PHISHING EMAIL ANALYSIS REPORT

# Objective

To Evaluate the authenticity of a suspicious email using technical header analysis, behavioral cues, and forensic tools.

# Sample Email Overview

Sender: service@paypal-alert.com  
Subject: "PayPal Security Notice: Unusual Activity Detected"  
Source: Publicly available phishing example from awareness blogs - Google

# Phishing Indicators Identified

* - Spoofed domain
* - Failed SPF/DKIM/DMARC
* - Mismatched links
* - Urgent and coercive language
* - Grammar and branding inconsistencies

# Methodologies and Code Used for Email Threat Analysis

## Header Extraction and Parsing

Tool Used: MXToolbox Email Header Analyzer

## SPF, DKIM, DMARC Validation

Linux Commands:

dig +short TXT paypal-alert.com  
dig +short TXT \_dmarc.paypal-alert.com  
dig +short TXT default.\_domainkey.paypal-alert.com

## URL Analysis

curl Command:

curl -I <http://paypal-verify.net/login>

## Logo & Visual Content Authentication

SSL Certificate Check:

openssl s\_client -connect paypal-verify.net:443

## DNS Intelligence & WHOIS Lookup

Commands:

whois paypal-alert.com  
dig paypal-alert.com ANY

## Behavior Classification

MITRE Technique | Description   
  
 T1586.002 Domain Spoofing / Typosquatting   
 T1566.002 Spearphishing via Link   
 T1059.003 Execution of scripts ( via malicious attachment)   
 T1598 Phishing for information

# Automation Possibility

Most of the steps outlined above can be automated via Bash, or SIEM tools. For small teams, free tools like MXToolbox, VirusTotal, LanguageTool, and cURL offer practical means of phishing analysis.

# Conclusion

This report follows a forensic, reproducible methodology combining:  
 Manual header and content analysis  
 DNS/email authentication evaluation  
 Link and payload inspection  
 Language and branding inconsistencies  
  
By applying layered analysis, phishing indicators are confirmed beyond reasonable doubt.