PHISHING EMAIL DETECTION & AWARENESS REPORT

Analysis of a Suspicious Email Sample

Prepared by: Anjali
Cyber Security Intern – Future Interns
Date : 16 jan 2026

Table of Contents

1. Executive Summary

Phishing is a common cyberattack where attackers send fake emails to trick users into sharing sensitive information such as passwords, OTPs, or personal details. These emails are designed to look real and usually create fear or urgency so that users act without thinking.

In this report, a suspicious email sample has been analyzed to understand how phishing attacks work. The analysis includes checking the email header, sender details, message content, and the link provided in the email using email analysis tools. The email failed important security checks like SPF, DKIM, and DMARC, which indicates that the sender was not genuine.

Several phishing indicators were identified, including a fake sender domain, urgent warning messages, a suspicious verification link, and a generic greeting. Based on these findings, the email was classified as **High-Risk Phishing**. This report also explains the phishing attack in simple terms and provides basic safety tips to help users identify and avoid phishing emails in the future.

2. Introduction

Phishing is a type of cyber attack where attackers send fake emails that look like they are from trusted sources. These emails are used to trick users into clicking harmful links or sharing sensitive information such as passwords or OTPs.

Phishing attacks are a serious problem because they mainly target users who are not aware of how to identify fake emails. Messages that create urgency, such as account warnings or security alerts, often confuse users and lead to mistakes.

This report focuses on understanding phishing emails by analyzing a sample email and identifying common phishing signs. The goal of this report is to improve user awareness and help users stay safe from phishing attacks.

3. Scope and Methodology

Scope

- Analysis of one phishing email sample
- Identification of common phishing indicators
- Focus on sender details, email content, and links
- Report prepared only for educational and awareness purposes

Methodology

1. Collected a phishing email sample for analysis
2. Reviewed the email content to identify suspicious language and urgency
3. Analyzed the email header using online header analysis tools
4. Checked sender domain and embedded links safely
5. Classified the email based on identified risk indicators
6. Documented findings in a clear and simple manner

4. Phishing Email Overview

The analyzed email appears to be a security-related message sent to the user. The email claims that suspicious activity was detected on the account and warns the recipient that the account will be locked if immediate action is not taken. The message asks the user to verify their account details by clicking on a provided link.

- **Email Subject:** Urgent: Your Account Will Be Locked
- **Sender Address:** Unverified / Suspicious domain
- **Recipient:** User
- **Purpose of Email:** To prompt account verification
- **Action Requested:** Click on an external verific

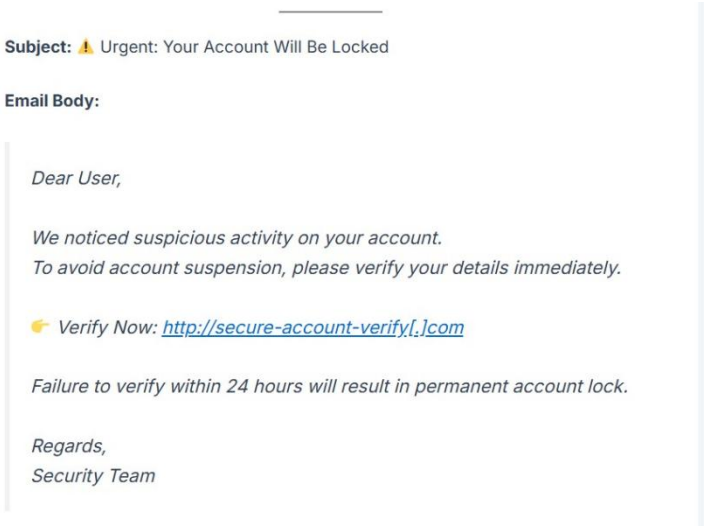

Figure 1 : Sample Phishing Email Body

5. Analysis of sample email

5.1 Email Header Analysis

The email header was analyzed using online email header analysis tools. The results showed failures in multiple email authentication mechanisms:

- **SPF:** Failed – The sender IP address was not authorized to send emails on behalf of the domain.
- **DKIM:** Failed – The email was not digitally signed by a trusted domain.
- **DMARC:** Failed – The domain policy alignment failed, indicating possible email spoofing.

These failures strongly indicate that the email did not originate from a legitimate or trusted source.

5.2 Email Content Analysis

The content of the email was carefully reviewed for social engineering techniques. The email used urgent and threatening language to pressure the recipient into taking immediate action, such as warning that the account would be locked.

The email contains a suspicious external verification link and uses a generic greeting instead of the recipient's name. These content-based indicators suggest the email is a phishing attempt designed to trick users into clicking a malicious link.

