| **No.** | **Indicator** | **Description** |
| --- | --- | --- |
| 1 | Spoofed Email Address | The sender uses support@paypalsecurity.com, which is not an official PayPal domain. Authentic emails come from @paypal.com. |
| 2 | Suspicious URL | The embedded link https://paypal.com.verify-user-login.info appears to contain “paypal.com” but is actually a malicious domain trying to mimic PayPal. |
| 3 | Urgency and Threats | The email pressures the recipient with urgency (“Your account has been suspended”, “within 24 hours”, “final warning”), a classic social engineering tactic. |
| 4 | Generic Greeting | “Dear Customer” is used instead of a personalized greeting. Legitimate companies usually address users by name. |
| 5 | Suspicious Attachment | An HTML file (verify\_account.html) is included. HTML attachments in emails often contain fake login pages to steal credentials. |
| 6 | Grammar and Style | The overall tone is aggressive and overly formal, which can be a red flag in phishing attempts. |
| 7 | Header Analysis (if available) | Email headers may show mismatched Return-Path, From, or Received domains, suggesting spoofing. Example: Return-Path: <phish@fraudmail.net> |

**Phishing Indicators Identified**

**Tools Used for Analysis**

* MxToolbox Email Header Analyzer – used to examine discrepancies in sender information and routing paths.
* URL Hover and Inspection – link hovered to reveal actual redirection target.
* Text Editor – to view and extract the full email body.
* Google Safe Browsing – to check whether the link domain is flagged as malicious.

**Conclusion**

The analyzed email demonstrates multiple phishing red flags, including a spoofed domain, deceptive URL, urgency, and an HTML attachment likely used to steal credentials. This exercise highlights how easily phishing attacks can bypass basic user awareness if proper training is not in place.

**Recommendations**

1. Always verify the sender’s email domain.
2. Never click on links or download attachments from unknown sources.
3. Use browser extensions to preview and scan URLs.
4. Report phishing attempts to the security team or email provider.