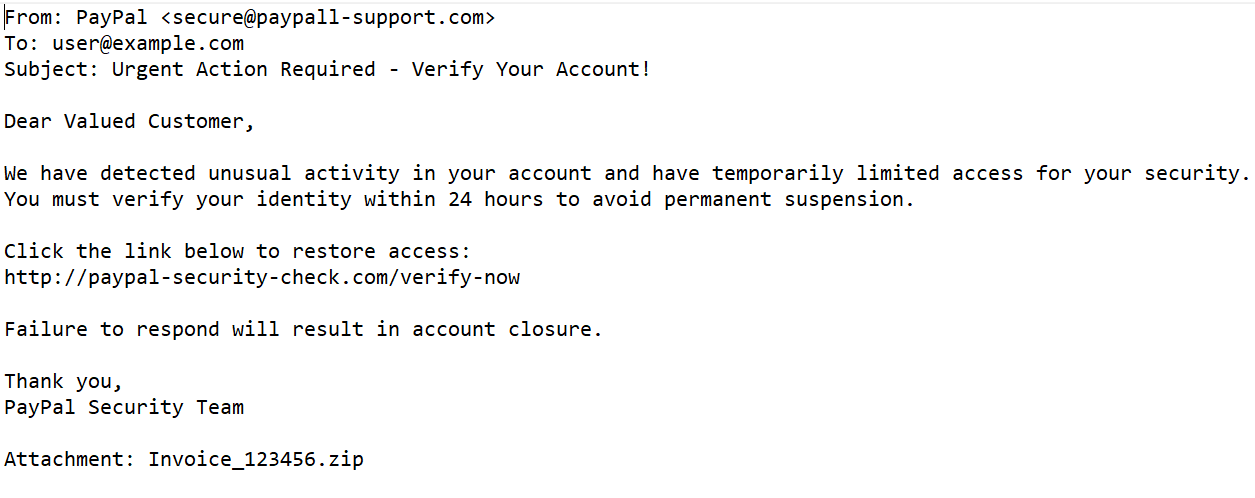
# Phishing Email Analysis Report

**Sample Email**



## Email Summary

Subject: Urgent Action Required - Verify Your Account!

Sender Email: secure@paypall-support.com (Spoofed)

## Header Analysis

SPF: FAIL, DKIM: FAIL, DMARC: FAIL

Received from IP: 194.123.45.67 (Not associated with PayPal)

Conclusion: Fails email authentication checks — phishing suspected.

## Suspicious Links

Displayed link: http://paypal-security-check.com/verify-now

Actual destination is not owned by PayPal — likely a credential stealing site.

## Suspicious Attachment

Attachment: Invoice\_123456.zip

Conclusion: Potential malware delivery — should not be opened.

## Urgent or Threatening Language

Phrases like 'Urgent Action Required' and 'Verify within 24 hours' indicate social engineering attempts.

## Mismatched URLs

Link text appears legitimate, but redirects to fraudulent domain (paypal-security-check.com).

## Spelling/Grammar Errors

Minor language and formatting errors; unprofessional tone.

## Conclusion

This email contains multiple red flags indicating phishing, including spoofed sender, suspicious links and attachments, failed header checks, and emotionally manipulative language.

| **Concept** | **Explanation** |
| --- | --- |
| **Phishing** | A type of cyber attack where fake emails trick you into revealing personal info. |
| **Spoofing** | Faking the sender’s email address to appear legitimate. |
| **Email Headers** | Metadata showing where the email came from and how it was handled. |
| **SPF/DKIM/DMARC** | Authentication methods to verify email legitimacy. |
| **Social Engineering** | Manipulation techniques (urgency, fear) used to deceive users. |
| **Malware Attachments** | Files (usually .zip/.exe/.doc) meant to infect the system. |
| **Fake URLs** | Links disguised to look real but lead to attacker websites. |