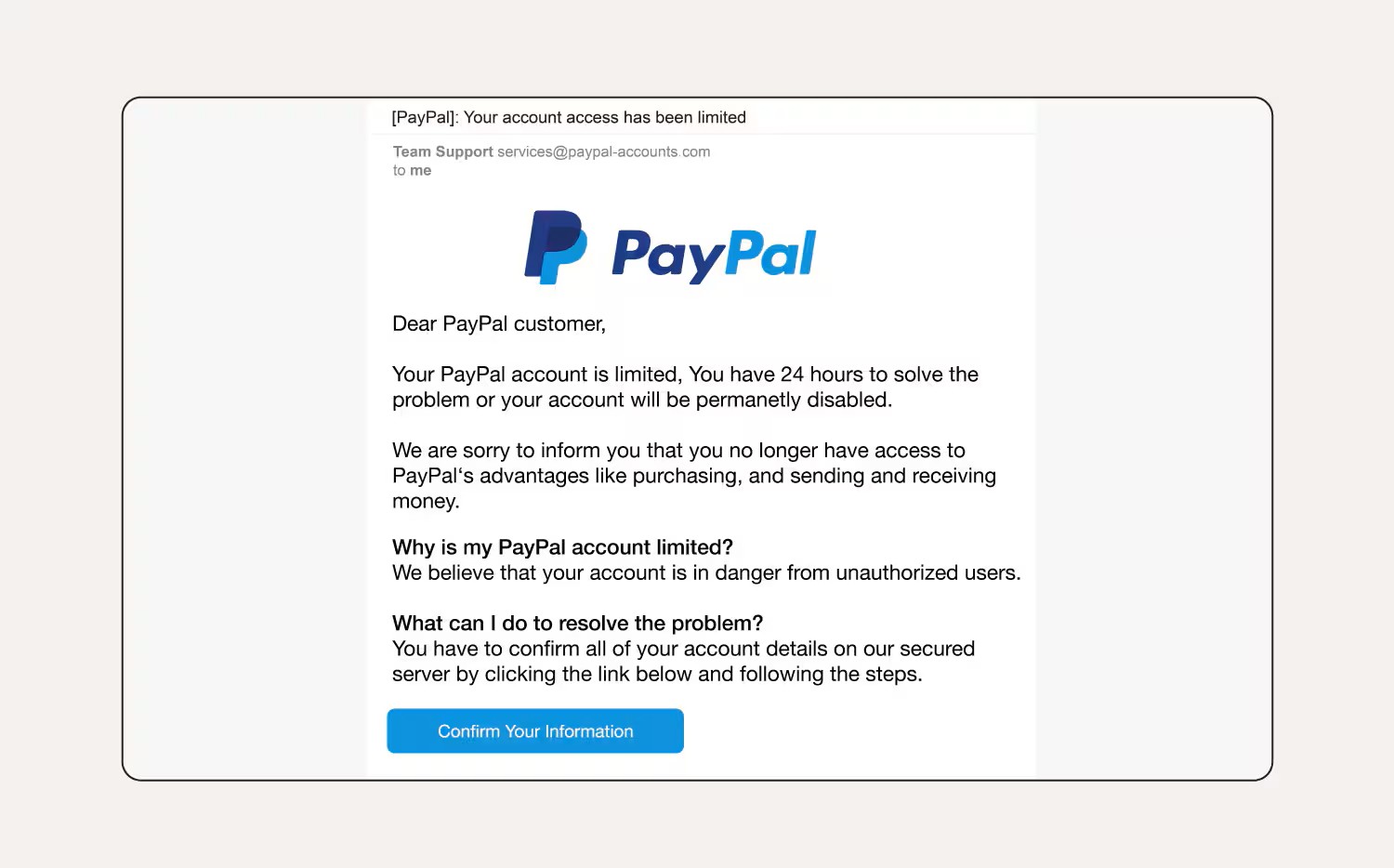
# **Task 2**

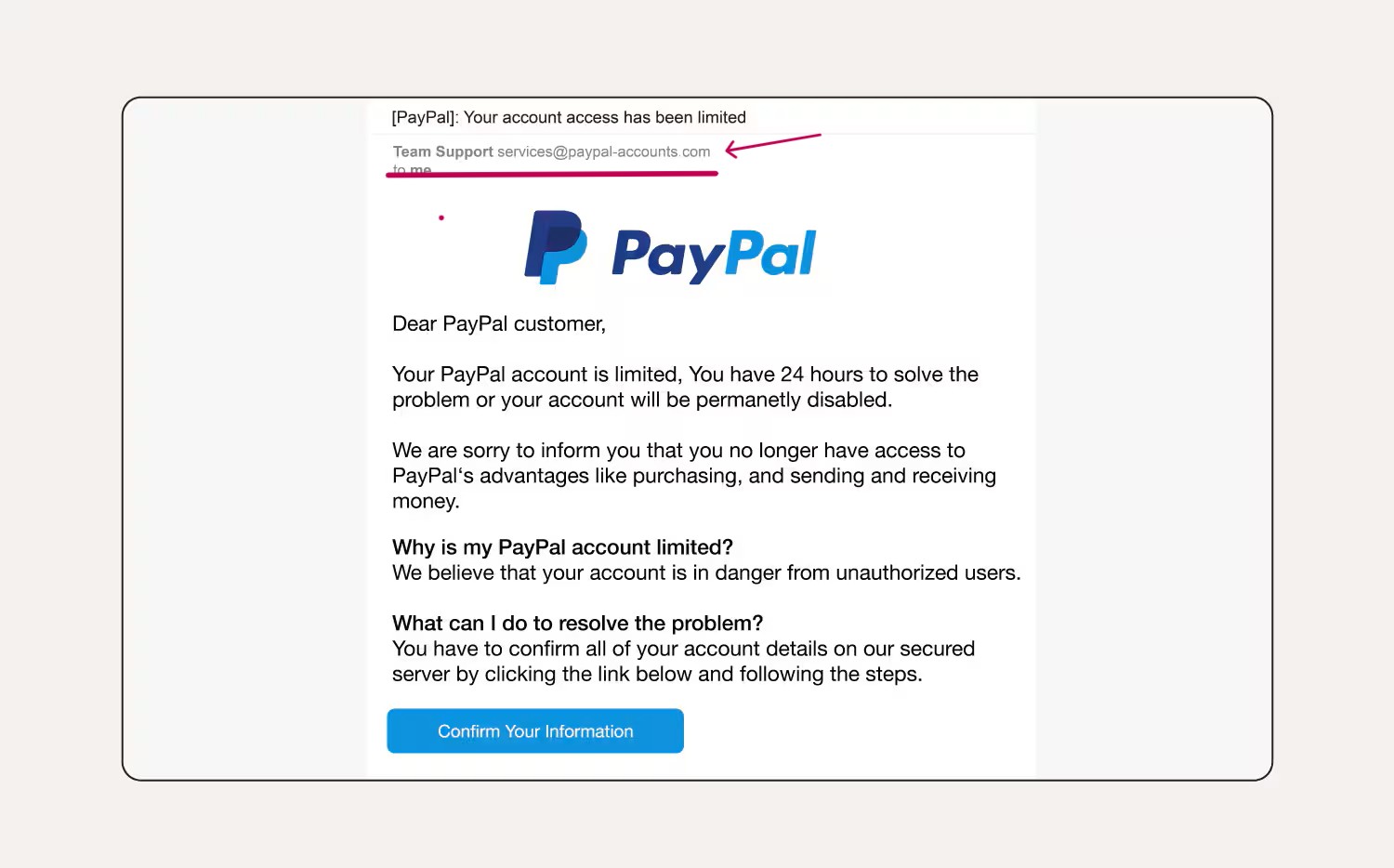
# **Analyze a Phishing Email Sample**

**Task: Phishing Email Analysis**  
I analyzed a sample phishing email by examining the sender's address, headers, suspicious links, and urgent language to identify common phishing traits and security risks.

