Phishing Email Analysis Report

# Task

Analyze a phishing email sample and identify all indicators using structured methodology.

# Tools Used

• Email Client (for viewing email)  
• Free Online Header Analyzer: MXToolbox  
• Hover-over feature to inspect URLs  
• Web-based WHOIS and IP lookup tools

# Step-by-Step Analysis

## Step 1: Obtain a Sample Phishing Email

• Source: Public phishing email archive  
• Type: Text-based sample  
• Subject Line: “URGENT: Account Suspension Warning”  
• Sender: support@paypaI.com (Note: fake domain with capital 'i' instead of 'l')

## Step 2: Examine Sender's Email Address

• Actual sender: support@paypaI.com  
• Legitimate version: support@paypal.com  
• Observation: Minor domain spoofing using visually similar characters.  
• Conclusion: Spoofed sender address used to trick the recipient.

## Step 3: Analyze Email Headers

Used MXToolbox Email Header Analyzer  
  
Header Findings:  
• SPF Check: ❌ Fail  
• DKIM Signature: ❌ Not Signed  
• DMARC Policy: ❌ Fail  
• Origin IP: 178.54.32.12 (Registered in Russia)  
  
Conclusion: Failing SPF/DKIM/DMARC is a strong indicator of phishing.

## Step 4: Identify Suspicious Links or Attachments

• Attachment: Account\_Verification\_Form.zip  
• Displayed Link: https://www.paypal.com/verify-now  
• Actual URL (hover): http://paypa1-login.ru/secure  
Conclusion: Dangerous ZIP file and phishing URL.

## Step 5: Look for Urgent or Threatening Language

• Email Message Excerpt:  
 “If you fail to respond within 24 hours, your PayPal account will be suspended permanently.”  
Conclusion: Creates urgency and fear.

## Step 6: Note Mismatched URLs

• Example:  
 - Shown: https://paypal.com/  
 - Actual: http://paypa1-login.ru  
Conclusion: URL mismatch is a classic phishing indicator.

## Step 7: Check for Grammar or Spelling Errors

• Examples:  
 - “We reccomend you to verify immediatelly.”  
 - “Your acount is under suspenssion due to unrecognise login.”  
Conclusion: Multiple grammar/spelling errors suggest malicious intent.

## Step 8: Summarize Phishing Traits

• Spoofed sender: support@paypaI.com  
• Failed authentication: SPF/DKIM/DMARC  
• Suspicious origin IP: Russian server  
• Mismatched URLs: Hover shows different link  
• Suspicious ZIP file: Potential malware  
• Threatening tone: Urgent account suspension  
• Poor language: Grammar/spelling issues

# Final Conclusion

This email clearly exhibits all major phishing indicators:  
- Email spoofing  
- Header manipulation  
- Fake domains  
- Malicious attachments  
- Deceptive tone and language  
The combination of these elements confirms that this is a phishing attempt.

# Learning Outcome

• Gained practical skills in phishing email analysis.  
• Improved awareness of social engineering and spoofing tactics.  
• Understood how to use tools like header analyzers and URL inspectors.