PHISHING EMAIL DETECTION & SECURITY AWARENESS REPORT

(TASK – 2 | EMAIL SECURITY INVESTIGATION PROJECT)

Prepared By:

Rushikesh borse

Cyber Security Intern

Organization / Internship Program:

[Future Interns]

Project Overview

This project focuses on the identification, analysis, and classification of phishing emails using professional email security investigation techniques.

The objective of this report is to:

- Analyze suspicious email samples
- Examine email headers using authentication tools
- Inspect malicious links safely using browser techniquesThis project emphasizes security awareness and defensive analysis, not offensive activities.

Tools Used in This Investigation

1.Email Header Analysis Tool
Google Admin Toolbox – Messageheader

2.Browser Inspection Techniques

Email Sample 1 – Fake Bank Account Verification

Summary

From: **alert@secure-bank-login.com**
Subject: **Urgent: Verify Your Bank Account Immediately**

Email 1.

Fake Bank – Phishing Email Content

Subject: Urgent: Verify Your Bank Account Immediately

Dear Customer,

We detected unusual activity on your bank account.
For your protection, your account has been temporarily restricted.

To restore access, please verify your account immediately:

http://secure-bank-login.com/verify

Failure to verify within 24 hours will result in permanent suspension.

Fake Bank – Phishing Email Overview

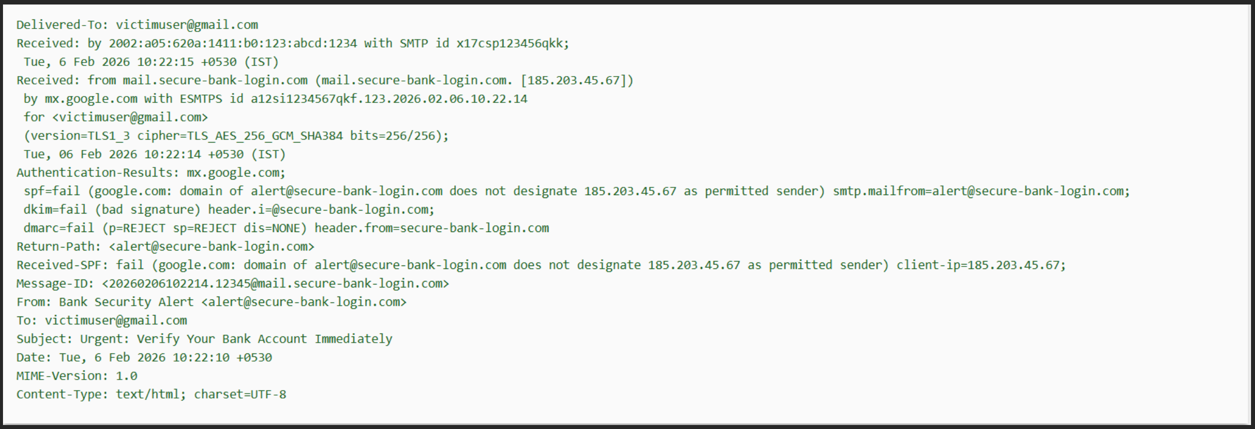
This email impersonates a bank and claims unusual account activity.

It creates urgency by stating the account is temporarily restricted.

The victim is pressured to verify through a suspicious link.

The goal is to steal banking credentials through a fake login page.

