Step 7: Summary of Phishing Traits

Objective:

To compile all the findings from previous steps and clearly list out the phishing indicators found in the email.

Summary of Phishing Indicators:

1. **Spoofed Sender Email**:
   - Email came from support@paypa1.com instead of the real paypal.com
   - Domain used number "1" instead of letter "l" — a common trick

2. **Failed Authentication**:
   - SPF and DKIM checks failed in the header analysis
   - Return-Path was different from From address (scammer@malicious.com)

3. **Suspicious Link**:
   - Hyperlink text was disguised as PayPal
   - Real URL was http://paypal-security-alert.com/login (not PayPal)

4. **Malicious Attachment**:
   - File named “Account_Update.exe” – an executable, likely malware
   - Flagged on VirusTotal

5. **Social Engineering (Language Tricks)**:
   - Used urgency (“24 hours” deadline)
   - Created fear (“Your account will be suspended”)
   - Claimed authority (“PayPal Security Team”)

6. **Grammar and Formatting Errors**:

- Unprofessional phrases like “This is your final warning”
- Generic greeting: “Dear Customer”
- Repetitive threats

✅ **Final Conclusion:**

The email exhibits multiple signs of phishing — spoofed identity, failed security checks, malicious content, and manipulation tactics. These findings confirm that the email is not legitimate and is designed to deceive the recipient.

This report improves awareness of how phishing attacks are structured and how to analyze them.