Phishing Email Analysis Report

1. Sender Information

Observed sender: security-update@paypa1.com
Suspicious trait: The domain uses “paypa1.com” instead of the legitimate paypal.com (typosquatting).

2. Email Header Analysis

Return-Path domain does not match the 'From' address.
Received headers show origin from an unknown mail server in another country.
SPF/DKIM/DMARC checks failed (from header analyzer).

3. Links & Attachments

Displayed hyperlink: https://paypal.com/security-check
Actual link: http://192.185.21.55/login/verify (IP-based, suspicious).
Attachment included: update_info.html (possible phishing form).

4. Email Body Language

Message stated: "Your account has been suspended due to unusual activity. Please verify your account immediately to avoid permanent closure."
Indicators: Urgent and threatening tone to pressure recipient.

5. Spelling and Grammar

Contains errors like: "Your accont is limitted. Please verfy now."
Such mistakes are common in phishing attempts.

6. Overall Phishing Indicators Identified

1. Spoofed sender address (typosquatted domain).
2. Header anomalies (failed authentication, mismatched sending server).
3. Mismatched URLs (text vs hover link).
4. Suspicious IP-based link instead of official domain.
5. Urgent/threatening tone urging immediate action.
6. Grammar/spelling errors lowering legitimacy.
7. Unexpected attachment designed to harvest data.

Conclusion

This email shows multiple phishing characteristics, including spoofed domains, header inconsistencies, malicious links, and social engineering tactics. It should be reported to the appropriate authority (e.g., PayPal’s phishing email report service) and deleted immediately without clicking links or opening attachments.