PHISHING EMAIL DETECTION & AWARENESS REPORT

Analysis of Suspicious Email Samples

Intern name: Cinchana S
Date : 14-02-2026

1. Executive Summary

Phishing attacks remain one of the most common and costly cyber threats affecting organizations worldwide. Attackers exploit human psychology rather than technical vulnerabilities by sending deceptive emails that appear legitimate. These emails aim to trick users into revealing sensitive information, clicking malicious links, or transferring funds.

This report analyzes two phishing email samples:

1. A credential harvesting attack (Account Suspension Scam)

2. A financial fraud attack (Business Email Compromise – Invoice Scam)

Both emails were examined using header analysis tools and content inspection techniques to identify phishing indicators and assess risk levels. The findings confirm that both emails are malicious and pose significant organizational risk.

2. Objectives

The objective of this task was to:

- Analyze phishing email samples
- Identify technical and content-based phishing indicators
- Perform email header authentication analysis
- Classify email risk levels
- Develop awareness and prevention guidelines for employees

3. 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.

4. 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

5. Sample Email 1 – Invoice Fraud

Phishing Email Overview

This email targets the finance department and claims an invoice is overdue. It requests immediate payment and provides updated bank account details.

- **Email Subject:** Invoice #88421 Overdue – Immediate Payment Required
- **Sender Address:** accounts@vendor-payments.com (Suspicious vendor domain)
- **Recipient:** Finance Department
- **Purpose:** Request urgent invoice payment
- **Action Requested:** Transfer funds to provided bank details
- **Attack Type:** Business Email Compromise (BEC) / Invoice Fraud

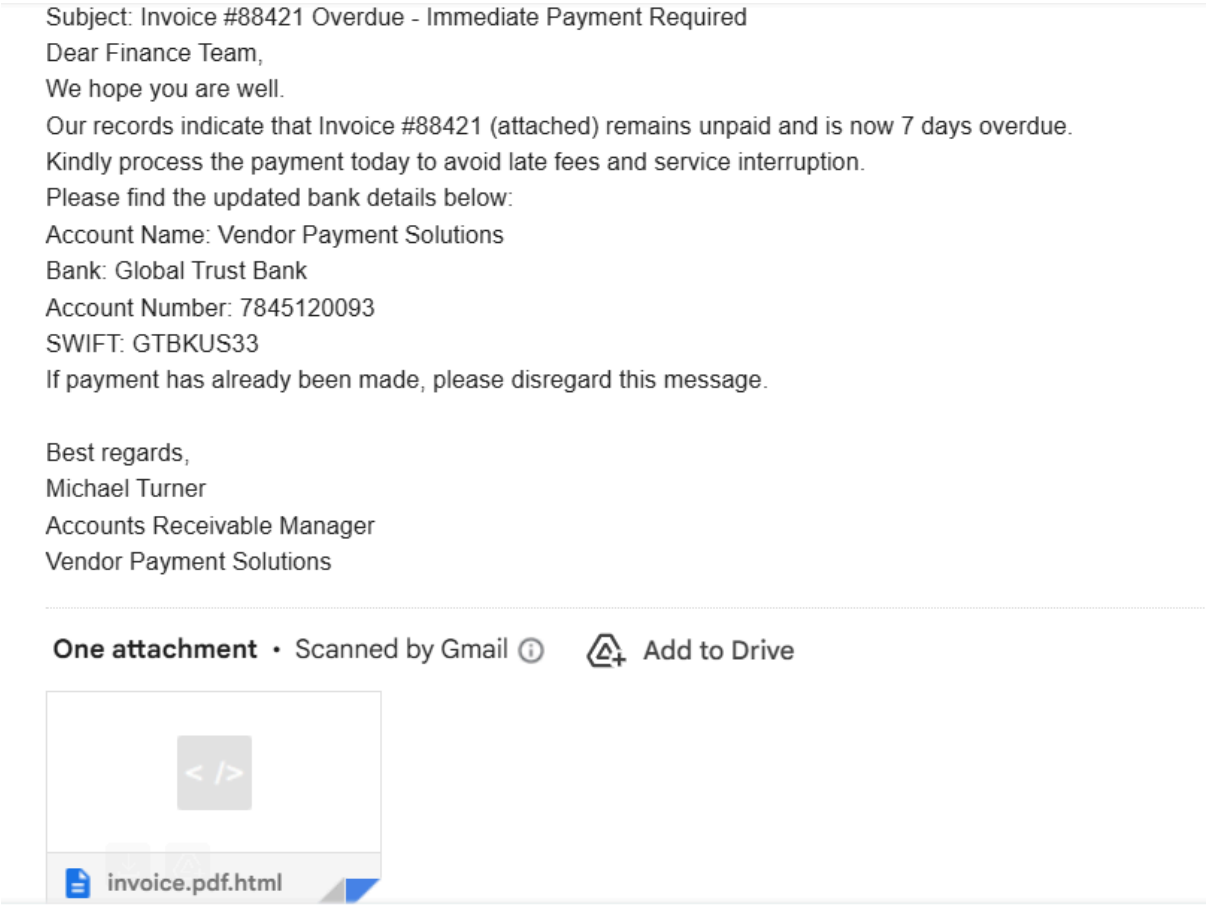

Figure 1 : Sample Phishing Email Body

Email Header Analysis

Header analysis revealed multiple authentication failures.