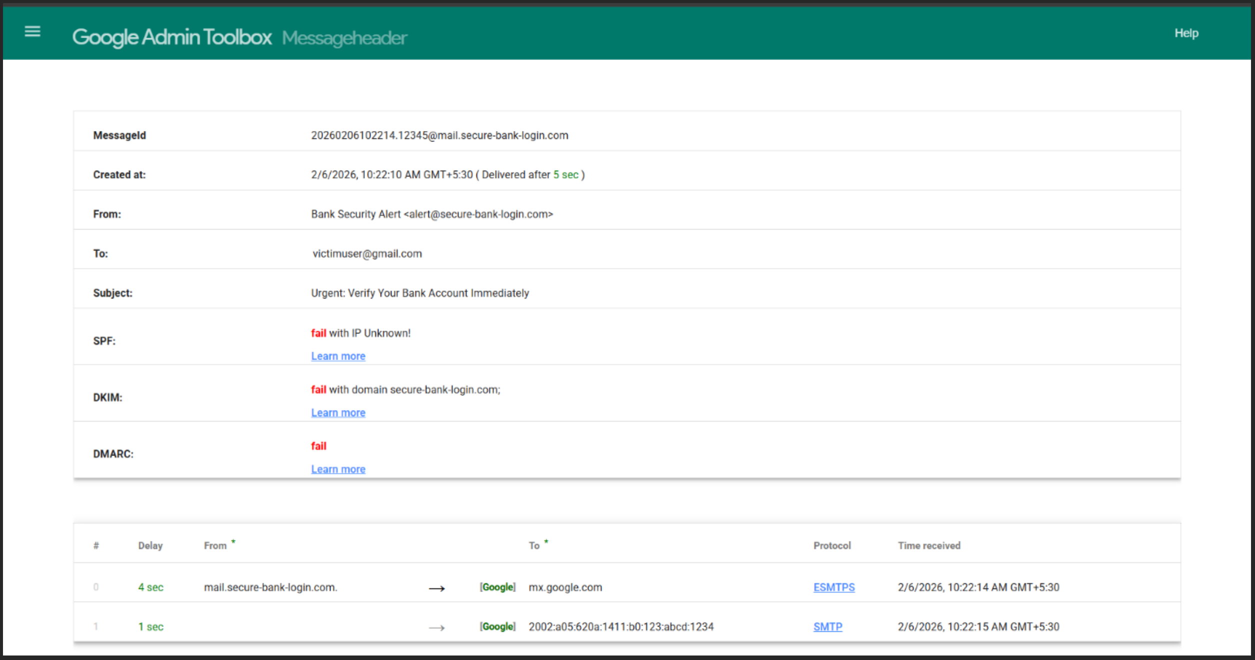
Header



```
Delivered-To: victimuser@gmail.com
Received: by 2002:a05:620a:1411:b0:123:abcd:1234 with SMTP id x17csp123456qkk;
 Tue, 6 Feb 2026 10:22:15 +0530 (IST)
Received: from mail.secure-bank-login.com (mail.secure-bank-login.com. [185.203.45.67])
 by mx.google.com with ESMTPS id a12si1234567qkf.123.2026.02.06.10.22.14
 for <victimuser@gmail.com>
 (version=TLS1_3 cipher=TLS_AES_256_GCM_SHA384 bits=256/256);
 Tue, 06 Feb 2026 10:22:14 +0530 (IST)
Authentication-Results: mx.google.com;
 spf=fail (google.com: domain of alert@secure-bank-login.com does not designate 185.203.45.67 as permitted sender) smtp.mailfrom=alert@secure-bank-login.com;
 dkim=fail (bad signature) header.i=@secure-bank-login.com;
 dmarc=fail (p=REJECT sp=REJECT dis=NONE) header.from=secure-bank-login.com
Return-Path: <alert@secure-bank-login.com>
Received-SPF: fail (google.com: domain of alert@secure-bank-login.com does not designate 185.203.45.67 as permitted sender) client-ip=185.203.45.67;
Message-ID: <20260206102214.12345@mail.secure-bank-login.com>
From: Bank Security Alert <alert@secure-bank-login.com>
To: victimuser@gmail.com
Subject: Urgent: Verify Your Bank Account Immediately
Date: Tue, 6 Feb 2026 10:22:10 +0530
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
```

Tools Used in This Investigation

- **Email Header Analysis Tool**
- **Google Admin Toolbox – Messageheader**



MessageId	20260206102214.12345@mail.secure-bank-login.com
Created at:	2/6/2026, 10:22:10 AM GMT+5:30 (Delivered after 5 sec)
From:	Bank Security Alert <alert@secure-bank-login.com>
To:	victimuser@gmail.com
Subject:	Urgent: Verify Your Bank Account Immediately
SPF:	fail with IP Unknown! Learn more
DKIM:	fail with domain secure-bank-login.com; Learn more
DMARC:	fail Learn more

