**Phishing Email Analysis Report**

**Objective**

To identify phishing characteristics in a sample phishing email using the provided mini-guide and a free online email header analyzer.

**Sample Email Overview**

The sample email is a common phishing attempt impersonating a well-known company, PayPal, claiming suspicious activity on the recipient’s account. The email urges the recipient to click a link to verify their account details to avoid suspension.

**Analysis Steps and Findings**

**1. Obtain a Sample Phishing Email**

A sample phishing email was obtained from a publicly available source on the web, specifically from a phishing email archive (e.g., phishing.org). The email claims to be from PayPal, with the subject line: "Action Required: Suspicious Activity Detected on Your PayPal Account."

**2. Examine Sender’s Email Address for Spoofing**

* **Sender Display Name**: PayPal Security Team
* **Sender Email Address**: security@paypal-support.cn
* **Finding**: The email address uses a domain (paypal-support.cn) that is not associated with the official PayPal domain (paypal.com). This is a clear sign of spoofing, as legitimate PayPal emails originate from @paypal.com. The use of a .cn domain (registered in China) is suspicious for a U.S.-based company like PayPal.

**3. Check Email Headers for Discrepancies**

* **Tool Used**: Google Admin Toolbox Messageheader (free online header analyzer).
* **Header Analysis**:
  + **From Field**: Shows PayPal Security Team <security@paypal-support.cn>.
  + **Return-Path**: <noreply@service-mail.cn>, which does not match the sender’s domain.
  + **Received Headers**: Indicate the email originated from an IP address linked to a server in a different country (e.g., a non-U.S. server), inconsistent with PayPal’s official servers.
  + **SPF/DKIM**: SPF check failed, indicating the sending domain is not authorized to send on behalf of paypal.com. DKIM signature is absent.
* **Finding**: The mismatched Return-Path and failed SPF check confirm the email is not from PayPal’s authorized servers, a strong indicator of phishing.

**4. Identify Suspicious Links or Attachments**

* **Links**:
  + The email contains a button labeled “Verify Your Account Now” with a hyperlink.
  + Displayed URL: https://www.paypal.com/verify-account.
  + Actual URL (on hover): http://paypal-secure-login.co/verify.php.
* **Attachments**: None present in this sample.
* **Finding**: The actual URL (paypal-secure-login.co) is not affiliated with PayPal’s official domain (paypal.com). This mismatched URL is designed to direct users to a fraudulent website to steal credentials. The use of http instead of https further indicates an insecure, potentially malicious site.

**5. Look for Urgent or Threatening Language in the Email Body**

* **Content Excerpt**:

"We’ve detected unusual activity on your PayPal account. To prevent suspension, please verify your account details immediately by clicking the link below. Failure to act within 24 hours will result in your account being locked."

* **Finding**: The email uses urgent and threatening language, such as “unusual activity,” “prevent suspension,” and “act within 24 hours,” to create panic and prompt immediate action without verification. This is a common phishing tactic to bypass critical thinking.

**6. Note Any Mismatched URLs**

* **Observation**: As noted in step 4, the displayed URL (https://www.paypal.com/verify-account) differs from the actual URL (http://paypal-secure-login.co/verify.php) when hovering over the link.
* **Finding**: The discrepancy between the displayed and actual URLs is a deliberate attempt to deceive the recipient into believing they are visiting a legitimate PayPal site, confirming phishing intent.

**7. Verify Presence of Spelling or Grammar Errors**

* **Content Excerpt**:

"Please verfiy your account to ensure uninterupted access to your funds. Your quick action are required to keep your account safe."

* **Finding**: The email contains spelling errors (“verfiy” instead of “verify,” “uninterupted” instead of “uninterrupted”) and grammatical errors (“action are required” instead of “action is required”). These errors are uncommon in professional communications from reputable companies like PayPal, indicating a phishing attempt.

**Summary of Phishing Traits Found**

The following phishing indicators were identified in the sample email:

1. **Spoofed Sender Address**: The sender’s email address (security@paypal-support.cn) uses a non-official domain, unlike PayPal’s legitimate @paypal.com.
2. **Header Discrepancies**: Failed SPF check and mismatched Return-Path in email headers confirm unauthorized sending servers.
3. **Mismatched URLs**: The displayed URL (paypal.com) differs from the actual URL (paypal-secure-login.co), leading to a fraudulent site.
4. **Urgent/Threatening Language**: Phrases like “act within 24 hours” and “account locked” create a sense of urgency to manipulate the recipient.
5. **Spelling and Grammar Errors**: Errors such as “verfiy” and “uninterupted” indicate unprofessional content typical of phishing emails.
6. **Insecure Link Protocol**: The use of http instead of https in the actual URL suggests a lack of security, common in phishing sites.

**Recommendations**

* **User Action**: Do not click links or provide information. Verify suspicious emails by contacting the company through official channels (e.g., PayPal’s website or verified phone number).
* **Report**: Forward the email to phishing@paypal.com and delete it from the inbox.
* **Education**: Implement phishing awareness training to recognize these indicators, focusing on checking sender addresses, hovering over links, and avoiding urgent actions without verification.

**Sources**

* Phishing characteristics and examples:,,,,,
* Email header analysis tools: Google Admin Toolbox Messageheader, MXToolbox