**Phishing Email Analysis Report**

1. **Email Overview**

The subject of the email is "Urgent Action Required – Account Suspended." It was sent from an email address posing as PayPal Support with the address [support@paypall-service.com](mailto:support@paypall-service.com) and sent to [user@example.com](mailto:user@example.com). The exact date of receipt is not specified and should be entered. The email includes an attachment named "restore\_account\_form.zip."

1. **Header Analysis**

The email header was analyzed using MxToolbox. The analysis showed that the email failed SPF, DKIM, and DMARC checks, which are key email authentication methods. These failures strongly suggest that the email was spoofed. Additionally, the source IP address 198.51.100.12 does not match any legitimate PayPal mail servers. This raises concerns about a potentially forged origin.

1. **Sender Domain Analysis**

The claimed sender email address is [support@paypall-service.com](mailto:support@paypall-service.com). However, the legitimate domain for PayPal is paypal.com. The suspicious domain includes a misspelling with an extra “l” and the addition of “-service,” which is a common tactic used to impersonate trusted companies. This indicates that the sender is attempting to mimic PayPal in order to deceive the recipient.

1. **Link Analysis**

The email contains a hyperlink that appears to be a PayPal login page: <https://www.paypal.com.account-verify-login.securepage.co/restore>. While the link includes “paypal.com,” the actual domain is securepage.co, which is not associated with PayPal. This is a deceptive tactic designed to trick users into believing the link is legitimate. The URL was submitted to VirusTotal for analysis and was flagged as malicious or phishing by multiple antivirus engines.

1. **Attachment Analysis**

The attached file is named restore\_account\_form.zip. When scanned using a simulated VirusTotal file upload, it was identified as potentially harmful. Zip files are commonly used by attackers to conceal malware such as trojans and credential stealers. Receiving such an unsolicited file, especially in a suspicious email, poses a serious security risk.

1. **Language and Tone Analysis**

The email uses a tone designed to create urgency and fear. Phrases such as “Your account will be permanently closed” and “Limited your account access” are examples of threat-based messaging. This is a common social engineering technique meant to pressure recipients into taking immediate action without thinking. Although the email does not contain significant grammatical errors, the formal and urgent tone further contributes to its suspicious nature.

1. **Phishing Indicators Summary**

Multiple red flags were identified in the analysis. The sender’s domain is misspelled, indicating a spoofed identity. The link in the email uses a fake domain designed to appear as if it belongs to PayPal. The tone of the email is urgent and threatening, which is a typical tactic in phishing attempts. The attachment is a zip file that was not expected and could contain malware. Additionally, all email authentication methods (SPF, DKIM, and DMARC) failed, which strongly indicates spoofing.

1. **Conclusion**

This email is clearly a phishing attempt aimed at deceiving the recipient into clicking a malicious link and downloading a harmful file under the pretense of account verification. All the main indicators of phishing are present, including sender spoofing, a suspicious and misleading URL, urgency in the message, a dangerous attachment, and failed authentication checks.

1. **Recommendations**

Recipients should not click on any links or open attachments included in the email. The email should be reported immediately to the appropriate IT or security team. Users should be educated on how to identify domain impersonation, psychological pressure tactics, and common signs of phishing. Additionally, organizations should implement email filtering tools that can detect spoofing and prevent such messages from reaching users' inboxes.