**Sample Email Overview**

* **Subject Line**: “Your Account Has Been Suspended – Immediate Action Required”
* **Sender Address**: support@paypa1.com
* **Date Received**: August 5, 2025
* **Attachments**: Account\_Verification.pdf
* **Links Included**: http://secure-paypa1.com/login
* **Phishing Indicators Identified**

**1. Spoofed Sender Address**

* Sender uses paypa1.com instead of the legitimate paypal.com.
* This is a classic example of domain spoofing.

**2. Header Discrepancies**

* Using an email header analyzer, the “Return-Path” and “Received” fields show routing through suspicious servers not associated with PayPal.
* SPF/DKIM authentication failed.

**3. Suspicious Links**

* Hovering over the login link reveals secure-paypa1.com, which is not a legitimate PayPal domain.
* URL mismatch is a strong phishing indicator.

**4. Urgent Language**

* Phrases like “Immediate Action Required” and “Your account will be permanently suspended” are designed to create panic and prompt hasty action.

**5. Spelling and Grammar Errors**

* “Your account has been suspend due to suspicious activity.”
* “Please verify your informations.”

**6. Unusual Attachments**

* PDF file named Account\_Verification.pdf urges the user to open and fill in credentials.
* Legitimate companies rarely ask for sensitive info via attachments.

**🧠 Summary of Phishing Traits**

| **Indicator** | **Description** |
| --- | --- |
| Spoofed Email Address | support@paypa1.com mimics PayPal |
| Header Authentication Failure | SPF/DKIM failed; suspicious routing |
| Mismatched URLs | Hover reveals fake login domain |
| Threatening Language | Urgency and fear tactics used |
| Grammar Errors | Multiple spelling and syntax mistakes |
| Malicious Attachment | PDF requesting sensitive information |

**✅ Recommendations**

* Do not click on any links or download attachments.
* Report the email to your IT/security team.
* Block the sender and mark the email as phishing.
* Educate users on identifying spoofed domains and urgent language.