

## Task 2<sup>nd</sup>: Phishing Email Analysis Report

### What is Phishing Email Analysis?

#### What Is a Phishing Email?

A phishing email is a fraudulent message that tries to:

- Trick users into clicking a malicious link or attachment
- Steal sensitive information (like passwords or banking details)
- Install malware (e.g., ransomware, remote access tools)
- Impersonate trusted entities (like banks, companies, or colleagues)

---

#### What Happens in Phishing Email Analysis?

Step	Description
1. Header Analysis	Check sender's email, reply-to address, received paths, IPs — to see if it's spoofed.
2. Body Content Inspection	Look for urgent language, suspicious links, fake branding, grammar errors.
3. URL Analysis	Hover or extract links, analyze with tools like VirusTotal or by decoding URL shorteners.
4. Attachment Analysis	Scan for embedded malware or scripts (.zip, .docm, .xlsm, etc). Sandbox if needed.
5. Technical Indicators (IOCs)	Extract domains, IPs, hashes, and track them for threat intel or correlation.
6. Behavioral Analysis	If opened in a sandbox, observe what the attachment or link does.
7. Threat Attribution	Try to determine if it's part of a known campaign or threat actor activity.

## Task 2<sup>nd</sup>: Phishing Email Analysis Report

### Analyzed Email Sample

**Subject:** Account Verification Required – Suspicious Login Attempt

**From:** [support@secure-paypals.com](mailto:support@secure-paypals.com)

**To:** [victim@example.com](mailto:victim@example.com)

**Reply-To:** [support@paypals-verify.com](mailto:support@paypals-verify.com)

**Date:** Tue, 14 May 2024 10:22:05 +0000

**Attachments:** Account\_Lock\_Details.zip

**Body Text:**

*Dear Valued Customer,*

*We have detected suspicious login attempts on your PayPal account from an unrecognized device in Russia (IP: 85.143.27.99).*

*For your security, we have temporarily restricted access to your account until the verification process is complete.*

*Please verify your account activity immediately by clicking the button below. This is necessary to protect your information and restore full access.*

*Failure to complete the verification process within 24 hours may result in permanent suspension of your PayPal account.*

[verify now](#)

*You can also find the verification instructions in the attached document.*

*Thank you for helping us keep your account secure.*

*– PayPal Security Team*

<https://www.paypal.com>

## Task 2<sup>nd</sup>: Phishing Email Analysis Report

### 1. Obtain a sample phishing email

Sample Email Subject:

*"[Action Required] Your PayPal Account Has Been Limited"*

From:

[support@secure-paypals.com](mailto:support@secure-paypals.com)

Body Excerpt:

"We've noticed suspicious activity on your account. You must verify your identity within 24 hours to prevent permanent suspension."

Link:

[Verify Account](#)

Attachment:

Verify\_Account\_Info.zip

---

### 2. Examine sender's email address for spoofing

From Address:

support@secure-paypals.com — Spoofed domain, mimicking PayPal, but using a fake domain (secure-paypals.com instead of paypal.com).

SPF/DKIM/DMARC check via [MXToolbox](#):

- SPF: FAIL
- DKIM: FAIL
- DMARC: NOT CONFIGURED

This confirms spoofing behavior.

---

### 3. Check email headers for discrepancies (using online header analyzer)

Header Fields Noticed:

- Return-Path: bounce@paypals-verify-mail.net
- Reply-To: support@paypals-verify.com
- Received From: IP 154.12.65.78 (blacklisted on AbuseIPDB)

Discrepancies:

- From, Return-Path, and Reply-To all use different domains
- IP address used not registered to PayPal — originates from an untrusted hosting provider

Used [Google Header Analyzer](#) to extract these insights.

---

## Task 2<sup>nd</sup>: Phishing Email Analysis Report

---

### 4. Identify suspicious links or attachments

- **Hyperlink text:** "Verify your account"  
**Actual URL (on hover):** <http://secure-paypal-confirm-portal.info>  
*Mismatched domain; not related to paypal.com*
  - **Attachment:** Verify\_Account\_Info.zip  
*ZIP files often used to deliver malware. Scanned via VirusTotal and flagged as containing a trojan dropper.*
- 

### 5. Look for urgent or threatening language in the email body

Email Body:

"We've noticed suspicious activity on your account. Please confirm your details now. Failure to respond within 24 hours will result in account suspension."

