Phishing Detection & Awareness Report :

Intern Name : THEJAS R SHETTY

CIN ID : FIT/FEB26/CS6248

Internship : Future Interns – Cyber Security Internship

Task 2 –> Phishing Email Detection & Awareness System

Repository Name: FUTURE_CS_02

Submission Date: 21/02/2026

1. Overview :

Phishing is a social engineering attack used by cybercriminals to deceive individuals into revealing confidential information such as login credentials, financial details, or personal data. Attackers impersonate legitimate organizations to gain the victim's trust.

This report presents a structured analysis of four suspected phishing emails using header authentication verification and manual inspection techniques. The analysis focuses on identifying:

- Email authentication failures (SPF, DKIM, DMARC)
- Domain spoofing attempts
- Social engineering tactics
- Suspicious content indicators

Based on technical analysis and phishing indicators, **all four email samples were classified as PHISHING – >HIGH RISK.**

2. Objectives of the Analysis :

The purpose of this task was to :

- Identify phishing indicators in suspicious emails
- Analyze email headers using professional tools
- Evaluate SPF, DKIM, and DMARC results
- Classify email risk levels
- Provide user awareness and prevention guidelines

3. Tools Used :

The following tools were used for analysis :

- ❖ MXToolbox Header Analyzer
- ❖ Web browser for link inspection

4. Email Sample Analysis :

Email 1 – Fake Account Lock Alert

Subject: Urgent: Your Account Will Be Locked
Sender: security@secure-account-alert.com

Identified Phishing Indicators

- Use of urgent and threatening language
- Suspicious sender domain not associated with a legitimate company
- Generic greeting (“Dear User”)
- Embedded suspicious verification link

Header Authentication Results

- SPF: Fail
- DKIM: None
- DMARC: Fail

Risk Classification :

PHISHING – >HIGH RISK

Screenshots :