#	Delay	From *			To *	Protocol	Time received
0	4 sec	mail.secure-bank-login.com.	→	[Google]	mx.google.com	ESMTPS	2/6/2026, 10:22:14 AM GMT+5:30
1	1 sec		→	[Google]	2002:a05:620a:1411:b0:123:abcd:1234	SMTP	2/6/2026, 10:22:15 AM GMT+5:30

Identification of Phishing Indicators

- SPF authentication failure
- DKIM signature failure
- DMARC policy failure
- Fake look-alike domain (secure-bank-login.com)
- Urgency-based language
- Threat of account suspension
- Suspicious verification link
- Generic greeting

Email Risk Classification

Phishing (High Risk)

Reason: Authentication failures + domain impersonation + social engineering tactics.

Simple Explanation of How the Attack Works

The attacker pretends to be a bank and sends an urgent message claiming suspicious activity.
The victim is pressured to click a link and enter login details

Do’s and Don’ts
Do’s
• Type official bank URL manually in browser • Contact bank customer support directly • Check email authentication warnings
Don’ts
• Do not click suspicious login links • Do not share OTP or password • Do not respond to urgent financial threats

Email Risk Classification

Phishing (High Risk)

Email Sample 2 – Fake Google Security Alert

Type official bank URL manually in Check email authentication warnings Summary

From: support@google-secure-alert.net
Subject: Security Alert – Suspicious Login Attempt

EMAIL 2 :-

Fake Google Security Alert

Subject: Security Alert – Suspicious Login Attempt

Dear User,

We detected a login attempt from a new device in Russia.

If this was not you, please secure your account immediately:

http://google-secure-alert.net/recover

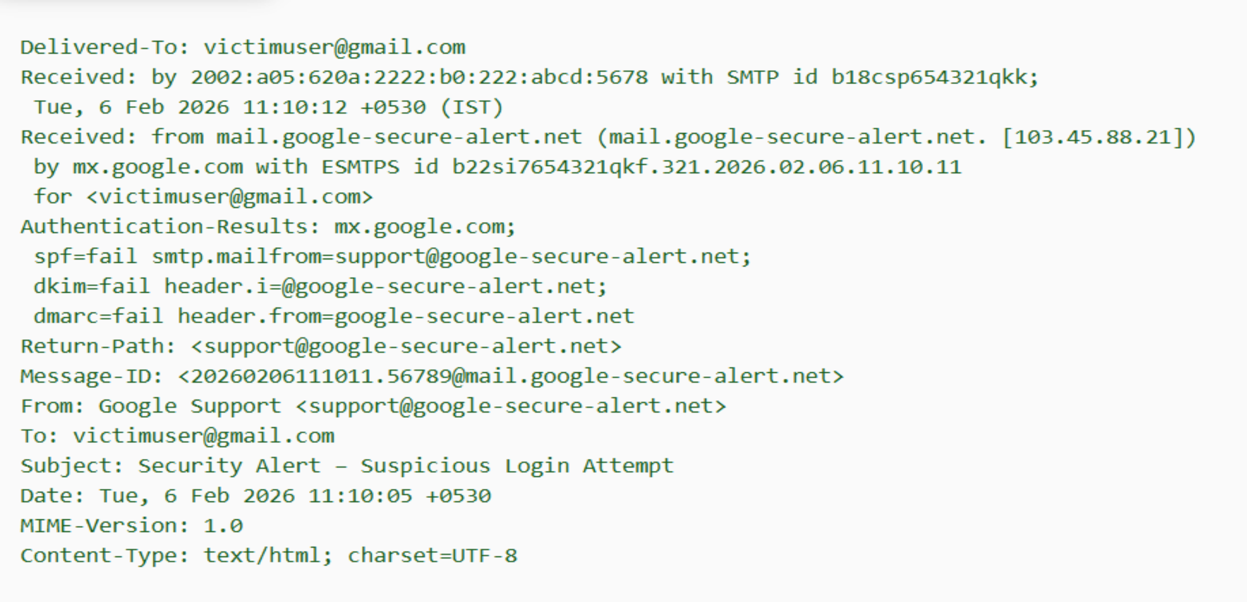
Failure to respond may result in account suspension.