Authentication Results:

- **SPF:** SoftFail – IP (103.145.67.92) not properly authorized
- **DKIM:** Failed – Signature verification failed
- **DMARC:** Failed – Policy alignment failure
- **Reply-To Mismatch:** Different from From address
- **Suspicious Hosting Environment**

The authentication failures combined with reply-to mismatch strongly indicate email spoofing and malicious intent.

Email Content Analysis

The email uses authority and urgency to pressure the finance team:

- Generic greeting (“Dear Finance Team”)
- Urgent payment demand
- Threat of late fees
- Bank account details included
- Suspicious attachment format (.pdf.html)

This is a common financial fraud tactic used to redirect payments to attacker-controlled accounts.

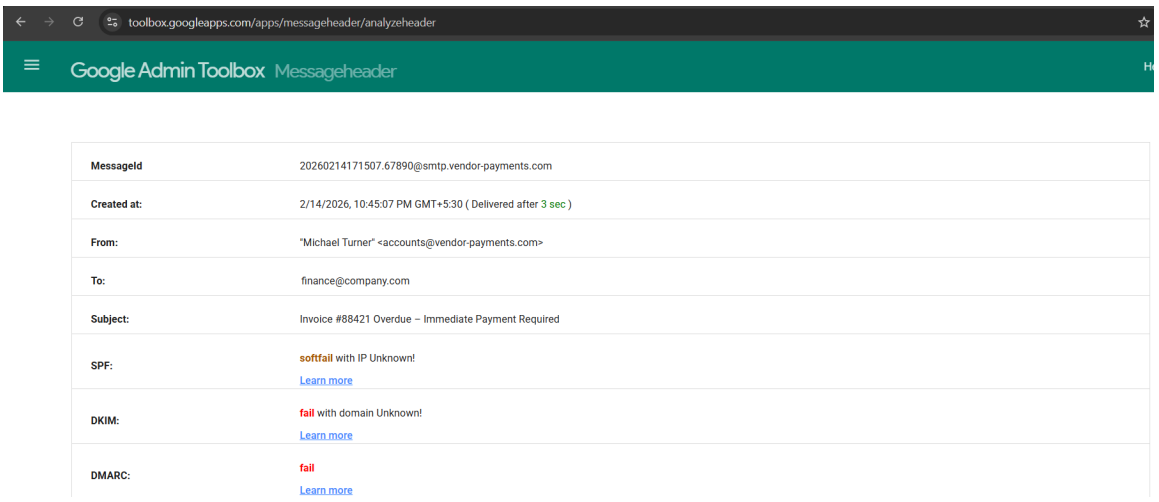

Figure 2 : Phishing Email Header Analysis Using Google Admin Toolbox

5.1 Sample Email 2 – Account Suspension Phishing

Phishing Email Overview

The analyzed email appears to be a security-related message claiming suspicious activity was detected on the user's account. The email warns that the account will be locked within 24 hours unless immediate verification is completed.

- **Email Subject:** ⚠️ Urgent: Your Account Will Be Locked
- **Sender Address:** security@secure-account-verify.com (Unverified domain)
- **Recipient:** User
- **Purpose:** Prompt account verification
- **Action Requested:** Click on external verification link
- **Attack Type:** Credential Harvesting

Subject: ⚠️ Urgent: Your Account Will Be Locked

Email Body:

Dear User,

We noticed suspicious activity on your account.
To avoid account suspension, please verify your details immediately.

👉 *Verify Now: http://secure-account-verify[.]com*

Failure to verify within 24 hours will result in permanent account lock.

Regards,
Security Team

Figure 3: Sample Phishing Email Body

Email Header Analysis

The header was analyzed using Google Message Header Analyzer.

Authentication Results:

- **SPF:** Failed – Sender IP (185.234.219.87) not authorized
- **DKIM:** None – No digital signature detected
- **DMARC:** Failed – Policy alignment failed
- **Sending Server:** Suspicious external hosting IP

Failure of SPF, DKIM, and DMARC indicates that the email was not sent from an authorized mail server. These failures strongly suggest domain spoofing and phishing activity.