SAMPLE EMAIL : 

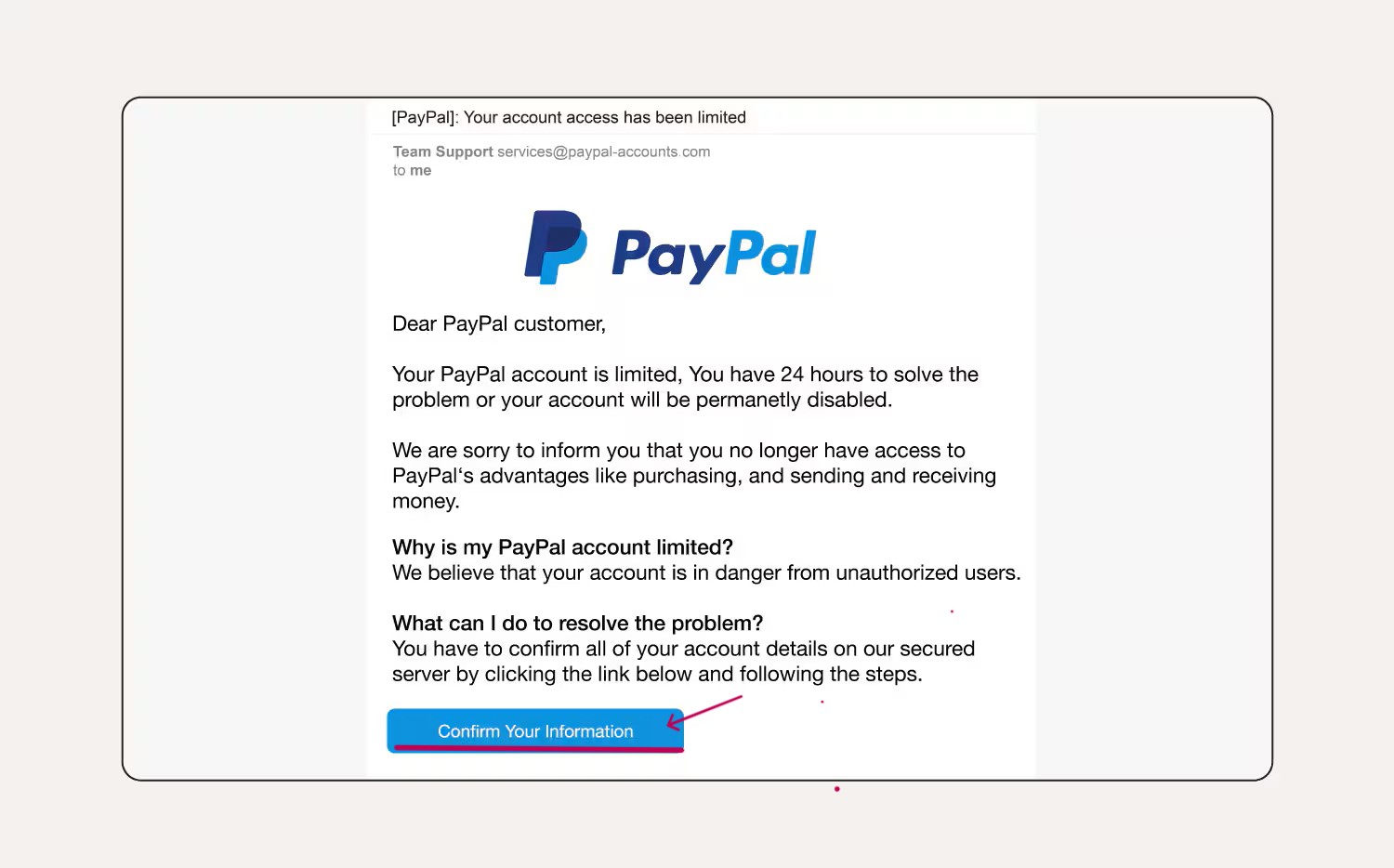
Suspicious Email Detected:

**The email was sent from support@paypal-accounts.com, which cleverly uses supporting