Google Security Team

Fake Google Security Alert – Overview

This email pretends to be a Google security notification.
It mentions a login attempt from Russia to create fear.
The user is asked to secure their account via a fake recovery link.
The objective is to capture Google account credentials.

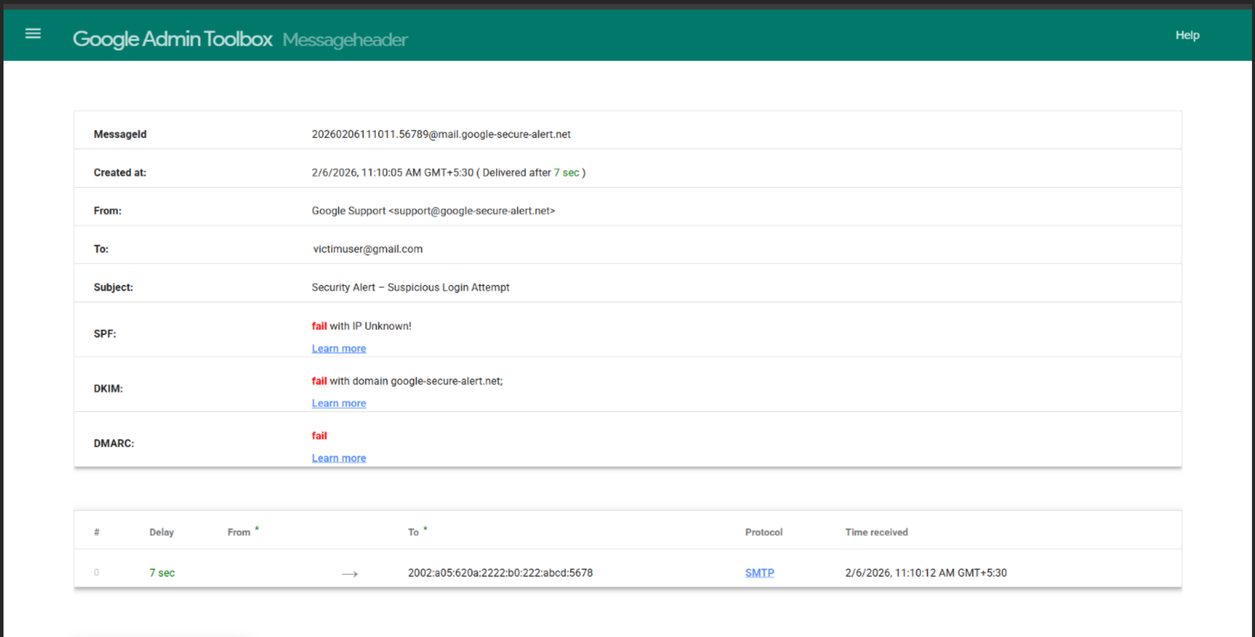
Header



```
Delivered-To: victimuser@gmail.com
Received: by 2002:a05:620a:2222:b0:222:abcd:5678 with SMTP id b18csp654321qkk;
 Tue, 6 Feb 2026 11:10:12 +0530 (IST)
Received: from mail.google-secure-alert.net (mail.google-secure-alert.net. [103.45.88.21])
 by mx.google.com with ESMTPS id b22si7654321qkf.321.2026.02.06.11.10.11
 for <victimuser@gmail.com>
Authentication-Results: mx.google.com;
 spf=fail smtp.mailfrom=support@google-secure-alert.net;
 dkim=fail header.i=@google-secure-alert.net;
 dmarc=fail header.from=google-secure-alert.net
Return-Path: <support@google-secure-alert.net>
Message-ID: <20260206111011.56789@mail.google-secure-alert.net>
From: Google Support <support@google-secure-alert.net>
To: victimuser@gmail.com
Subject: Security Alert – Suspicious Login Attempt
Date: Tue, 6 Feb 2026 11:10:05 +0530
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
```

