Phishing Email Detection & Awareness Report

Prepared by : Sirajudin Seid
Purpose: Employee Security Awareness & Internal Risk Assessment

Table of Contents

1. Executive Summary

Phishing is one of the most common cyber threats affecting organizations today. It involves fraudulent emails designed to trick employees into clicking malicious links, downloading harmful files, or sharing sensitive information such as passwords or one-time passcodes.

Phishing emails are dangerous because they target human trust rather than technical system weaknesses. A single successful phishing attempt can lead to account compromise, data breaches, financial loss, and reputational damage for an organization.

The purpose of this report is to analyze phishing email examples, identify common warning signs, classify the level of risk, and educate employees on how to recognize and safely respond to phishing attempts.

2.1 Sample-1 Email Analysis

Analyzed Email: Sample 1

Received Header

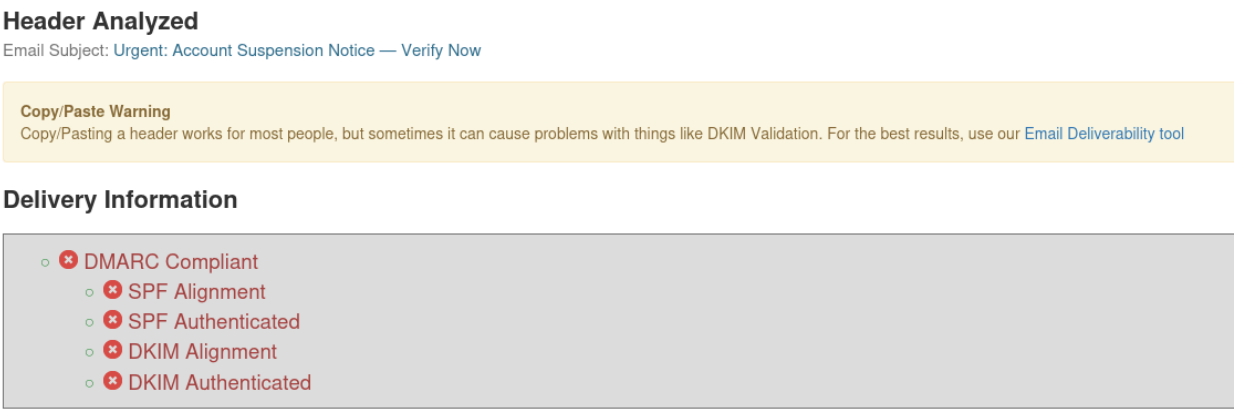
```
Return-Path: <support@amaz0n-security.com>
Received: from smtp5.hostingprovider (smtp5.hostingprovider [198.51.100.24])
        by mx.example.com (Postfix) with ESMTPS id 123ABC
        for <user@example.com>; Mon, 15 Sep 2025 12:34:56 +0530 (IST)
Authentication-Results: mx.example.com; spf=fail (mx.example.com: domain of support@amaz0n-security.com does not designate 198.51.100.24 as permitted sender) smtp.mailfrom=support@amaz0n-security.com; dkim=none; dmarc=fail
From: "Amazon Support" <support@amaz0n.com>
Reply-To: support@amaz0n-security.com
To: user@example.com
Subject: Urgent: Account Suspension Notice – Verify Now
Date: Mon, 15 Sep 2025 12:34:56 +0530
Message-ID: <CA+12345abcd@example.org>
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8

<html>
<body>
<p>Dear Customer,</p>
<p>We detected suspicious activity on your Amazon account and temporarily suspended access. To avoid permanent suspension, please verify your account within 24 hours.</p>
<p><a href="http://secure-amazon.verify-123.com/login" target="_blank">https://amazon.com/verify</a></p>
<p>Failure to verify will result in permanent account suspension.</p>
<p>Sincerely,<br>Amazon Support Team</p>
</body>
</html>
```

Header Analysis

Google Admin Toolbox Messageheader

MessageId	CA+12345abcd@example.org
Created at:	9/15/2025, 10:04:56 AM GMT+3 (Delivered after)
From:	"Amazon Support" <support@amaz0n.com>
To:	user@example.com
Subject:	Urgent: Account Suspension Notice — Verify Now
SPF:	**fail** with IP Unknown! Learn more

Header Analysis Failer



Sender Analysis

- Displayed sender name: "Amazon Support"
- From address: support@amaz0n.com
- Return-Path / Reply-To: support@amaz0n-security.com

Indicators

1. Sense of Urgency / Threats

The email pressures the recipient by stating that the account has been suspended and must be verified within 24 hours to avoid permanent suspension. This artificial deadline is designed to create panic and force quick action without proper verification.

