Phishing Email Analysis Report

1. Email Sample (Suspicious Email Text)

From: PayPaI Support
Subject: Urgent: Verify your account immediately
Body:
Dear Customer,
Your PayPal account has been limited due to suspicious activity.
Please click the link below to verify your account and restore full access:
http://secure-paypal-login-update.com
Failure to verify within 24 hours will result in account suspension.
Thank you,
PayPal Security Team
Attachment: Account_Verification_Form.zip

2. Phishing Indicators Identified

1. **Sender Email Spoofing**: Domain is *paypa1-secure.com* instead of official *paypal.com*.
2. **Suspicious URL**: Hidden behind text, points to *secure-paypal-login-update.com*.
3. **Urgent / Threatening Language**: “Verify immediately or account suspension.”
4. **Spelling / Grammar Tricks**: “PayPaI” with hidden character swap.
5. **Unusual Attachment**: *Account_Verification_Form.zip*.
6. **Header Analysis**: Return-path mismatch, SPF/DKIM failed.

3. Why This Is Dangerous

- Can steal login credentials via fake link.
- Attachment may install malware.
- Uses social engineering (fear + urgency).

4. Recommended Actions

- Do NOT click links or open attachments.
- Report email to phishing@paypal.com.
- Block sender domain.
- Educate users about spotting red flags.

5. Key Learning Outcomes

- Detect spoofed addresses.
- Identify fake domains & mismatched URLs.
- Understand header analysis.
- Recognize social engineering tactics in phishing.