Phishing Email Analysis Report

Task 2: Analyze a Phishing Email Sample

Objective:

To identify phishing characteristics in a suspicious email and report all indicators found.

Sample Email (Simulated):

From: support@paypalsecurity.com

To: you@example.com

Subject: Your PayPal Account Has Been Limited

Dear Customer,

We noticed suspicious activity in your PayPal account. For your protection, we have temporarily limited access.

Please verify your identity immediately by clicking the secure link below:

https://paypal-security-check.com/login

Failure to do so will result in permanent suspension of your account.

Thank you for your cooperation.

Sincerely,

PayPal Security Team

Phishing Indicators Identified:

1. **Email Spoofing**:
   - The sender address looks like it belongs to PayPal but uses the domain `paypalsecurity.com`, which is not official.
   - The real domain used by PayPal is `paypal.com`. This is a lookalike and is a classic case of spoofing.

2. **Email Header Discrepancies** (Simulated via MXToolbox or Google Header Analyzer):
   - SPF: FAIL - the email fails domain validation (spoofed)
   - DKIM: FAIL - not signed by the trusted domain
   - Return-Path: scammer@gmail.com (does not match sender)
   - Reply-To: scammer@gmail.com (redirects responses to attacker)
   - Received: Email originates from unknown/suspicious IP, not linked to PayPal

3. **Suspicious URL**:
   - The URL appears secure but is fake: `paypal-security-check.com` is not a real PayPal domain.

4. **Urgent Language**:
   - Terms like "immediately," "failure to do so," and "permanent suspension" are designed to scare the user.

5. **Grammar and Tone**:
   - The language is formal but lacks typical PayPal branding and personalization.

6. **Lack of Personalization**:

   - Addressed to "Dear Customer" instead of using the recipient's actual name.

7. **Social Engineering Tactics**:

   - The attacker creates fear (account suspension) to trick the user into clicking the malicious link.

Conclusion:

This phishing email is well-crafted to mimic a real PayPal alert but contains clear indicators of fraud such as spoofed sender, failed authentication, fake links, and scare tactics. Users should avoid interacting with such emails and report them to IT/security teams immediately.