Phishing Email Analysis Report

1. Sample Phishing Email

Subject: Urgent: Your PayPal Account Has Been Suspended
From: PayPal Security Alert <support@paypalsecurity-alert.com>
To: user@example.com

Dear Customer,

We noticed unusual activity in your PayPal account and have temporarily limited it to protect your information.
Please verify your identity by logging in through the secure link below:
👉 https://paypal.com.recovery-alerts.info/login

Failure to confirm within 24 hours will result in permanent suspension.

Thank you,
PayPal Security Team

2. Sender Email Analysis

The sender email 'support@paypalsecurity-alert.com' is suspicious as it mimics a legitimate PayPal address but uses a domain not owned by PayPal. This is a common spoofing technique.

3. Header Analysis

Using MXToolbox header analyzer, the following discrepancies were found:
- SPF Check: Fail
- DKIM: None
- Return-Path: return@fraudlink.biz
- Received from: IP 185.65.34.178 (not associated with PayPal)
These indicators suggest the email did not originate from a trusted server.

4. Suspicious Links and Attachments

- Link: https://paypal.com.recovery-alerts.info/login → This is a lookalike domain and not owned by PayPal.
- Attachment: Secure_Account.html → This HTML file opens a fake PayPal login page for credential harvesting.

5. Urgent or Threatening Language

Phrases such as 'Failure to confirm within 24 hours will result in permanent suspension' use fear tactics to pressure the recipient into taking immediate action without thinking critically.

6. Mismatched URLs

Although the displayed link appears to be 'paypal.com', hovering over it reveals the real destination is 'paypal.com.recovery-alerts.info/login', which is not affiliated with PayPal.

7. Spelling and Grammar Errors

Minor grammatical issues, such as awkward phrasing ('Your account is at risked of being closure'), indicate a lack of professional language, common in phishing emails.

8. Summary of Phishing Traits

- Spoofed sender address
- Failed SPF/DKIM records
- Mismatched URLs
- Suspicious attachment
- Urgent and threatening language
- Grammatical errors
- Links redirect to untrusted domains