# Phishing Email Analysis Report

## Screenshot

A screenshot of a paypal

Description automatically generated

**1. Obtain a Sample Phishing Email**

The provided image 1 serves as the sample phishing email for this analysis.

**2. Examine the Sender's Email Address**

* The sender's email address is "[services@paypal-accounts.com](mailto:services@paypal-accounts.com)" 1.
* While it contains "paypal" in the domain, the full domain "paypal-accounts.com" is suspicious and not the official "paypal.com" domain 1. This is a common tactic to trick users into believing it's legitimate.

**3. Check Email Headers for Discrepancies**

* Although the full headers are not visible in the image, in a real scenario, one would use a header analyzer.
* Discrepancies would likely include the actual sending server not matching PayPal's infrastructure, or the "Return-Path" being from an unrelated domain.

**4. Identify Suspicious Links or Attachments**

* The email contains a button labeled "Confirm Your Information" 1.
* The exact URL behind this button is not visible in the image, but in a real phishing attempt, hovering over it would reveal a non-PayPal URL (e.g., one with a typo, an extra subdomain, or a completely different domain) 1. There are no attachments visible in this sample 1.

**5. Look for Urgent or Threatening Language**

* The subject line states: "Your account access has been limited" 1.
* The body of the email contains urgent and threatening language: "Your PayPal account is limited, You have 24 hours to solve the problem or your account will be permanetly disabled" 1.
* It also states, "We are sorry to inform you that you no longer have access to PayPal's advantages like purchasing, and sending and receiving money" 1. This is designed to create a sense of urgency and fear to prompt immediate action.

**6. Note Any Mismatched URLs**

* While the specific URL is not shown, the email prompts the user to "confirm all of your account details on our secured server by clicking the link below" 1.
* The generic "Confirm Your Information" button 1 hides the actual malicious URL. This is a classic mismatched URL tactic, where the displayed text is innocuous but the underlying link is fraudulent.

**7. Verify Presence of Spelling or Grammar Errors**

* There is a clear spelling error: "permanetly" instead of "permanently" 1. This is a strong indicator of a phishing attempt, as legitimate companies typically have high standards for written communication.

**8. Summarize Phishing Traits Found**

**Phishing Indicators Identified:**

* **Suspicious Sender Domain:** "[services@paypal-accounts.com](mailto:services@paypal-accounts.com)" is not the official PayPal domain 1.
* **Urgent and Threatening Language:** Phrases like "account access has been limited," "24 hours to solve the problem or your account will be permanetly disabled," and loss of "PayPal's advantages" 1.
* **Spelling Error:** "permanetly" instead of "permanently" 1.
* **Call to Action for Sensitive Information:** Asks the user to "confirm all of your account details" via a link 1.
* **Hidden Malicious Link:** The "Confirm Your Information" button likely conceals a fraudulent URL (not directly visible but implied by the context of phishing) 1.