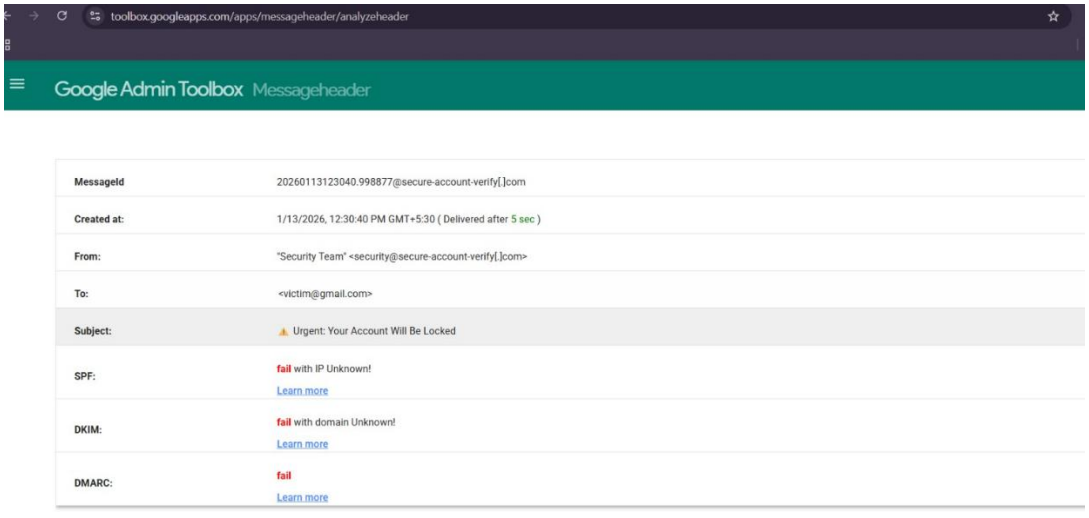

Figure 2 : Phishing Email Header Analysis Using Google Admin Toolbox

6. Findings Summary

The findings summary highlights key technical and behavioral indicators identified during the phishing email analysis.
These findings help assess the overall risk level and confirm that the email is a phishing attempt.

ID	Finding	Risk Level	Explanation
01	SPF Authentication Failed	High	The sender IP is not authorized, indicating possible spoofing.
02	DKIM Validation Failed	High	The email was not cryptographically signed by a trusted domain.
03	DMARC Policy Failed	High	The email failed domain alignment checks.
04	Use of Urgent Language	Medium	Creates fear to pressure the user into acting quickly.
05	Suspicious Verification Link	High	Link redirects to an untrusted external domain.
06	Generic Greeting	Low	No personalization, common in phishing emails.

Final Risk Decision:

Based on the identified technical and content-based indicators, the analyzed email is classified as **High Risk** and is confirmed to be a phishing attempt.

7. How the Phishing Attack Works

The following diagram illustrates the typical flow of a phishing attack. It shows how an attacker sends a phishing email, tricks the victim into clicking a malicious link, collects sensitive information, and misuses the stolen credentials.

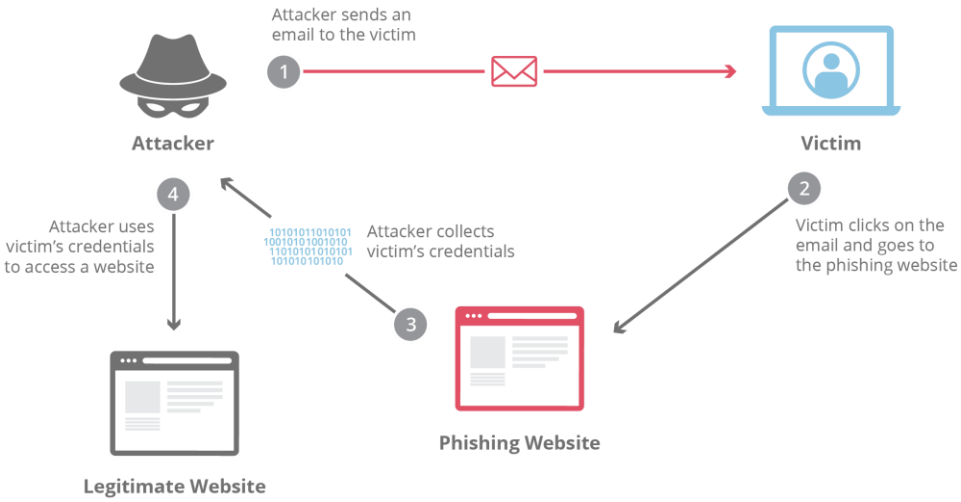

Figure 3: Flow of a phishing attack showing how attackers steal user credentials.

Phishing attacks usually follow a simple process designed to trick users into revealing sensitive information. The steps below explain how the phishing attack shown in the diagram works:

- The attacker sends a phishing email that appears to be from a legitimate organization.
- The email creates urgency and encourages the victim to click a verification link.
- The victim clicks the link and is redirected to a fake phishing website.
- The victim unknowingly enters login or personal details on the fake site.
- The attacker collects the credentials and may use them to access legitimate services.

8. Prevention and Awareness Guidelines

To protect users from phishing attacks, it is important to follow basic security practices and remain alert while handling emails. The following guidelines can help reduce the risk of falling victim to phishing attacks:

Do's

- Verify the sender's email address carefully before taking any action.
- Check links by hovering over them to see the actual URL before clicking.
- Look for signs of urgency or threatening language in emails.
- Report suspicious emails to the IT or security team.
- Use strong and unique passwords for online accounts.

Don'ts

- Do not click on links from unknown or untrusted sources.
- Do not share passwords, OTPs, or personal details via email.
- Do not download attachments from suspicious emails.
- Do not act immediately on emails that create fear or pressure.

Following these simple precautions can help users identify phishing emails and protect their accounts from unauthorized access.

9. Conclusion

Phishing attacks remain a serious cybersecurity threat due to their ability to exploit user trust and urgency. Through the analysis of the sample email, several phishing indicators were identified, including failed email authentication checks, a suspicious sender domain, and a malicious verification link. This report highlights the importance of user awareness and cautious email handling to prevent phishing attacks and protect sensitive information.