

Phishing Email Analysis Report

Report Title: Phishing Email Sample Analysis

Analyst: [Parijat Das]

Date: [24/08/2025]

1. Executive Summary

This report analyzes a suspicious email sample to identify potential phishing characteristics. The objective was to examine email headers, content, and attachments/links to highlight indicators of compromise (IoCs) and assess the threat level.

Outcome: The analysis found multiple phishing indicators including spoofed sender address, suspicious links, and urgent/pressure-based language.

2. Email Details

Attribute	Value (from sample)
-----------	---------------------

Sender Address support@paypal-login[.]com

Recipient victim@example.com

Subject "Urgent: Verify Your Account Now!"

Date/Time 2025-08-24 10:15 UTC

Attachments invoice.pdf (potential malicious)

Links hxxp://secure-paypal[.]com/login

3. Phishing Indicators

Category	Observations
----------	--------------

Sender Address Domain spoofing: "paypal" misspelled.

Headers Return-path mismatch: sender domain ≠ return domain.

Links Hovered link redirects to fake domain, not PayPal official domain.

Attachments Suspicious PDF invoice included (possible malware dropper).

Language Urgent/Threatening: "Verify account immediately to avoid suspension."

Errors Multiple spelling errors ("paypal", "secur account").

4. Risk Assessment

Indicator	Risk Level
Spoofed sender address	● High
Suspicious link redirection	● High
Malicious attachment	● High
Urgency/Threatening tone	● Medium
Grammar/Spelling mistakes	● Low

Overall Risk Rating: High

5. Recommended Actions

- 1. Do not click links or download attachments.**
- 2. Report the email to security@yourorg.com.**
- 3. Block sender domain paypal-login[.]com.**
- 4. Educate the recipient on phishing awareness.**
- 5. Upload email to SIEM for correlation with other alerts.**

Interview Questions with Answers

1. What is phishing?

Phishing is a type of social engineering attack where attackers impersonate trusted entities (like banks or companies) to trick users into revealing sensitive information such as passwords, credit card numbers, or downloading malware.

2. How can you identify a phishing email?

By checking for red flags such as:

- Spoofed or misspelled sender addresses.
 - Urgent or threatening language (“verify immediately”).
 - Suspicious links or attachments.
 - Poor grammar/spelling.
 - Mismatched URLs (hover reveals fake domains).
-

3. What is email spoofing?

Email spoofing is forging the “From” address in emails to make them appear as if they came from a trusted domain or contact, tricking the recipient into trusting the message.

4. Why are phishing emails dangerous?

Because they can:

- Steal credentials and financial info.
 - Deliver malware or ransomware via attachments/links.
 - Enable further attacks like Business Email Compromise (BEC).
-

5. How can you verify the sender's authenticity?

- Check the full email header for “Return-Path” and SPF/DKIM/DMARC validation.
 - Hover over links to see the actual domain.
 - Cross-verify with official company contacts.
 - Use online header analysis tools.
-

6. What tools can analyze email headers?

- Online tools (e.g., MXToolbox, Google Admin Toolbox).
- Built-in email client “view headers” option.

- SIEM or SOAR platforms in enterprise environments.
-

7. What actions should be taken on suspected phishing emails?

- Do not click links/download attachments.
 - Report to security team/IT.
 - Block sender's domain.
 - Educate affected user(s).
 - Upload sample to sandbox or SIEM for further analysis.
-

8. How do attackers use social engineering in phishing?

They exploit human psychology such as:

- **Fear** ("Your account will be suspended").
- **Curiosity** ("You've received a bonus/invoice").
- **Trust** (impersonating a boss or company).
- **Urgency** (forcing quick action without thinking).

Flashcards – Phishing Interview Questions

Flashcard 1

Q: What is phishing?

A: A social engineering attack where attackers impersonate trusted entities to steal credentials, financial info, or deliver malware.

Flashcard 2

Q: How can you identify a phishing email?

A: Look for spoofed addresses, urgent/threatening language, suspicious links/attachments, poor grammar, mismatched URLs.

Flashcard 3

Q: What is email spoofing?

A: Forging the "From" address to make an email appear to come from a trusted source.

Flashcard 4

Q: Why are phishing emails dangerous?

A: They can steal credentials, financial info, deliver malware/ransomware, or enable further attacks like Business Email Compromise.

Flashcard 5

Q: How can you verify the sender's authenticity?

A: Check email headers, SPF/DKIM/DMARC validation, hover links, cross-check with official contacts, use header analyzers.

Flashcard 6

Q: What tools can analyze email headers?

A: MXToolbox, Google Admin Toolbox, email client "view headers" option, SIEM/SOAR tools.

Flashcard 7

Q: What actions should be taken on suspected phishing emails?

A: Don't click links, don't open attachments, report to IT/security, block sender, upload to sandbox or SIEM.

Flashcard 8

Q: How do attackers use social engineering in phishing?

A: Exploiting **fear, curiosity, trust, and urgency** to manipulate victims into taking harmful actions.