Email Content Analysis

The content uses classic social engineering techniques:

- Urgent and threatening language
- Fear-based messaging (account lock warning)
- Generic greeting (“Dear User”)
- Suspicious external link
- Unverified domain

These indicators confirm the email is designed to trick users into entering credentials on a fake website.

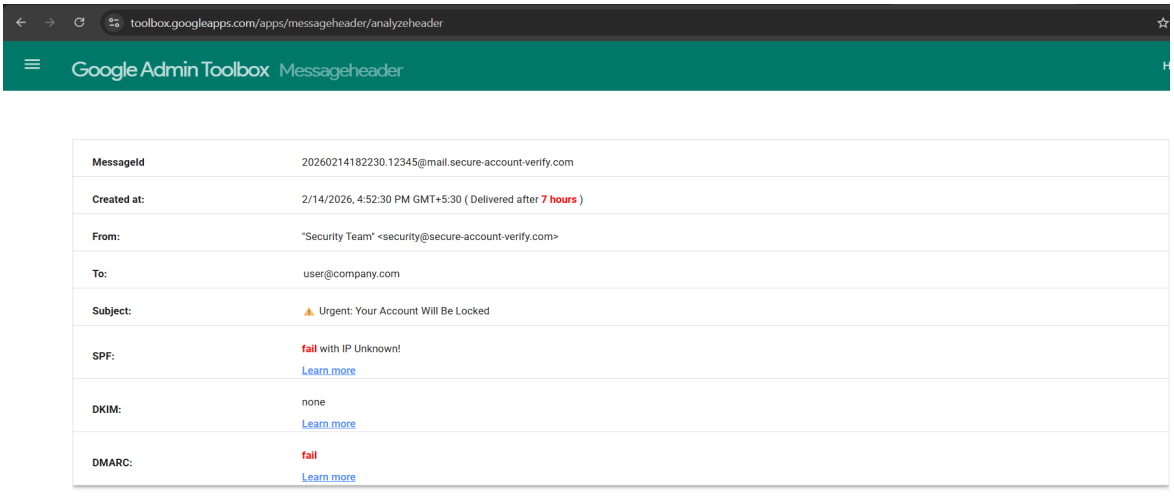

Figure 4 : Phishing Email Header Analysis Using Google Admin Toolbox

6. Risk Summary

Sample Email	Attack Type	Authentication Result	Risk Level
Sample Email 1	Business Email Compromise	SPF SoftFail, DKIM Fail, DMARC Fail	Critical
Sample Email 2	Credential Harvesting	SPF Fail, DKIM None, DMARC Fail	High

7. Common Phishing Indicators Identified

Content Indicators

- Generic greetings
- Urgent language
- Fear or financial pressure
- Suspicious attachments
- External verification links

Technical Indicators

- SPF failure
- DKIM failure
- DMARC failure
- Sender domain mismatch
- Reply-To mismatch
- Suspicious sending IP

8. 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.

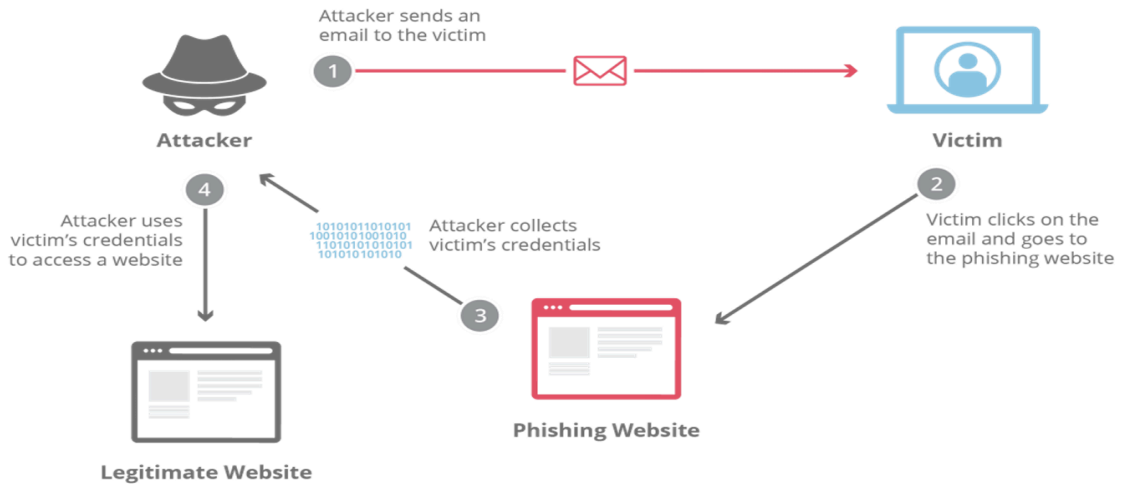

Figure 5: Flow of a phishing attack showing how attackers steal user credentials.

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.

9. 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.

10. 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.