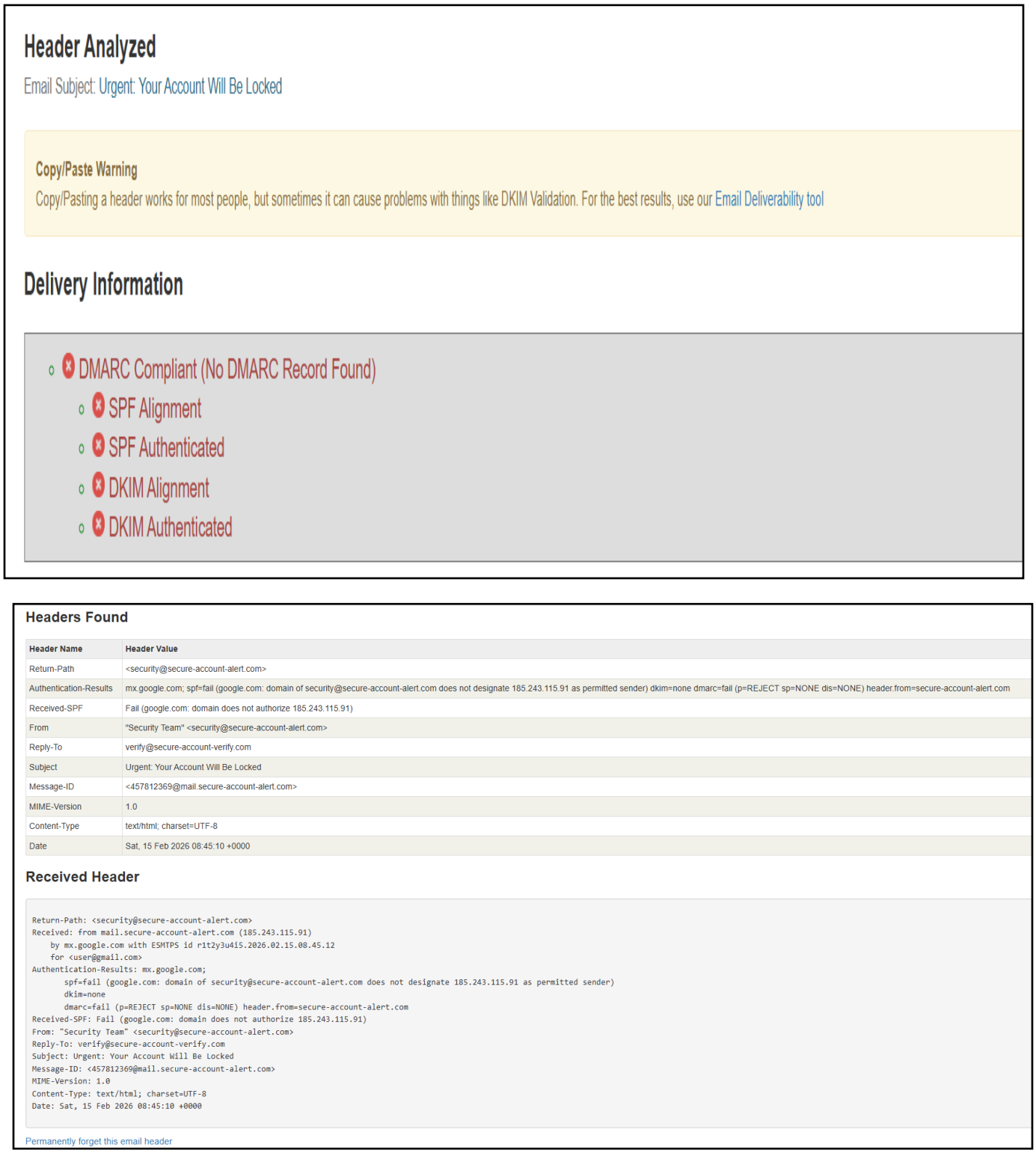


***Fig 1 : Email 1** Header Analysis Result*

Email 2 – Fake Lottery Winning Email

Subject: Congratulations! You Won ₹5,00,000
Sender: lottery@international-prize.net

Identified Phishing Indicators

- Unrealistic monetary reward offer
- Unknown and suspicious sender domain
- Request for personal information
- No prior participation in lottery
-

