# Phishing Email Analysis Report

## Objective

To identify and analyze phishing characteristics in a suspicious email, and prepare a structured report of all findings.

## Tools Used

- Email Client: Gmail / Outlook (to view full email and header)  
- Saved Email File (Text format): For offline analysis  
- Free Header Analyzer: MXToolbox, Mailheader Analyzer

## Step-by-Step Analysis

### 1. Obtaining a Sample Email

The suspicious email claimed to be from PayPal Security Team.  
Subject Line: 'Urgent: Verify Your Account Now or Your Account Will Be Blocked'  
Such urgent subject lines are a common phishing trick to create panic.

### 2. Sender’s Email Address (Spoofing Check)

Displayed sender: support@paypa1.com  
Genuine sender: @paypal.com  
Difference: Here '1' (digit one) is used instead of 'l' (letter L).  
Indicator: This is domain spoofing – attacker tries to mimic PayPal’s domain.

### 3. Email Header Analysis

Using MXToolbox header analyzer, the email showed:  
- Originating IP address from Russia, whereas PayPal servers are US-based.  
- 'Return-Path' field did not match 'From' field.  
- SPF (Sender Policy Framework) check failed → meaning the email is not authorized by the real domain.  
Indicator: Header mismatch = spoofed sender identity.

### 4. Suspicious Links & Attachments

Hyperlink shown in the body: https://www.paypal.com  
But when hovered: http://malicious-site.ru/login  
Email also had an attachment: Invoice.zip (likely contains malware or ransomware).  
Indicator: Fake/mismatched links & risky attachments.

### 5. Urgent / Threatening Language

Email body contained lines like:  
- 'Your account has been temporarily locked due to unusual activity.'  
- 'Verify your identity within 24 hours or your account will be permanently closed.'  
Indicator: Fear tactics, urgency → classic phishing technique.

### 6. Mismatched URLs

Example:  
Text showed: Click here to secure your account  
Real URL: http://hackersite.ru/paypal  
Indicator: Hidden redirection → user may unknowingly give credentials to attacker.

### 7. Spelling & Grammar Errors

Errors found:  
- 'Your account are suspended'  
- 'Kindly verify immediatelly'  
Genuine companies rarely send emails with such poor English.  
Indicator: Low-quality language = phishing sign.

### 8. Summary of Phishing Traits

|  |  |  |
| --- | --- | --- |
| Phishing Indicator | Observation in Email | Why Suspicious |
| Sender Address | support@paypa1.com | Spoofed domain (1 instead of l) |
| Email Header | Originating IP from Russia, SPF failed | Does not match real PayPal servers |
| Links | Shown: paypal.com, Real: malicious-site.ru | Fake links to steal login credentials |
| Attachments | Invoice.zip | Possible malware |
| Urgent Language | Verify in 24 hours or blocked | Creates fear to force quick action |
| Grammar Errors | Your account are suspended | Poor grammar, unprofessional |
| Mismatched URLs | Hover links lead to different domains | Classic phishing redirection |

## Conclusion

This email is 100% a phishing attempt.  
- The attacker tried to impersonate PayPal by using a spoofed email address.  
- The email contained malicious links, suspicious attachments, and urgent threatening language.  
- Technical header analysis confirmed that the email was not sent from PayPal servers.  
- The purpose of this phishing email is to steal login credentials and possibly install malware on the victim’s device.