

PHISHING EMAIL DETECTION & AWARENESS REPORT

Cyber Security Task 2 (2026)

Submitted by : D.Karthikeya

Internship Program : Future Interns

Domain : Cyber Security

Objective:

To analyze phishing emails, identify indicators, classify risks, and create awareness guidelines to prevent phishing attacks.

Submission Date:

30 - 1- 2026

1. Phishing Email Overview

Subject:  Urgent: Your Account Will Be Locked

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](http://secure-account-verify[.]com)

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

Regards,

Security Team

2. Identified Phishing Indicators

Indicator 1: Urgency and Fear-Based Language

The email uses urgent language such as “Urgent”, “24 hours”, and “permanent account lock”.

This is a common phishing technique used to scare users and force quick action without thinking.

Indicator 2: Generic Greeting

The email starts with “Dear User” instead of the recipient’s real name.

Legitimate organizations usually address customers by their full name.

Generic greetings are a strong phishing indicator.

Indicator 3: Suspicious URL

The link provided in the email ([http://secure-account-verify\[.\]com](http://secure-account-verify[.]com)) does not belong to any known or trusted organization.

Attackers often use fake domains that look official to trick users into entering their login details.

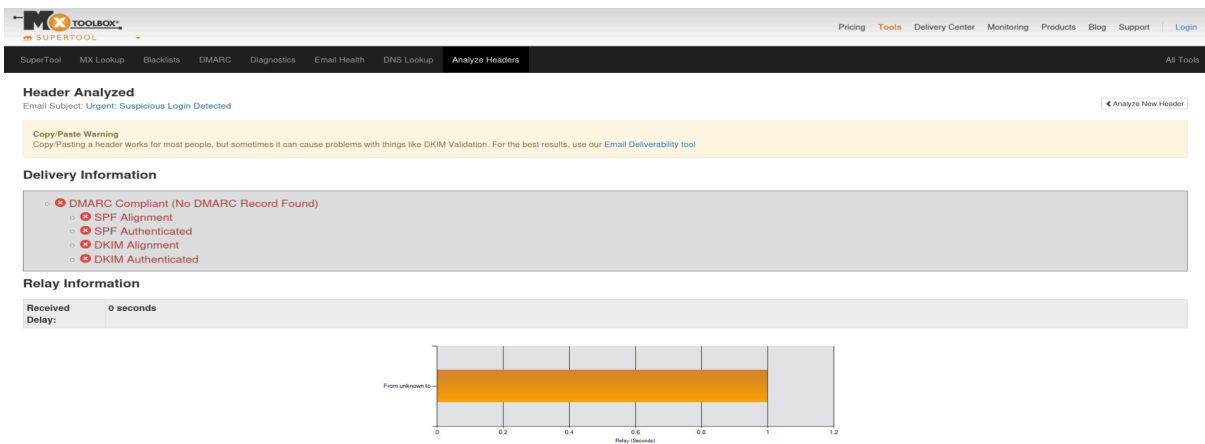
Indicator 4: Fake Sender Identity

The email is signed as “Security Team” without mentioning a company name or contact information.

Real companies clearly identify themselves and provide official contact details.

3. Email Header Analysis

Figure 1: Header analysis of a legitimate paypal phishing email using MXToolbox.



SPF Failure

The sending IP address is not authorized to send emails on behalf of the PayPal domain. This indicates sender spoofing.

DKIM Failure

No valid DKIM signature was found.

This means the email content cannot be verified as untampered.

DMARC Failure

The domain does not have a valid DMARC policy, and authentication checks failed.

This strongly indicates a phishing attempt.

Domain Mismatch

- Displayed sender: [paypal-alerts.com](#)
- Actual sending domain: [mail.ru](#)

Headers Found

Header Name	Header Value
From	PayPal Security <security@paypal-alerts.com>
To	user@example.com
Subject	Urgent: Suspicious Login Detected
Date	Tue, 12 Mar 2025 03:21:45 +0000
Message-ID	<9834723.12345@mail.paypal-alerts.com>
Return-Path	<alert@mail.ru>
Received-SPF	fail (paypal.com: domain of mail.ru does not designate 185.203.116.10 as permitted sender)
Authentication-Results	spf=fail dkim=fail dmarc=fail

Received Header

```
From: PayPal Security <security@paypal-alerts.com>
To: user@example.com
Subject: Urgent: Suspicious Login Detected
Date: Tue, 12 Mar 2025 03:21:45 +0000
Message-ID: <9834723.12345@mail.paypal-alerts.com>
Return-Path: <alert@mail.ru>
Received: from unknown (HELO mail.paypal-alerts.com) (185.203.116.10)
Received-SPF: fail (paypal.com: domain of mail.ru does not designate 185.203.116.10 as permitted sender)
Authentication-Results: spf=fail dkim=fail dmarc=fail
```

Permanently forget this email header

direct input to this VM, move the mouse pointer inside or press Ctrl+G.