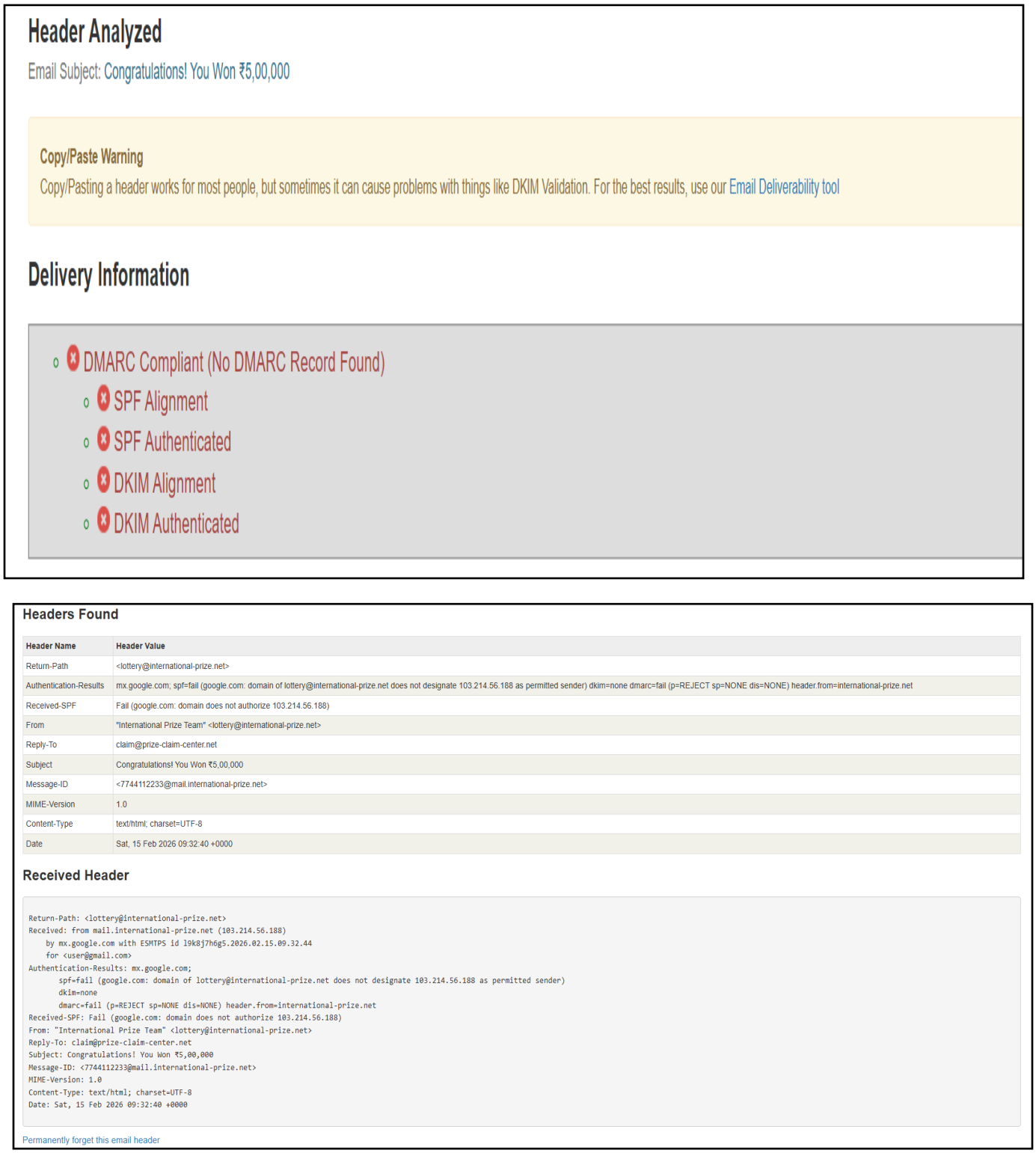
Header Authentication Results

- SPF: Fail
- DKIM: None
- DMARC: Fail

Risk Classification :

PHISHING – >HIGH RISK

Screenshots :



Header Analyzed

Email Subject: Congratulations! You Won ₹5,00,000

Copy/Paste Warning

Copy/Pasting a header works for most people, but sometimes it can cause problems with things like DKIM Validation. For the best results, use our Email Deliverability tool

Delivery Information

- DMARC Compliant (No DMARC Record Found)
  - SPF Alignment
  - SPF Authenticated
  - DKIM Alignment
  - DKIM Authenticated

Headers Found

Header Name	Header Value
Return-Path	<lottery@international-prize.net>
Authentication-Results	mx.google.com; spf=fail (google.com: domain of lottery@international-prize.net does not designate 103.214.56.188 as permitted sender) dkim=none dmarc=fail (p=REJECT sp=NONE dis=NONE) header.from=international-prize.net
Received-SPF	Fail (google.com: domain does not authorize 103.214.56.188)
From	"International Prize Team" <lottery@international-prize.net>
Reply-To	claim@prize-claim-center.net
Subject	Congratulations! You Won ₹5,00,000
Message-ID	<7744112233@mail.international-prize.net>
MIME-Version	1.0
Content-Type	text/html; charset=UTF-8
Date	Sat, 15 Feb 2026 09:32:40 +0000

Received Header

```
Return-Path: <lottery@international-prize.net>
Received: from mail.international-prize.net (103.214.56.188)
    by mx.google.com with ESMTPS id l9k8j7h6g5.2026.02.15.09.32.44
    for <user@gmail.com>
Authentication-Results: mx.google.com;
       spf=fail (google.com: domain of lottery@international-prize.net does not designate 103.214.56.188 as permitted sender)
       dkim=none
       dmarc=fail (p=REJECT sp=NONE dis=NONE) header.from=international-prize.net
Received-SPF: Fail (google.com: domain does not authorize 103.214.56.188)
From: "International Prize Team" <lottery@international-prize.net>
Reply-To: claim@prize-claim-center.net
Subject: Congratulations! You Won ₹5,00,000
Message-ID: <7744112233@mail.international-prize.net>
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Date: Sat, 15 Feb 2026 09:32:40 +0000
```

Permanently forget this email header

***Fig 2 : Email 2** Header Analysis Result*

Email 3 – Fake Job Offer (Amazon Spoof)

