Phishing Analysis Report

Introduction

This report analyzes a phishing email sample mimicking a PayPal account verification request, as part of Task 2 of the Eleyate Cybersecurity Internship. The objective is to identify phishing characteristics using the provided mini-guide. The sample, sourced as a fictional educational example based on templates from CanIPhish, was analyzed for sender spoofing, email header discrepancies, suspicious links, urgent language, mismatched URLs, and spelling/grammar errors. The findings confirm the email as a phishing attempt designed to steal user credentials.

Phishing Email Sample

- **Subject**: Urgent: Verify Your PayPal Account Now!
- **From**: PayPal Support support@paypa1.com
- **To**: user@example.com
- **Body**:
- Dear Costumer,
-
- We have detected unusual activity on your PayPal acccount. To protect your funds, you must verify your identity immediately. Failure to do so will result in your account being locked within 24 hours.
-
- Please click the link below to verify your account:
-
- [Verify Now](http://paypa1-login.co/secure-login)
-
- If you did not initiate this request, plese contact our support team at support@paypa1.com.
-
- Thank you,
  PayPal Security Team

- **Source**: Fictional sample created for educational purposes, inspired by CanIPhish templates.
- **Storage**: Saved as phishing_email_sample.txt in the GitHub repository.

Analysis Methodology

The analysis followed the task's hints using free tools:

- **Email Client**: Simulated using a text editor to view the sample safely.
- **Header Analyzer**: Google Admin Toolbox MessageHeader (https://toolbox.googleapps.com/apps/messageheader/).
- **URL Scanner**: VirusTotal (https://www.virustotal.com) for link analysis.
- **Text Review**: Manual inspection of the email body for language and errors.

Phishing Indicators

1. Sender’s Email Address (Spoofing)

- **Observation**: The sender’s address is support@paypa1.com.
- **Analysis**: The domain paypa1.com contains a deliberate misspelling of the official PayPal domain (paypal.com). The display name “PayPal Support” attempts to deceive the recipient into trusting the email.
- **Finding**: The mismatched domain indicates email spoofing, a common phishing tactic to impersonate a legitimate entity.

2. Email Header Discrepancies

- **Headers** (Simplified):
- `Received: from unknown [192.0.2.6] by smtp.paypa1.com`
- `From: PayPal Support <support@paypa1.com>`
- `To: user@example.com`
- `Subject: Urgent: Verify Your PayPal Account Now!`
- `Message-ID: <abc123@paypa1.com>`
- `SPF: FAIL`
`DKIM: NONE`

- **Tool**: Google Admin Toolbox MessageHeader.
- **Analysis**:
  - The Received header shows the email originated from an unknown server (IP: 192.0.2.6), not associated with PayPal’s official mail servers.
  - The SPF record is marked as FAIL, indicating the sender’s domain is not authorized to send emails on behalf of PayPal.
  - No DKIM signature is present, suggesting a lack of authentication.
- **Finding**: The SPF failure and missing DKIM signature confirm the email is forged. See header_analysis_screenshot.png for the analysis output.

3. Suspicious Links

- **Link**: Displayed as “Verify Now”.
- **Tool**: VirusTotal.
- **Analysis**:
  - The URL http://paypa1-login.co/secure-login uses a domain unrelated to PayPal (paypal.com).
  - The use of HTTP instead of HTTPS for a supposed login page is suspicious, as legitimate financial sites use secure connections.
  - For this fictional sample, VirusTotal is assumed to flag the URL as malicious based on its deceptive domain.
- **Finding**: The link is a phishing attempt to redirect users to a fraudulent site for credential theft. See virustotal_results.png for simulated results.

4. Urgent or Threatening Language

- **Examples**:
  - “You must verify your identity immediately.”
  - “Failure to do so will result in your account being locked within 24 hours.”
- **Analysis**: The email employs urgent language to create panic and pressure the recipient into clicking the link without verifying its legitimacy. This is a social engineering tactic commonly used in phishing attacks.
- **Finding**: The threatening tone is a clear indicator of phishing intent.

5. Mismatched URLs

- **Observation**:
  - Displayed link text: Implies a legitimate PayPal login page (e.g., www.paypal.com).
  - Actual URL: http://paypa1-login.co/secure-login.
- **Analysis**: The discrepancy between the displayed text and the actual destination URL is designed to deceive users into trusting the link.
- **Finding**: The mismatched URL reinforces the phishing nature of the email.

6. Spelling and Grammar Errors

- **Examples**:
  - “Costumer” instead of “Customer”.
  - “Acccount” instead of “Account”.
  - “Plese” instead of “Please”.
- **Analysis**: These errors indicate a lack of professionalism, uncommon in official communications from reputable companies like PayPal.
- **Finding**: The presence of multiple spelling and grammar errors is a strong phishing indicator.

Conclusion

The analyzed email exhibits multiple phishing characteristics:

- A spoofed sender address (support@paypa1.com) with a misspelled domain.
- Email headers showing SPF failure and no DKIM signature, indicating forgery.
- A suspicious link (http://paypa1-login.co) flagged as malicious.
- Urgent language to manipulate the recipient.
- Mismatched URLs to deceive users.
- Spelling and grammar errors suggesting unprofessional content.

These findings confirm the email as a phishing attempt aimed at stealing user credentials. The analysis enhances awareness of phishing tactics and demonstrates email threat detection skills.

Supporting Evidence

- **phishing_email_sample.txt**: Text file containing the full email sample.
- **header_analysis_screenshot.png**: Screenshot of Google Admin Toolbox header analysis.
- **virustotal_results.png**: Simulated VirusTotal results for the suspicious URL.

Recommendations

- **User Actions**: Do not click links or respond to such emails. Report to the email provider (e.g., Gmail) and delete the email.
- **Organizational Measures**: Implement SPF, DKIM, and DMARC to prevent spoofing, and conduct user training on phishing awareness.

Tools Used

- **Google Admin Toolbox MessageHeader**: For header analysis.
- **VirusTotal**: For URL scanning (simulated for this fictional sample).
- **Text Editor (VS Code)**: To review the email sample and draft the report.