Phishing Email Header Analysis Report

Basic Info

From: support@paypal-secureaccount.com

Subject: Important: Verify Your Account to Avoid Suspension

Reported Issue: Fake PayPal email asking the user to verify account urgently.

Key Indicators Found in the Header

1. Sender Address Spoofed

   - Detail: paypal-secureaccount.com

   - Explanation: Looks like PayPal but is not a valid PayPal domain.

2. Mismatched 'From' and 'Return-Path'

   - Detail: From: support@paypal-secureaccount.com, Return-Path: something else

   - Explanation: This mismatch shows it is not a legit sender.

3. No SPF/DKIM Authentication

   - Detail: SPF: Fail / DKIM: Not present

   - Explanation: The domain owner has not approved this sender - possible forgery.

4. IP Address Blacklisted

   - Detail: Source IP listed in RBL

   - Explanation: Indicates the sending server is known for spam/phishing.

5. Unusual Mail Server

   - Detail: Server: smtp.fakehost.in

   - Explanation: Not a recognized mail server for PayPal.

6. Received Path Too Long

   - Detail: Many 'Received' headers

   - Explanation: Often a sign of email routing trickery.

7. Urgent Language in Subject

   - Detail: Important: Verify Your Account

Phishing Email Header Analysis Report

- Explanation: Tries to scare you into clicking links.

Conclusion

This email is a phishing attempt:

- It uses spoofed sender info

- Has failing email authentication

- Tries to trick users with urgency and threats

- Includes a malicious link or attachment