Incident Report: Simulated Phishing Attempt

---

1. Incident Title: Simulated Phishing Attempt - Analysis & Report

2. Date of Report: June 3, 2025

3. Analyst Name: [Your Name/Analyst ID]

4. Incident Type: Phishing / Social Engineering Attempt

5. Affected User/System: Test User Account (James) / Personal Email Account

---

Incident Summary:

On June 3, 2025, a simulated phishing email, designed to mimic an urgent account verification request from PayPal, was delivered to a test user account (James). The email leveraged strong social engineering tactics, including a high sense of urgency and threats of account suspension and fund forfeiture, to coerce the user into immediate action. While the email's content appeared grammatically sound, analysis revealed a deceptive hyperlink designed to mislead the recipient. The user, experiencing legitimate concern over their funds, proceeded to click the link, which unexpectedly redirected them to their Internet Service Provider's (ISP) default error page, confirming the illegitimate nature of the link.

Incident Details & Analysis:

A. Observed Indicators of Compromise (IoCs):

- **Sender Display Name:** PayPal Security Center (or similar)
- **Actual Sender Email Address:** example@gmail.com (Discrepancy with legitimate PayPal sender domains)
- **Email Subject:** "Urgent: Your PayPal Account Has Been Temporarily Limited - Action Required Immediately"
- **Malicious Hyperlink:** http://verify-paypal-login-now.com/ (The actual URL did not match the perceived legitimate text. This domain is non-existent.)
- **Social Engineering Tactics:**
  - **Urgency:** Explicit deadline ("within 5 hours") and severe consequences ("permanent account closure," "forfeiture of pending transactions").
  - **Fear/Threat:** Warnings of "unauthorized access" and "account suspension."
  - **False Authority:** Inclusion of "PayPal Security Department" and a "Reference ID."

- **Absence of Personalization:** The email used a generic salutation ("Dear PayPal Member") instead of the user's specific name.

B. Analysis Findings:

1. **Deceptive Sender & Subject:** The combination of a seemingly official display name and an urgent subject line (Urgent: Your PayPal Account Has Been Temporarily Limited - Action Required Immediately) is a classic phishing technique to bypass initial scrutiny and prompt immediate action.
2. **Hyperlink Discrepancy:** The most critical finding was the **mismatch between the perceived legitimate hyperlink text and the actual URL**. The actual URL (http://verify-paypal-login-now.com/) is a non-existent domain, confirming its malicious intent despite the convincing email body.
3. **Redirection to ISP Page:** The redirection to the ISP's default error page upon clicking the link further validated that the URL was illegitimate and not connected to PayPal. This outcome is consistent with attempting to access a non-existent domain.
4. **Psychological Manipulation:** The attacker effectively exploited psychological triggers like urgency and fear of loss (funds, account access) to bypass the user's critical thinking, leading to a hurried click.
5. **User's Proactive Response:** Post-click, the user (James) demonstrated good security hygiene by:
   - Independently navigating to the official PayPal website.
   - Verifying no unauthorized fund withdrawals occurred.
   - Updating their account password.
   - Enabling Multi-Factor Authentication (MFA).

Simulated Containment & Mitigation Steps:

Based on a real-world scenario, the following actions would be advised/taken by a SOC analyst:

1. **Immediate User Education:** Reinforce phishing awareness with the affected user, emphasizing vigilance and the dangers of clicking suspicious links.
2. **Email Deletion:** Advise the user to delete the phishing email to prevent future accidental clicks.
3. **Threat Intelligence Update:** Add the identified malicious URL (http://verify-paypal-login-now.com/) to internal threat intelligence feeds for blocking at network and endpoint levels.
4. **Gateway/Endpoint Blocking:** Implement rules on email gateways and network firewalls to block emails from the observed sender domain and prevent access to the malicious URL.
5. **Proactive Password Reset (if applicable):** If credentials were potentially compromised (even in simulation), advise a password reset on the legitimate service.

6. **MFA Enforcement:** Strongly recommend and assist users in enabling Multi-Factor Authentication (MFA) on all critical accounts.

Lessons Learned:

This simulation highlighted several key takeaways for improving cybersecurity posture and incident response:

1. **The Human Factor Remains Critical:** Even with increasing email security measures, sophisticated social engineering can still trick users into compromising actions. Continuous user education is paramount.
2. **Always Verify, Never Trust:** Users should be trained to independently verify suspicious requests by directly navigating to official websites or using trusted contact information, rather than clicking embedded links.
3. **Email Header Analysis is Key:** Understanding email headers is crucial for discerning legitimate emails from phishing attempts, particularly for analyzing From:, Received:, and Authentication-Results headers.
4. **Importance of Layered Security:** The user's post-incident actions (going to the official site, password change, MFA setup) demonstrate the effectiveness of layered security controls and proactive user behavior in mitigating potential damage.