**Phishing Email Analysis Report**

**Name:** Asna Mirza  
**Task:** Cyber Security — Analyze a Phishing Email Sample.  
**Date:** October 21, 2025

**Objective :** dentify and analyze phishing characteristics in a suspicious email sample.

**Introduction: What is Phishing?**

Phishing is a cyberattack where attackers use fake emails to trick users into revealing personal information, downloading malware, or clicking malicious links. Phishing emails imitate trusted organizations but contain tricks to steal data or infect systems.

**Sample Phishing Email:**

|  |
| --- |
| **Subject**: Urgent: Account Suspension Notice  **From: "PayPal Security Team"**[**support@paypa1.com**](mailto:support@paypa1.com)  **Body:**  Dear Customer, We noticed unusual activity in your PayPal account. For your protection, your account will be suspended within 24 hours unless you confirm your information. Please click the link below to verify your account and restore access: [**Verify Your Account**](http://malicious-link.com/)If you do not verify within 24 hours, your account will bepermanently disabled. Thank you, **PayPal Security Team** |

**Detailed Analysis of Phishing Indicators:**

1. **Sender’s Email Address Spoofing :**

The sender uses “[support@paypa1.com](mailto:support@paypa1.com)” (note the ‘1’ instead of ‘l’), a classic spoof to trick victims into thinking it’s real PayPal.

1. **Email Header Checking:**

A real analysis should include checking headers with an online tool (such as MXToolbox). This helps spot mismatched “Return-Path”, suspicious IP addresses, or non-corporate sending domains. (For online samples, state: “Email header analysis would be performed if headers were available.”)

1. **Suspicious Links:**

The ‘Verify Your Account’ link points to “malicious-link.com” and not paypal.com. Hovering over links can reveal this trick.

1. **Urgent/Threatening Language:**

Phrases like “suspended within 24 hours” and threats of permanent disabling create panic and force fast action.

1. **Attachments:**

Some phishing emails contain dangerous attachments. This sample does not, but never open .exe, .zip, or random documents from unknown senders.

1. **Mismatched URLs:**

The visible link text appears official, but the real link (on hover) is different and malicious.

1. **Spelling & Grammar Errors:**

Look for mistakes or awkward sentences. This email is mostly correct, but the language is generic and impersonal.

1. **Generic Greetings:**

Uses “Dear Customer” instead of your real name, showing it is sent in bulk and not personalized.

**Summary of Phishing Traits :**

* Spoofed sender domain (“paypa1.com”).
* Suspicious and mismatched link (“malicious-link.com”).
* Urgency and threat to force reaction.
* Generic greeting, no personal details.
* No actual evidence of activity mentioned.
* (Would also look for header analysis issues if possible.)

**Recommendations:**

* Never click suspicious links in emails.
* Use online header analyzer tools when possible for suspected phishing emails.
* Do not open attachments from unknown senders.
* Report phishing emails to your IT admin or email service.

**References/Tools:**

* Phishing header analyzer: MXToolbox, Google Admin Toolbox
* Phishing samples/education: CanIPhish, phishing.org