Phishing Email Analysis Report

📧 1. Email Overview

- **Sender:** support@paypalsecurity-alert.com
- **Subject:** *Urgent: Account Suspension Notice!*
- **Date:** June 24, 2025
- **Recipient:** user@example.com

---

2. Phishing Indicators

Category	Observations
Spoofed Address	Domain paypalsecurity-alert.com is not official. Genuine PayPal uses paypal.com.
Suspicious Link	Displayed as https://www.paypa1-verification.com → Misspelled "paypal".
Urgent Language	Phrases like *"Account Suspended"*, *"Verify within 24 hours"* used to scare user.
Generic Greeting	No personalization: "Dear Customer" instead of real name.
Poor Domain Match	Link domain does not match email domain.
Lack of Branding	No logo or official styling.
Header Issues	If header is checked, Return-Path and From don't match (spoofing likely).
Grammar Errors	"PayPal Security Team" is not the official sign-off used by PayPal.

---

3. Tools Used

- MXToolbox Email Header Analyzer
- VirusTotal for URL checking
- Google Header Analyzer

---

4. Conclusion

This email is a **phishing attempt** designed to:

- Trick the user into giving credentials via a **fake login page**.
- Use **email spoofing** and social engineering (urgency, fear).

Recommendation:

- Do **NOT click** the link.
- Report to the IT/security team.
- Educate others about such threats