■ PHISHING EMAIL ANALYSIS REPORT

Date: August 5, 2025
Analyst: [Your Name]
Sample Source: Publicly available phishing email repository

1. ■ Email Overview

Subject: "URGENT: Your Account Will Be Suspended!"
Sender: support@paypa1.com
Recipient: [Redacted for Privacy]
Date Received: August 2, 2025

2. ■■■■■ Sender's Email Address

Suspicious Email: support@paypa1.com
Analysis: The domain is attempting to mimic "paypal.com" by substituting the letter "l" with the number "1". This is a classic email spoofing technique.

3. ■ Header Discrepancies

- SPF: Fail (unauthorized sender domain)
- DKIM: Fail (signature mismatch)
- Return-Path: mailer@unknownserver.xyz
- IP Address Origin: Geolocated to an ISP in Eastern Europe

4. ■ Suspicious Links or Attachments

Attachment: AccountDetails.pdf.exe – Disguised executable file with a double extension.
Hyperlink Text: "Click here to secure your account"
Displayed URL: https://paypal.com/security
Actual URL (on hover): http://malicious-site.ru/login.php

5. ■■ Urgent or Threatening Language

- Your account has been temporarily suspended.
- Failure to act within 24 hours will result in permanent suspension.
- You must verify your account immediately.

6. ■ Mismatched URLs

Displayed URL: Reputable domain (paypal.com)
Actual URL: Redirects to a phishing site hosted overseas

7. ✍■ Spelling or Grammar Errors

- We noticed unussual activity on you’re account.
- Pleese confirm your login detales.

8. ■ Summary of Phishing Traits Found

Trait	Present
Spoofed email address	■ Yes
Header authentication failure	■ Yes
Suspicious/malicious attachment	■ Yes
Mismatched URLs	■ Yes
Urgent or threatening language	■ Yes
Spelling and grammar issues	■ Yes
Generic greeting (“Dear user”)	■ Yes

■■ Conclusion

This email is a confirmed phishing attempt designed to steal user credentials by impersonating PayPal. The spoofed sender address, mismatched URLs, urgency tactics, and grammar issues all align with typical phishing red flags.

Recommendation: Do not click any links or download attachments. Report the email to your email provider and delete it immediately.