually.
- The link behind the button does not belong to the official domain.

These red flags are very important for users to learn and recognize.

5. Landing Page Fake Website) Setup

5.1 Design of the Landing Page

The phishing email link sends the user to a fake login page that imitates a common service login screen (for example, email or cloud account).
The page includes:

- A logo at the top to look like a real brand (or a generic “Secure Login” logo).
- A heading such as “Account Verification” or “Secure Sign-In”.
- Two form fields: “Email/Username” and “Password”.
- A “Sign In” or “Verify” button.

The overall design is simple but clean, so that a normal user might think it is genuine at first g la nce.

5.2 Functionality

When the user enters their email and password and clicks the button, one of the following happens (depending on the implementation I chose):

- The data is captured (for simulation purposes only) and then the user is redirected to a generic page such as “Verification Failed” or “Thank you, your request is being processed.”
- Or the page simply refreshes and shows a basic message, just to simulate what a real phishing site would do after stealing the credentials.

No real accounts were harmed or accessed; only dummy credentials were used during testing.

5.3 Red Flags on the Landing Page

The landing page also contains clear signs that it is not legitimate:

- The URL is not an official domain (for example, it might be `http://localhost/phish/login.html` or a non-brand domain).
- It may lack HTTPS or show a browser warning if not properly configured.

- The design is similar to a real site but not exactly the same.
- The page asks for credentials immediately without any additional context or navigation.

A careful user who checks the address bar and certificate could detect that this is a fake site.

6. Campaign Execution and Results

6.1 Test Scenario

I acted as both the attacker and the victim in this simulation by sending the phishing email to a test account that I control (or by manually opening the email template and link).
This allowed me to safely observe how a user might interact with such an email and website.

Steps followed:

Prepared the phishing email and linked it to the fake landing page.

Opened the email in the test inbox.

Clicked on the "Verify Account" / "Reset Password" link.

Reached the fake login page.

Entered dummy credentials such as testuser@example.com and Test@1234.

Submitted the form and observed the behavior.

6.2 Observations

- The email looked reasonably convincing at first glance, especially with the urgent tone.
- The call-to-action button made it easy to just click without thinking.
- Once on the landing page, if I did not check the URL carefully, it felt like a normal login.
- As soon as I paid attention to details (domain name, HTTPS, grammar), I could clearly see it was suspicious.

These observations show how powerful social engineering can be when users are in a hurry or not paying attention.

7. Phishing Detection – Identifying Red Flags

From this simulation, the main indicators that help detect phishing are:

- Sender Email: Slightly altered or unknown domain instead of the official one.
- Generic Greeting: "Dear User/Customer" instead of real name.
- Urgent Language: Threats of account closure, fines, or loss of access if you don't act immed ia t ely.
- SuspiciousLinks: Link text looks normal, but when you hover over it, the real URL is different or weird.

- Unexpected Requests: **Asking to log in, reset password, or share sensitive information without a clear reason.**
- StrangeURL in Browser: **The login page URL does not match the genuine company web sit e.**
- Missing HTTPS or Certificate Issues: **No secure connection, or browser warnings.**

Training users to spot these red flags is one of the most effective phishing defenses.

8. Why Phishing is Dangerous

Phishing is extremely dangerous for both individuals and organizations because:

- **Attackers can steal login credentials, banking information, and personal data.**
- **Compromised accounts can lead to financial loss, identity theft, or data breaches.**
- **In companies, one successful phishing email can give attackers a foothold into the network, which can then lead to malware, ransomware, or large-scale attacks.**
- **Many users still trust emails too easily, so phishing remains one of the most successful attack methods today.**

This simulation clearly showed how easy it is to trick someone who is not paying attention or who is stressed and in a hurry.

9. Prevention Methods and Best Practices

To reduce the risk of phishing, both technical measures and user awareness are important.

9.1 Technical Measures

- **Use strong email filters and spam detection to block known phishing emails.**
- **Implement SPF, DKIM, and DMARC to make it harder to spoof your domain.**
- **Use URL filtering and web security gateways to block known malicious websites.**
- **Enable multi-factor authentication MFA) so that stolen passwords alone are not enough for attackers.**

9.2 User Awareness and Behavior

- **Always check the sender’s email address carefully, not just the display name.**
- **Hover over links before clicking to see the real URL.**
- **Never enter your credentials after clicking a link in an email; instead, manually type the official website address in the browser.**
- **Be suspicious of emails that create urgency, fear, or unrealistic offers.**
- **Do not open attachments or links from unknown or unexpected senders.**
- **Report suspicious emails to the security team or delete them immediately.**

Regular awareness sessions and phishing simulations like this one help users build a habit of verifying emails before acting.

10. Social Engineering Awareness – What I Learned

From completing this task, I gained a more practical understanding of social engineering:

- I saw how a combination of design (logo, layout) and psychology (fear, urgency) makes phishing effective.
- I understood how easy it is for someone to click a link and enter credentials if they are not trained to look for red flags.
- I learned how to design both the phishing email and the landing page, which also helps me recognize similar patterns in real life.
- Most importantly, I realized that technical security is not enough; human awareness is a critical part of cybersecurity.

This exercise has improved my ability to detect phishing attempts and reinforced the importance of educating users and conducting regular simulations.

11. Files and GitHub Repository

As part of the deliverables, I have included the following in my GitHub repository:

- `email-template/` – Phishing email template HTML/text).
- `landing-page/` – Fake login page files HTML/CSS .
- `screenshots/` – Screenshots of the email, landing page, and steps.
- `phishing_simulation_report.md` – This report.
- `README.md` – Overview of what I did, how I set it up, and how to view the templates.

GitHubRepositoryLink: `https://github.com/karthikp-creator/Task-11-Phishing-Attack-Simulation-Detection`

12. Conclusion

This phishing attack simulation gave me hands-on experience in how phishing campaigns are created and executed, and how they exploit human psychology rather than just technical v ulnera b ilit ies.
By analyzing my own phishing email and fake website, I improved my ability to recognize similar attacks in the real world and learned how important it is to combine technical defenses with strong user awareness and training.