Subject: Job Offer – Immediate Joining
Sender: hr@amaz0n-careers.com

Identified Phishing Indicators

- Domain spoofing (amaz0n instead of amazon)
- Unexpected job offer without prior application
- Request for identity proof
- Suspicious attachment/link

Header Authentication Results

- SPF: Fail
- DKIM: None
- DMARC: Fail

Risk Classification :

PHISHING –> HIGH RISK

Screenshots :

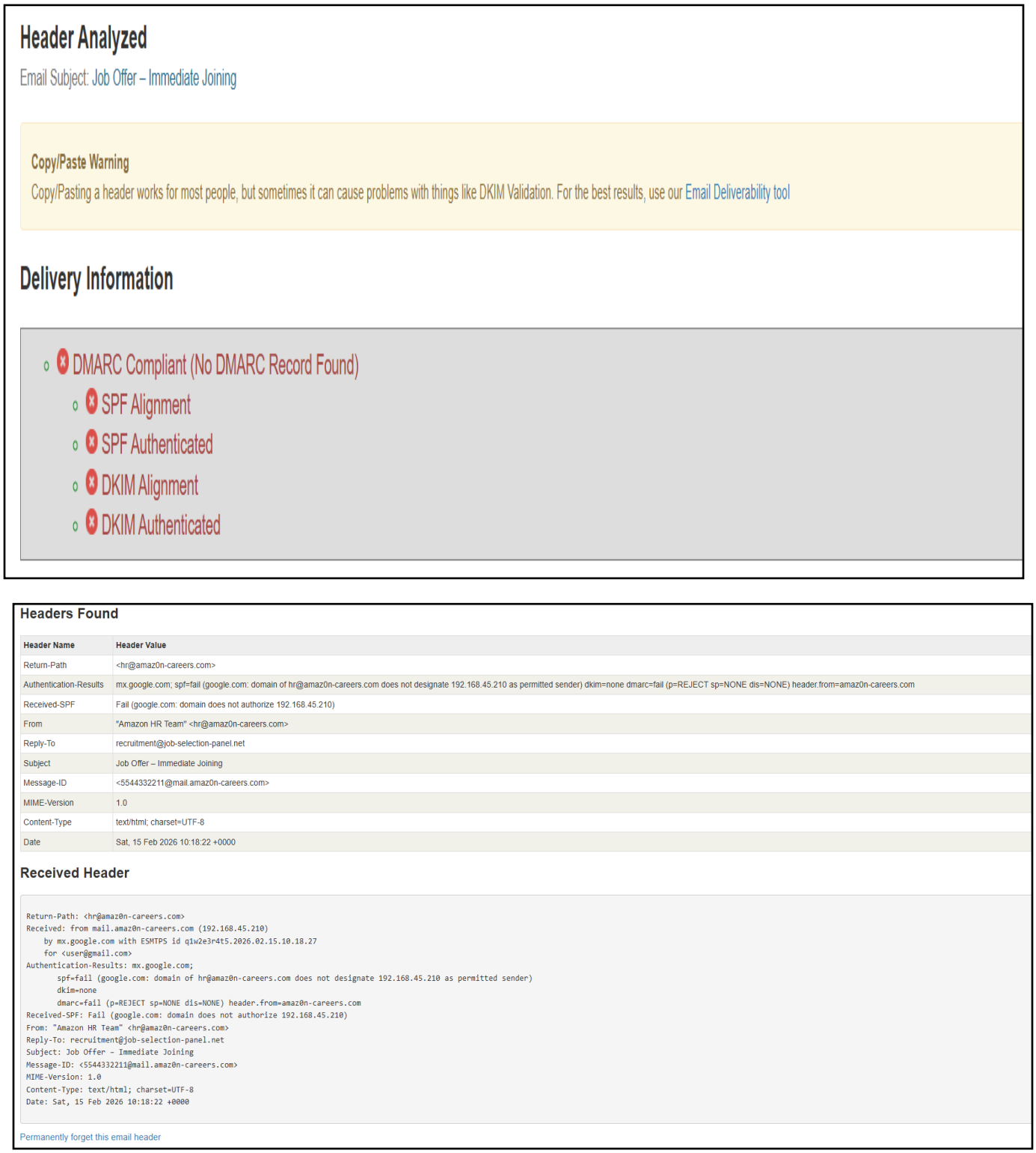


***Fig 3 : Email 3** Header Analysis Result*

Email 4 – Fake PayPal Security Alert

Subject: Important Notice: Unusual Login Attempt Detected
Sender: support@paypaI-security.com