service-based words to impersonate the official PayPal domain — a common phishing tactic.**

****

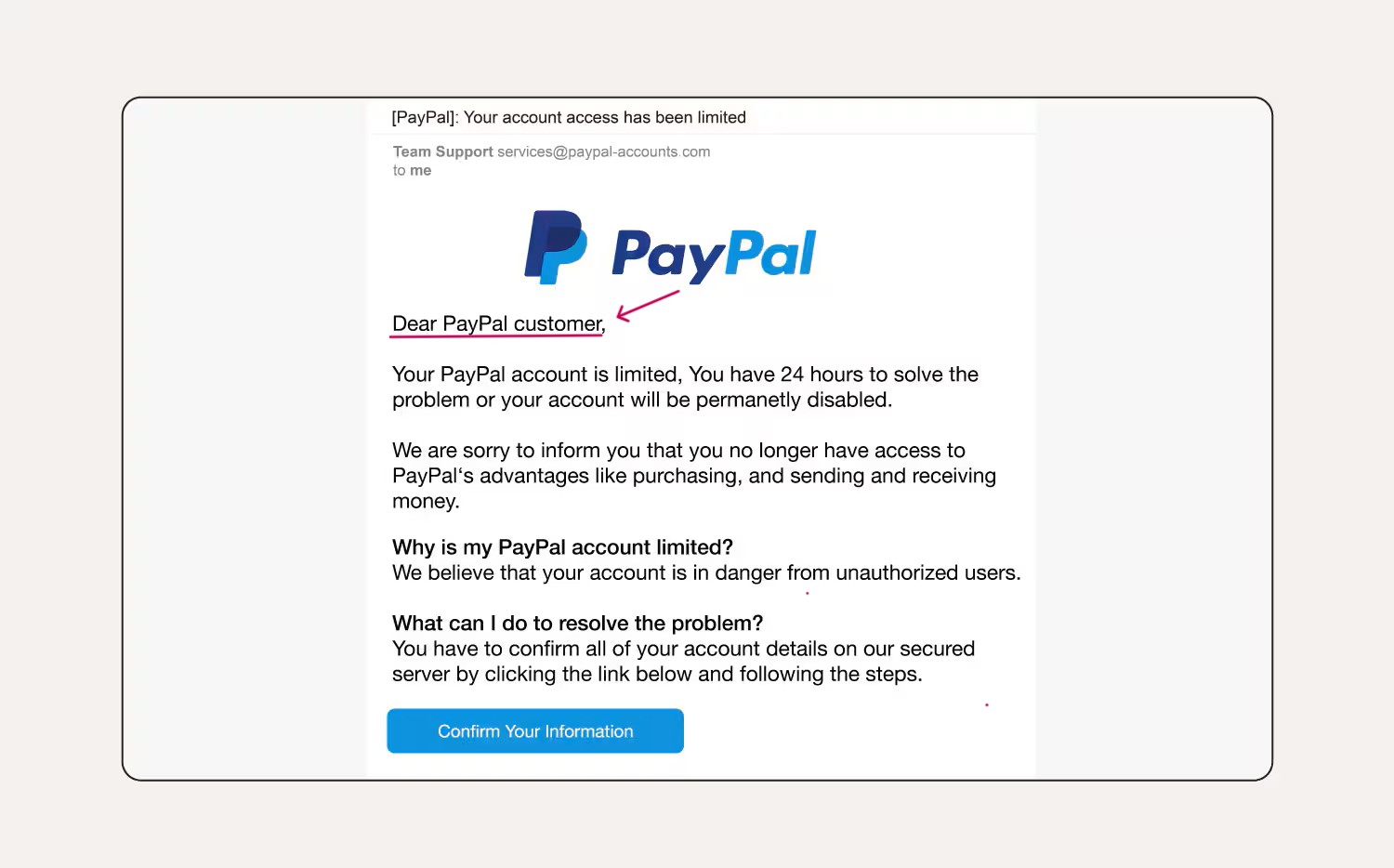
**Deceptive Confirmation Links:**