Tools Used in This Investigation

- **Email Header Analysis Tool**
- **Google Admin Toolbox – Message header**



MessageId	20260206111011.56789@mail.google-secure-alert.net
Created at:	2/6/2026, 11:10:05 AM GMT+5:30 (Delivered after 7 sec)
From:	Google Support <support@google-secure-alert.net>
To:	victimuser@gmail.com
Subject:	Security Alert – Suspicious Login Attempt
SPF:	fail with IP Unknown! Learn more
DKIM:	fail with domain google-secure-alert.net; Learn more
DMARC:	fail Learn more

#	Delay	From *		To *	Protocol	Time received
0	7 sec		→	2002:a05:620a:2222:b0:222:abcd:5678	SMTP	2/6/2026, 11:10:12 AM GMT+5:30

Identification of Phishing Indicators

- Domain is not google.com
- SPF/DKIM/DMARC failed
- Suspicious domain extension (.net)
- Fake security alert
- Urgent login recovery request

Simple Explanation of How the Attack Works

The attacker sends a fake security alert claiming someone logged into the account. The victim panics and clicks “secure your account.”

Instead of Google, the link opens a fake login page.

Clear Prevention Tips for Users

- Check if sender domain is exactly google.com
- Never click login links from emails
- Visit official site manually
- Use Google’s security activity page directly
- Enable 2-Step Verification

Do’s and Don’ts

Do’s

- Verify suspicious login from official account dashboard
- Check full email address, not just display name

Don’ts

- Do not trust display name “Google Support”
- Do not enter credentials on redirected pages

Email Risk Classification

🔴 Phishing (High Risk)

Reason: Brand impersonation + failed authentication + malicious link.

Email Sample 3 – Fake PayPal Account Limitation

Summary

From: alert@secure-bank-login.com
Subject: Urgent: Verify Your Bank Account Immediately

EMAIL :-

Fake PayPal Account Limitation

Subject: Your PayPal Account Has Been Limited

Dear Customer,

Your PayPal account has been limited due to suspicious transactions.

Please confirm your identity:

http://paypal-verify-account.org/login

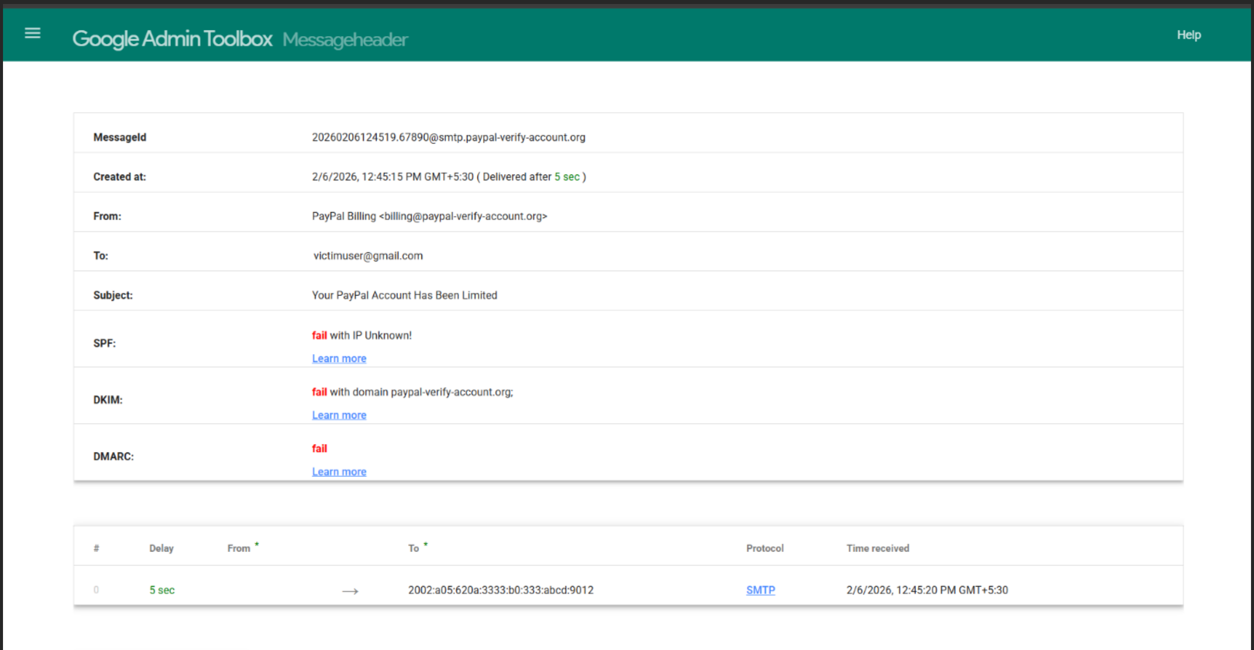
Failure to act may result in account closure.

