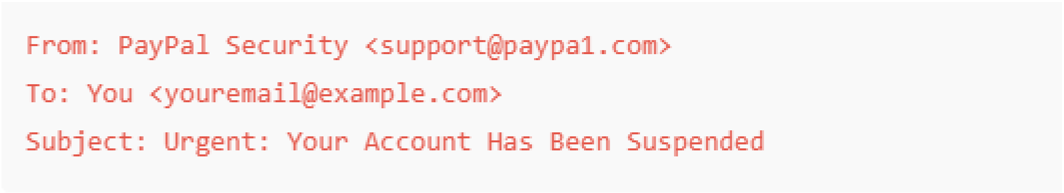
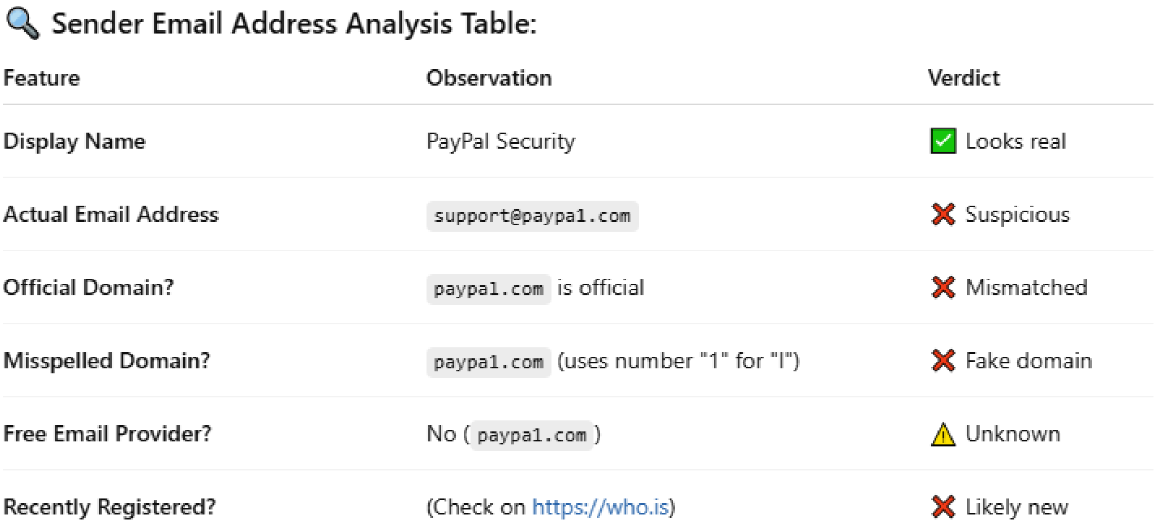
Step 2: Inspect the Sender's Email Address

- Check for:
  - Fake domains (e.g., `paypal-service@gmail.com` instead of `service@paypal.com`)
  - Misspelled domains (e.g., `paypa1.com` instead of `paypal.com`)
  - Free email providers used as senders (`@gmail.com`, `@yahoo.com`, etc.)



```
From: PayPal Security <support@paypa1.com>
To: You <youremail@example.com>
Subject: Urgent: Your Account Has Been Suspended
```



🔍 Sender Email Address Analysis Table:

Feature	Observation	Verdict
Display Name	PayPal Security	✅ Looks real
Actual Email Address	`support@paypa1.com`	❌ Suspicious
Official Domain?	`paypal.com` is official	❌ Mismatched
Misspelled Domain?	`paypa1.com` (uses number "1" for "l")	❌ Fake domain
Free Email Provider?	No (`paypa1.com`)	⚠️ Unknown
Recently Registered?	(Check on https://who.is)	❌ Likely new

Conclusion:

The email is sent from a **spoofed domain** (`paypa1.com`) designed to look like PayPal (`paypal.com`).
This is a **clear sign of phishing**, attempting to mislead the recipient by using a lookalike domain.