2. Suspicious Sender Address

The sender claims to be “Amazon Support,” but the email address uses a look-alike domain (amaz0n instead of amazon).
Additionally, the From, Return-Path, and Reply-To addresses do not match, which is uncommon for legitimate corporate emails and strongly indicates spoofing.

3. Generic Greetings & Tone

The email begins with “Dear Customer” instead of addressing the recipient by name. Legitimate companies typically personalize important security notifications, while phishing emails use generic greetings to target many users at once.

4. Unexpected Attachments / Links

The recipient is asked to click a verification link without having requested any account changes or reported suspicious activity. Unexpected requests to "verify" or "confirm" account details are a common phishing tactic.

5. Suspicious Links

The visible link text appears related to Amazon, but the actual destination leads to a non-Amazon domain (secure-amazon.verify-123.com).
Using a trusted brand name within a longer, misleading URL is a common method used to trick users into entering credentials on fake websites.

6. Poor Grammar / Spelling

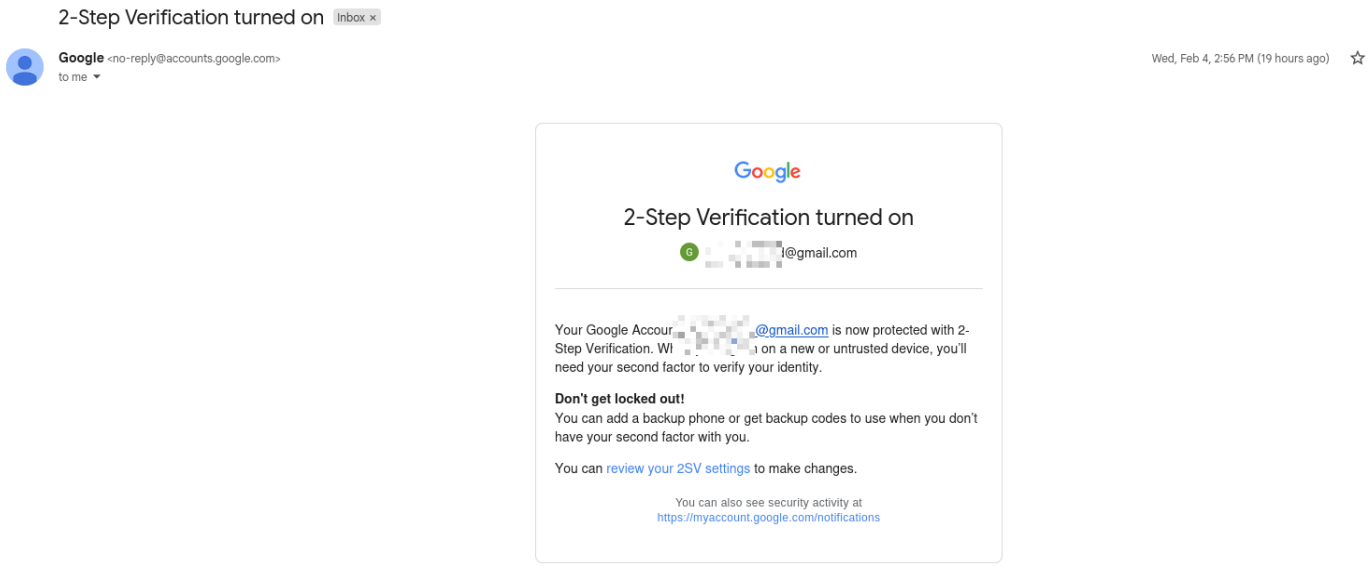
The email content is written in relatively correct English. However, the domain spelling manipulation (amaz0n) is a deliberate deception technique, which still qualifies as a strong phishing indicator even when grammar appears professional.