*The tone creates urgency and fear — classic social engineering tactic to pressure users into immediate action.*

---

### 6. Note any mismatched URLs (hover to see real link)

Visible Text: "Click here to verify your account"

Actual Link (on hover): <http://secure-paypal-confirm-portal.info>

*Appears legitimate at a glance but redirects to a phishing site using a fraudulent domain.*

---

### 7. Verify presence of spelling or grammar errors

Examples Found:

- "Please confirm you details now" → "your"
- "Your account has been limited" → "limited"

*Minor grammar mistakes are typical in phishing emails, especially from non-native attackers or autogenerated scripts.*

---

### 8. Summarize phishing traits found in the email

Phishing Trait	Evidence
Spooled Email Address	support@secure-paypals.com
Header Discrepancies	Different From, Reply-To, and Return-Path
Suspicious Link	<a href="http://secure-paypal-confirm-portal.info">http://secure-paypal-confirm-portal.info</a> (not PayPal)

## Task 2<sup>nd</sup>: Phishing Email Analysis Report

<b>Urgent Tone</b>	<b>Threat of account suspension in 24 hours</b>
<b>Grammar Errors</b>	<b>“you details”, “limitation”</b>
<b>Malicious Attachment</b>	<b>.zip file flagged on VirusTotal</b>
<b>Blacklisted IP</b>	<b>Email sent from flagged address on AbuseIPDB</b>
<b>Failing Authentication</b>	<b>SPF and DKIM failed, DMARC not set</b>

## Task 2<sup>nd</sup>: Phishing Email Analysis Report

### Deep Scans of Phishing email

#### Header Analysis Summary

Field	Value	Analysis
From	<a href="mailto:support@secure-paypals.com">support@secure-paypals.com</a>	Spoofed domain (not official PayPal)
Reply-To	<a href="mailto:support@paypals-verify.com">support@paypals-verify.com</a>	Different from "From" field – highly suspicious
Return-Path	<a href="mailto:bounce@secure-mail-pay.info">bounce@secure-mail-pay.info</a>	Domain mismatch with "From"
Received From IP	154.12.65.78	Blacklisted (checked on AbuseIPDB)
Message-ID	<a href="mailto:abc98765432@mail.paypals-verify.com">abc98765432@mail.paypals-verify.com</a>	Generated via spoofed server
SPF/DKIM/DMARC	SPF: Fail, DKIM: Fail, DMARC: Absent	Classic spoof signature
Subject	"Account Verification Required – Suspicious Login Attempt"	Uses urgency/fear – social engineering

#### Red Flags Identified

Indicator	Evidence
Spoofed Email Address	<a href="mailto:support@secure-paypals.com">support@secure-paypals.com</a> (fake domain)
Different Reply-To Address	Diverts user response to an attacker-controlled email
Suspicious Links	Hovering reveals: <a href="http://secure-paypals-security-check.info">http://secure-paypals-security-check.info</a> (not PayPal)
Urgency & Threat	"Verify within 24 hours" creates pressure
Suspicious Attachment	Account_Lock_Details.zip – potential malware
Grammar Errors	"We have noticed unauthorized login attempts..." poorly formatted
Domain Reputation	Domain registered 2 days ago, not associated with PayPal
Header Discrepancy	SPF/DKIM fail – classic indicators of spoofing
Blacklisted IP	Origin IP found in AbuseIPDB for spam/phishing reports

## Task 2<sup>nd</sup>: Phishing Email Analysis Report

### Static & Dynamic Analysis of URL and Attachment

#### Static Analysis:

- Link Domain: Newly registered (2 days ago)
- Virus Total: Flagged as phishing by 8 AV engines
- Attachment (.zip): Detected as a dropper trojan by Avast and Kaspersky

#### Dynamic Analysis (in sandbox):

- URL redirects to a cloned PayPal login page hosted on a VPS.
  - Clicking *Login* sends entered credentials to a PHP script on attacker-collect.php.
- 

#### Email Header Tools Used

- MX Toolbox: Verified fake mail server
  - Email Header Analyzer (Google): Showed failing SPF/DKIM
  - VirusTotal: Checked URL and ZIP file
  - AbuseIPDB: Identified malicious IP with >100 complaints
- 

#### Defensive Recommendations

- Enable SPF, DKIM, DMARC on all email domains
- Deploy anti-phishing email filters
- Use sandbox for suspicious attachments
- Conduct employee phishing awareness training
- Implement multi-factor authentication (MFA)