Identified Phishing Indicators

- Domain spoofing (paypaI using capital “I”)
- Urgent security warning
- Suspicious verification link
- Request for account credential confirmation

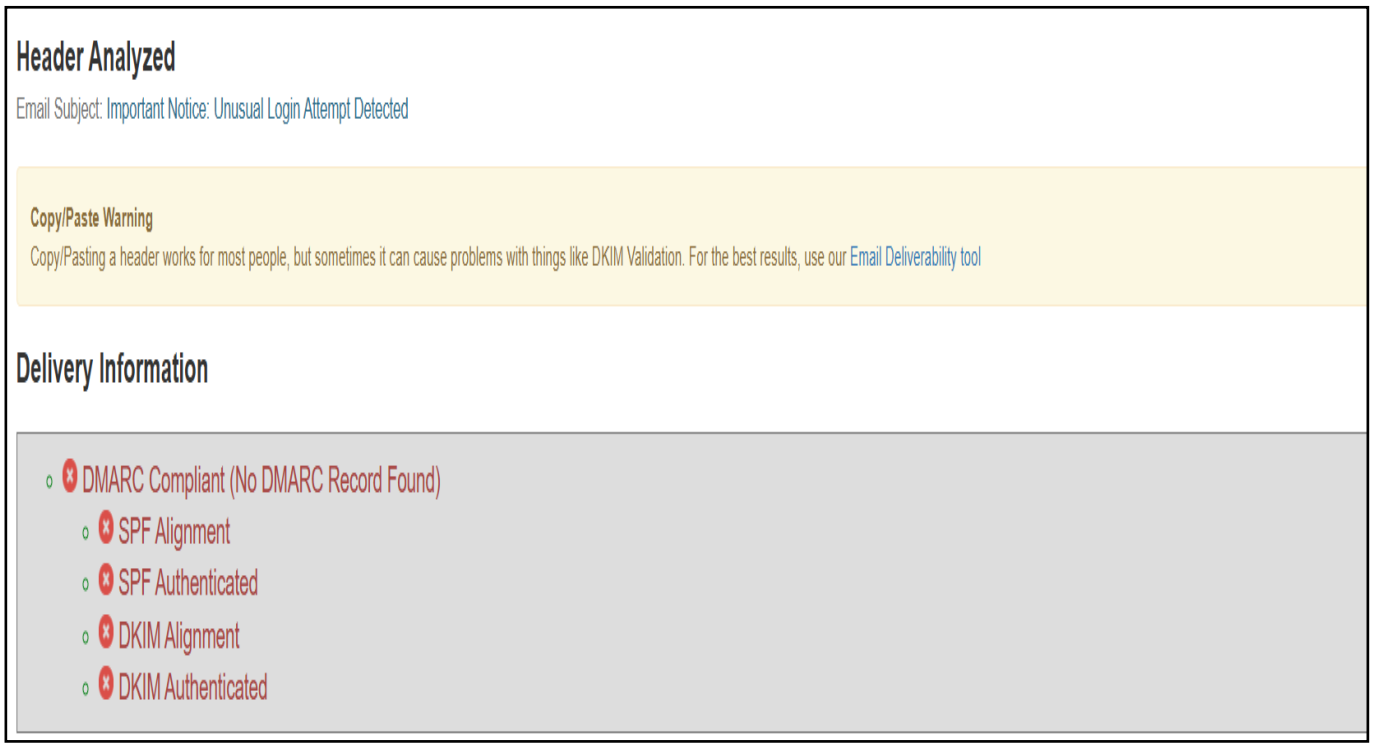
Header Authentication Results

- SPF: Fail
- DKIM: None
- DMARC: Fail

Risk Classification :