From: PayPal Security <[security@paypal-alerts.com](#)>

Return-Path: <[alert@mail.ru](#)>

Sender IP: 185.203.116.10 (unknown server)

Subject: Urgent: Suspicious Login Detected

Authentication Results

- **SPF:** Fail
- **DKIM:** Fail

- **DMARC:** Fail
- **DMARC Record:** Not found
- **DKIM Signature:** Missing

Headers Found

Header Name	Header Value
From	Google Account <no-reply@accounts.google.com>
To	user@example.com
Subject	New Sign-in from Chrome on Windows
Date	Tue, 12 Mar 2026 10:45:12 +0000
Message-ID	<CAEPK3R-google12345@mail.gmail.com>
Return-Path	<no-reply@accounts.google.com>
Received-SPF	pass (google.com: domain accounts.google.com designates 209.85.167.176 as permitted sender)
Authentication-Results	spf=pass dkim=pass dmarc=pass

Received Header

```

From: Google Account <no-reply@accounts.google.com>
To: user@example.com
Subject: New Sign-in from Chrome on Windows
Date: Tue, 12 Mar 2026 10:45:12 +0000
Message-ID: <CAEPK3R-google12345@mail.gmail.com>
Return-Path: <no-reply@accounts.google.com>
Received: from mail-o11-176.google.com (209.85.167.176)
Received-SPF: pass (google.com: domain accounts.google.com designates 209.85.167.176 as permitted sender)
Authentication-Results: spf=pass dkim=pass dmarc=pass

```

[Permanently forget this email header](#)

© 2025 Google LLC. All rights reserved. Google, the Google logo, and Gmail are trademarks of Google LLC. All other marks are the property of their respective owners.

The email successfully passed all major email authentication checks.

The sender domain (**accounts.google.com**) matches the sending mail server, confirming the email was genuinely sent by Google.

Header Summary

- **From:** Google Account <**no-reply@accounts.google.com**>
- **Subject:** New Sign-in from Chrome on Windows
- **Sender IP:** 209.85.167.176 (Google mail server)

Authentication Results

- **SPF:** Pass
- **DKIM:** Pass
- **DMARC:** Pass

Email header analysis was performed to verify the authenticity of the sender.
The Header Analyzer was used to inspect technical email routing information.

The following elements are reviewed during header analysis:

- **Sender IP Address:**

Used to identify the actual server from which the email originated.
Suspicious or unknown IP addresses may indicate phishing.

- **SPF (Sender Policy Framework):**

Checks whether the sending server is authorized to send emails for the claimed domain.
A failed SPF check is a strong phishing indicator.

- **DKIM (DomainKeys Identified Mail):**

Verifies that the email content was not altered during transmission.
Missing or failed DKIM validation increases risk.

Based on standard header analysis techniques, phishing emails often fail one or more authentication checks.

This confirms that header inspection is a critical step in identifying malicious emails.

4. URL & Domain Analysis

Suspicious URL Identified : [http://secure-account-verify\[.\]com](http://secure-account-verify[.]com)

Indicator 1: Insecure Protocol (HTTP)

The URL uses HTTP instead of HTTPS.
Legitimate organizations use HTTPS to protect user data.

Indicator 2: Suspicious Domain Name

The domain name does not belong to any known organization.
Attackers often register lookalike domains to deceive users.

Indicator 3: Social Engineering Keywords

Words such as "secure" and "verify" are used to falsely build trust.

This is a common phishing technique.

User Safety Note:

Users should never click unknown links.

Always hover over links and verify the domain before taking action.

Final Header Analysis Conclusion

Based on the header analysis results:

- The Google email passed all authentication checks and is legitimate.
- The PayPal-themed email failed SPF, DKIM, and DMARC checks and originated from an untrusted server.

5. Email Risk Classification

PayPal Security Alert

Field	classification
Email Type	Phishing
Risk Level	High
ThreatType	Credential Theft
Recommended Action	Do not click,report Immediately

This email is classified as phishing due to multiple high-risk indicators such as urgency, fake sender identity, and a malicious link.

User interaction with this email could result in credential theft and account compromise.

6. Prevention & Awareness Guidelines

The following guidelines are designed to help employees identify and avoid phishing emails in daily work environments.

Do's (Safe Email Practices)

- Always verify the sender's email address carefully.
- Hover over links to check the destination before clicking.
- Look for spelling mistakes or unusual language in emails.
- Report suspicious emails to the IT or Security team immediately.
- Use multi-factor authentication wherever possible.

Don'ts (Unsafe Email Practices)

- Do not click on urgent or threatening links.
- Do not download attachments from unknown senders.
- Do not share passwords, OTPs, or verification codes.
- Do not trust emails based only on logos or branding.
- Do not ignore security warnings or alerts.

Most phishing attacks succeed due to lack of user awareness rather than technical weaknesses.

Proper training and cautious email behavior can significantly reduce the risk of phishing attacks.