Email Risk Classification

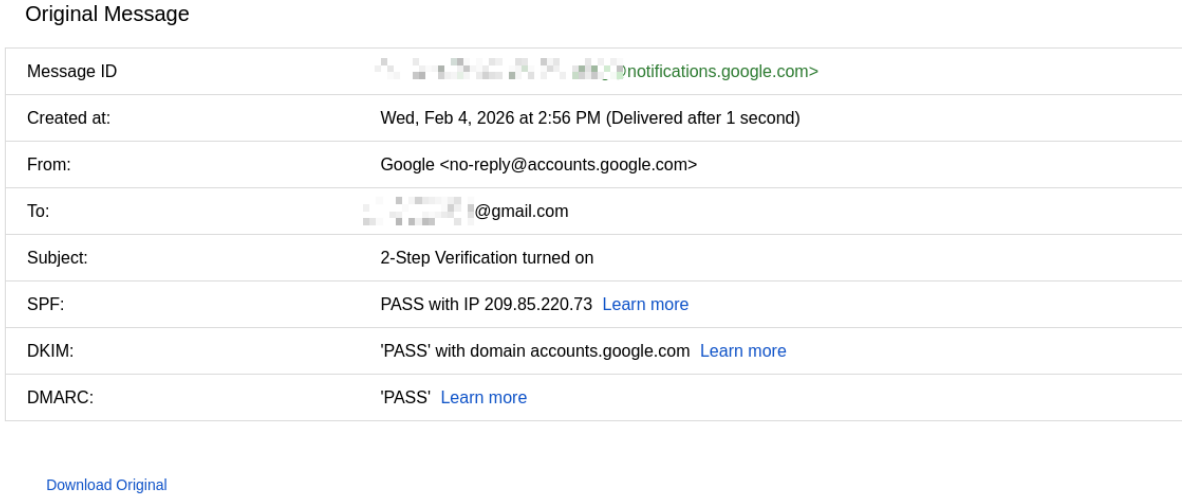
Risk Classification: **Phishing**

Justification: The email contains multiple phishing indicators, including a suspicious sender identity, malicious-looking URL, urgency-driven language, and a request for immediate account verification. These characteristics confirm malicious intent.

2.2 Sample-2 Email Analysis



Sender & Header Authentication Analysis



SPF: Pass – sending server is authorized for the domain
DKIM: Pass – message integrity verified
DMARC: Pass – domain alignment confirmed

These results confirm the email was sent from an authorized mail server and was not altered in transit.

Sender Address Verification

> Sender domain is legitimate and correctly spelled
> No use of look-alike characters or typosquatting
> Reply-To matches the sender domain

This indicates a trusted and authenticated sender.

Greeting & Tone Analysis

> Uses a neutral, professional tone
> No fear-based or threatening language
> No pressure to act immediately

The language is informational rather than manipulative.

Link & Content Analysis

> Links point to official and well-known domains
> No URL shortening or obfuscation techniques
> No unexpected attachments included

The email does not request credentials or sensitive information via email links.

Phishing Indicators Review

No phishing indicators were identified in this email.

Risk Classification

Risk Level: Safe Email

Justification: The email passes all authentication checks, originates from a legitimate domain, uses appropriate language, and contains no malicious indicators. It is a genuine security notification intended to inform the user.

3. How Phishing Attacks Work (Simple Explanation)

Phishing attacks rely on tricking people rather than breaking technical systems. Attackers pretend to be trusted organizations, such as banks or online services, to make the email look legitimate.

First, the attacker sends an email that creates urgency or fear, such as warning about account suspension or suspicious activity. This pressure is meant to make the recipient act quickly without thinking.

Next, the email includes a link or attachment that leads to a fake website or malicious file. The fake website is designed to look real so users feel safe entering their login details.

Once the user enters information such as a username, password, or one-time code, the attacker captures it. The attacker can then access company systems, steal sensitive data, or use the account to send further phishing emails.

4. Prevention & Awareness Guidelines

Strong awareness and cautious behavior are the most effective defenses against phishing attacks.

Do's

> Check the sender's email address carefully, not just the display name
> Hover over links to verify the real destination before clicking
> Be cautious of emails that create urgency or threats
> Verify unexpected requests through official channels
> Report suspicious emails to the IT or Security team immediately

Don’ts

> Do not click links or download files from unknown or unexpected emails
> Do not share passwords, one-time passcodes, or personal information by email
> Do not trust emails solely based on logos or professional appearance
> Do not respond to emails that pressure you to act quickly

5. Employee Quick Safety Checklist

Employees can use this quick checklist before interacting with any email:

> Is the sender’s email address legitimate?
> Does the message create urgency or fear?
> Are there links or attachments I was not expecting?
> Is the greeting generic or impersonal?
> Am I being asked to share sensitive information?

If any answer feels uncertain, do not interact with the email and report it.

6. Conclusion

Phishing attacks remain one of the most effective methods used by cybercriminals because they exploit human trust rather than technical weaknesses. Even well-secured systems can be compromised if users are unaware of phishing tactics.

By learning how to identify phishing indicators, verifying emails before taking action, and reporting suspicious messages promptly, employees play a critical role in protecting the organization. Continuous awareness and cautious behavior significantly reduce security risks.

7. Disclaimer

This report has been prepared for security awareness and educational purposes only. The email samples used are for analysis and training and do not represent real customer data. No systems were accessed, tested, or compromised during this assessment.