PHISHING –> HIGH RISK

Screenshots :



Header Name	Header Value
Return-Path	<support@paypal-security.com>
Authentication-Results	mx.google.com; spf=fail (google.com: domain of support@paypal-security.com does not designate 102.87.44.156 as permitted sender) dkim=none dmarc=fail (p=REJECT sp=NONE dis=NONE) header.from=paypal-security.com
Received-SPF	Fail (google.com: domain does not authorize 102.87.44.156)
From	"PayPal Security Team" <support@paypal-security.com>
Reply-To	verify@paypal-account-verification-secure.com
Subject	Important Notice: Unusual Login Attempt Detected
Message-ID	<6677889900@mail.paypal-security.com>
MIME-Version	1.0
Content-Type	text/html; charset=UTF-8
Date	Sat, 15 Feb 2026 11:05:29 +0000

Received Header

```
Return-Path: <support@paypaI-security.com>
Received: from mail.paypaI-security.com (102.87.44.156)
    by mx.google.com with ESMTPS id p9o8i7u6y5.2026.02.15.11.05.33
    for <user@gmail.com>
Authentication-Results: mx.google.com;
       spf=fail (google.com: domain of support@paypaI-security.com does not designate 102.87.44.156 as permitted sender)
       dkim=none
       dmarc=fail (p=REJECT sp=NONE dis=NONE) header.from=paypaI-security.com
Received-SPF: Fail (google.com: domain does not authorize 102.87.44.156)
From: "PayPal Security Team" <support@paypaI-security.com>
Reply-To: verify@paypal-account-verification-secure.com
Subject: Important Notice: Unusual Login Attempt Detected
Message-ID: <6677889900@mail.paypaI-security.com>
MIME-Version: 1.0
Content-Type: text/html; charset=UTF-8
Date: Sat, 15 Feb 2026 11:05:29 +0000
```

Permanently forget this email header

***Fig 4 : Email 4** Header Analysis Result*

5. Summary of Technical Findings :

All analyzed emails showed the following phishing characteristics :

1. Unauthorized sending servers
2. Failed SPF authentication
3. Missing or invalid DKIM signature
4. Failed DMARC authentication
5. Domain spoofing techniques
6. Social engineering tactics

Header Authentication Results	
SPF	**Fail**
DKIM	**None**
DMARC	**Fail**

These indicators strongly confirm that all emails were phishing attempts.

6. How Phishing Attacks Work :

Phishing attacks rely on psychological manipulation rather than technical vulnerabilities. Attackers impersonate trusted brands or institutions and create a sense of urgency or reward.

Typical phishing attack flow:

1. Victim receives fraudulent email.
2. Email contains malicious link or attachment.
3. Victim clicks link and enters sensitive information.
4. Data is transmitted to attacker-controlled servers.
5. Attacker uses credentials for fraud or identity theft.

7. Prevention Guidelines for Users :

To reduce phishing risks, Users should follow these safety practices :

- Carefully verify sender email addresses
- Check domain spelling carefully
- Do not click suspicious links
- Avoid sharing sensitive information via email
- Enable two-factor authentication
- Report suspicious emails to the IT/security team

8. Do’s and Don’ts for Employees :

Do’s

- Verify unexpected requests independently
- Hover over links to preview URLs
- Use official company portals
- Report suspicious emails immediately

Don’ts

- Do not click links in urgent unknown emails
- Do not download unexpected attachments
- Do not share sensitive data over email
- Do not ignore authentication warning signs

9. Organizational Security Recommendations :

Organizations should implement:

- SPF, DKIM, and DMARC email authentication policies
- Advanced email filtering solutions
- Regular phishing awareness training
- Phishing simulation exercises
- Incident response and reporting procedures

10. Conclusion :

This analysis confirmed that all four email samples were phishing attempts. Email header analysis and phishing indicator inspection revealed multiple authentication failures and spoofing techniques.

This project demonstrates practical cybersecurity skills in phishing detection, email analysis, and security awareness reporting.

This task strengthens cybersecurity skills in identifying and preventing phishing threats in real-world environments.

---------- **END OF REPORT**----------