PayPal Billing Department

Fake PayPal Account Limitation – Overview

This email impersonates PayPal's billing department.
It claims the account has been limited due to suspicious transactions.
The recipient is urged to confirm identity through a malicious link.
The purpose is to steal login and possibly financial information.

HEADER



MessageId	20260206124519.67890@smtp.paypal-verify-account.org
Created at:	2/6/2026, 12:45:15 PM GMT+5:30 (Delivered after 5 sec)
From:	PayPal Billing <billing@paypal-verify-account.org>
To:	victimuser@gmail.com
Subject:	Your PayPal Account Has Been Limited
SPF:	fail with IP Unknown! Learn more
DKIM:	fail with domain paypal-verify-account.org; Learn more
DMARC:	fail Learn more

#	Delay	From *		To *	Protocol	Time received
0	5 sec		→	2002:a05:620a:3333:b0:333:abcd:9012	SMTP	2/6/2026, 12:45:20 PM GMT+5:30

Tools Used in This Investigation

- **Email Header Analysis Tool**
- **Google Admin Toolbox – Message header**

Safe Browser Inspection Steps Used:

- Hovered over links (without clicking)
- Checked full URL structure
- Verified main domain name
- Examined suspicious keywords (secure, verify, alert)
- Checked if HTTPS was properly used
- Reviewed domain naming pattern

Findings:

- Domains are NOT official domains
- Contain impersonation keywords
- Look-alike domain structure
- Likely recently registered domains

Identification of Phishing Indicators

Across all three emails, the following indicators were identified:

SPF failure
DKIM failure
DMARC failure
Look-alike domain names
Urgent and threatening language
Generic greeting ("Dear User")
Suspicious login verification links
Mismatch between brand name and domain

Do’s and Don’ts for Employees

Do’s

- Verify sender domain before responding
- Contact organization through official website
- Use company email reporting procedure
- Keep antivirus and browser updated

Don’ts

- Do not click suspicious links
- Do not download unknown attachments
- Do not share login credentials
- Do not respond to urgent financial requests
- Do not ignore authentication failures

Email Risk Classification

Phishing (High Risk)

Reason: Payment service impersonation + authentication failure + deceptive domain.

Final Conclusion & Report Summary

Conclusion

This investigation analyzed three suspected phishing email samples impersonating a bank, Google, and PayPal.

Through structured header analysis and browser-level domain inspection, the emails were confirmed as high-risk phishing attempts due to:

- **SPF, DKIM, and DMARC authentication failures**
- **Look-alike and spoofed domains**
- **Social engineering tactics (urgency and fear)**
- **Credential harvesting intent**

All three emails were classified as:

High-Risk Phishing Emails

This project demonstrates how proper email header verification and safe browser inspection techniques can effectively identify phishing threats before damage occurs.

Key Topics Covered in This Report

- **Phishing Email Analysis**
- **Email Header Authentication (SPF, DKIM, DMARC)**
- **Domain Spoofing Detection**
- **Browser-Based URL Inspection**
- **Social Engineering Techniques**
- **Risk Classification (Safe / Suspicious / Phishing)**
- **Employee Awareness & Prevention Guidelines**
- **Do’s and Don’ts for Organizational Security**

SECURITY RECOMMENDATIONS

To reduce phishing risks, organizations should:

Conduct regular employee awareness training
Enable Multi-Factor Authentication (MFA)
Implement strong email filtering systems
Monitor SPF, DKIM, and DMARC policies
Establish a clear phishing reporting process
Encourage safe browsing habits

Phishing prevention is not only a technical responsibility but also a user awareness responsibility.
