1.SAMPLE EMAIL:

Subject: Your Account Has Been Suspended – Urgent Action Required!
From: support@paypalsecurity-alert.com
To: user@example.com
Date: June 25, 2025
Body:

Dear Customer,

We have noticed suspicious activity on your PayPal account.
To protect your account, we have temporarily suspended it.

Please click the link below to verify your information:

https://paypal.com.verify-login-alerts-secure.com

Failure to verify within 24 hours will result in permanent suspension.

Regards,
PayPal Security Team

2.Examine sender's email address for spoofing.

Actual Address: support@paypal-security.com

From: support@paypalsecurity-alert.com

- ✓ Domain is not official – The correct PayPal domain is paypal.com, but here it is paypalsecurity-alert.com, which is fake.
- ✓ Extra words in domain – "security-alert" is added to mislead the user into trusting it.
- ✓ No ownership by PayPal – This domain is not registered to PayPal, making it highly suspicious.

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

- **From:** support@paypalsecurity-alert.com
- **Return-Path:** <fraud@paypal-verification-alert.com>
- **SPF: Fail**
- **DKIM: Fail**
- **Sending IP:** Linked to unknown server in another country

SPF Check: Fail - Sender is not authorized to send emails for that domain

DKIM Check: Fail - Digital signature is missing or incorrect

4.Identify suspicious links or attachments.

Link in the body: https://paypal.com.verify-login-alerts-secure.com

- Appears to include “paypal.com”, but that’s a trick.
- **Actual domain:** verify-login-alerts-secure.com
- paypal.com is just a **subdomain**, not the real site.

No file attachment present, but phishing emails often include .zip, .pdf, .exe or .html files containing malware or phishing forms.

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

The email uses urgent and threatening language like “suspicious activity,” “temporarily suspended,” and “permanent suspension in 24 hours” to pressure the recipient into taking immediate action.

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

Visible Link: https://paypal.com.verify-login-alerts-secure.com

Actual Destination: verify-login-alerts-secure.com (not PayPal)

7.Verify presence of spe ling or grammar errors.

While the email has no obvious spelling errors, it shows subtle grammar issues and generic phrasing, which are common signs of phishing attempts.

8.Summarize phishing traits found in the email

- Spoofed sender address – Uses a fake domain: paypalsecurity-alert.com.
- Failed authentication checks – Likely SPF/DKIM/DMARC failures (if header analyzed).
- Suspicious link – Contains a fake domain designed to look like PayPal.
- Urgent/threatening language – Claims account suspension within 24 hours.
- Mismatched URL – Link pretends to be PayPal but redirects to a malicious site.
- Generic greeting and grammar – Uses “Dear Customer” and has formal, unnatural tone.

The email shows multiple phishing indicators—fake sender, threatening language, deceptive links, and generic wording—confirming it as a phishing attempt.