**The email urges the recipient to click a “Verify Now” button that redirects to a fake website, disguised to look like PayPal. This malicious link is designed to steal login credentials by tricking users into entering sensitive information on a fraudulent page.**

****

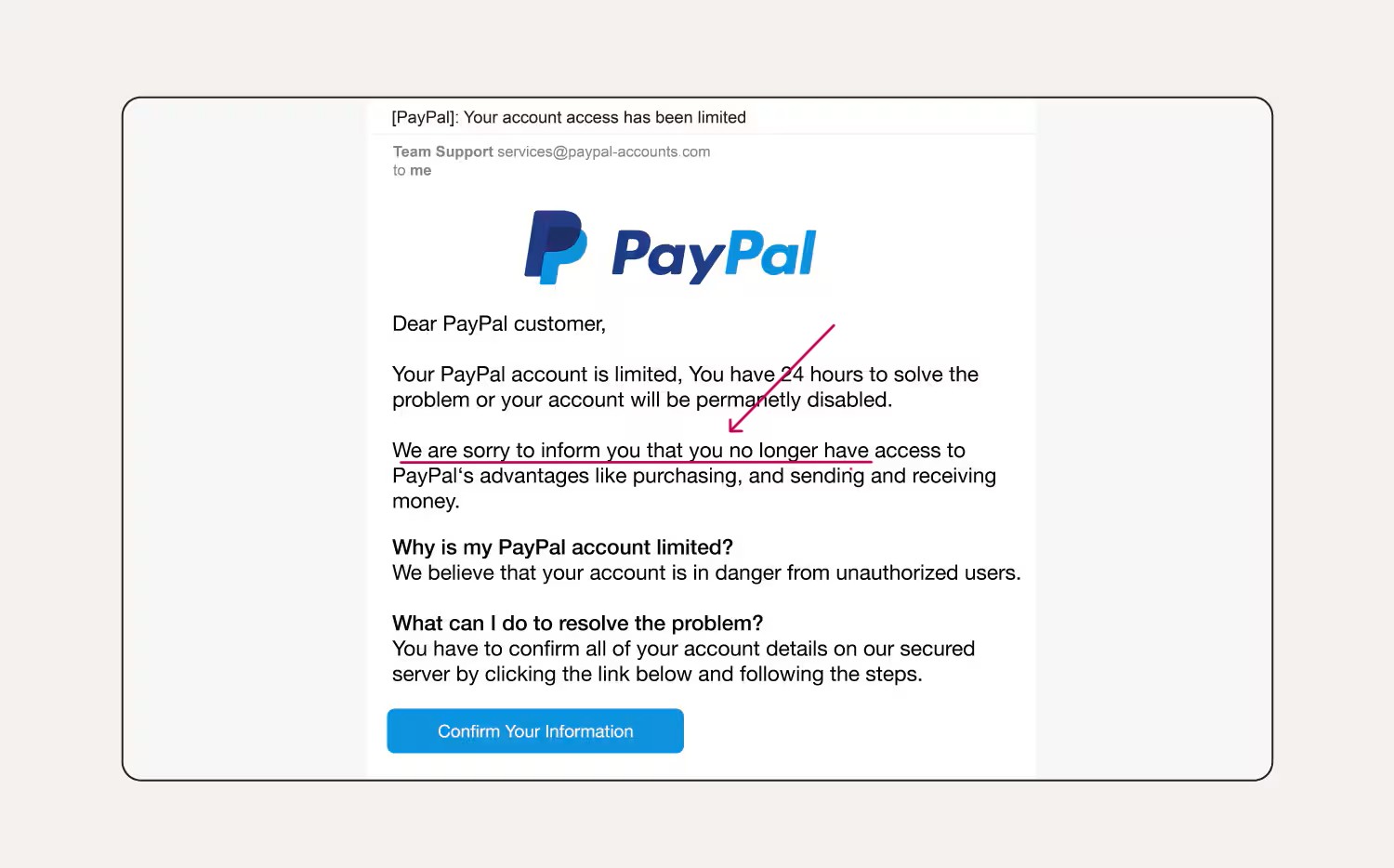
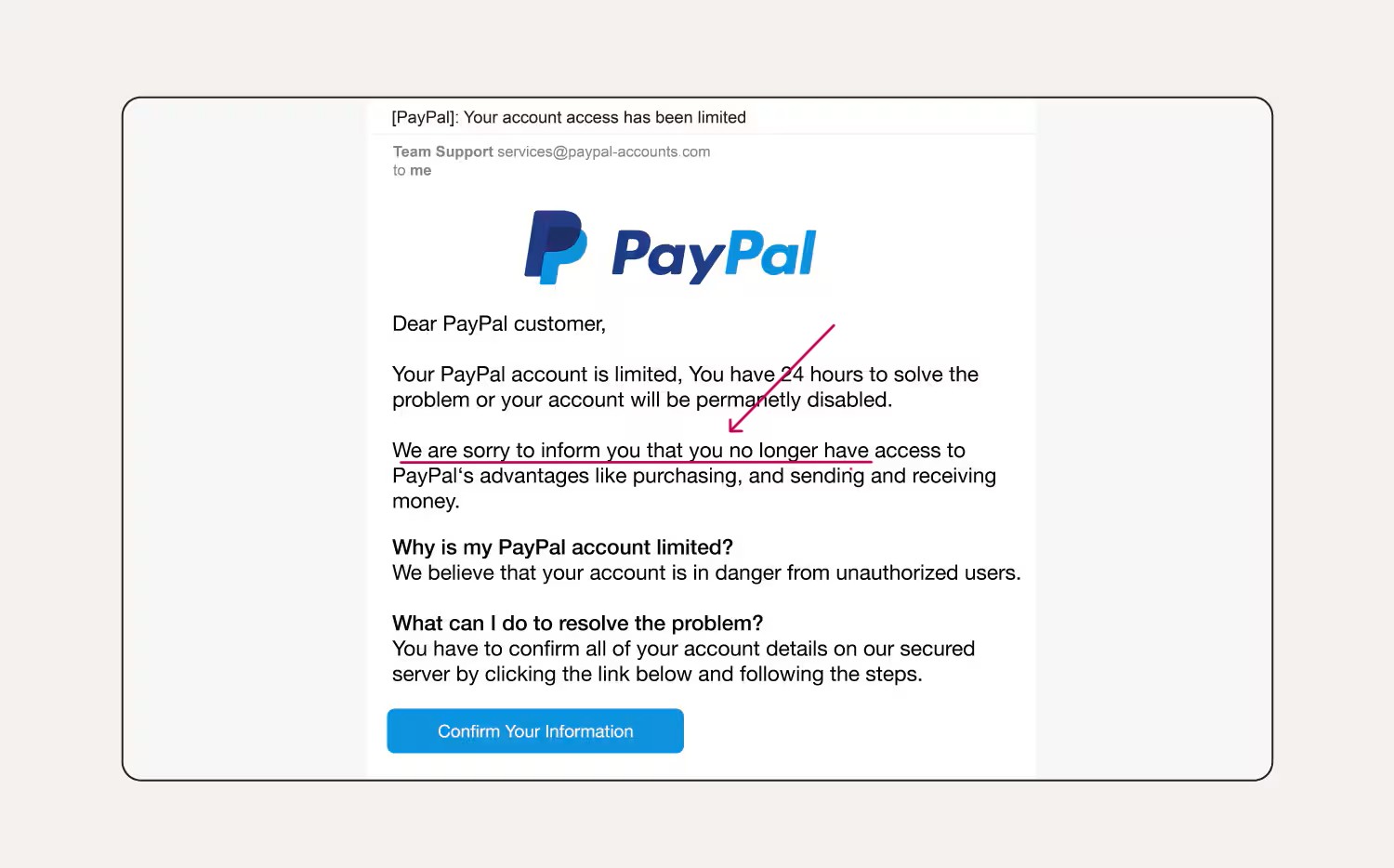
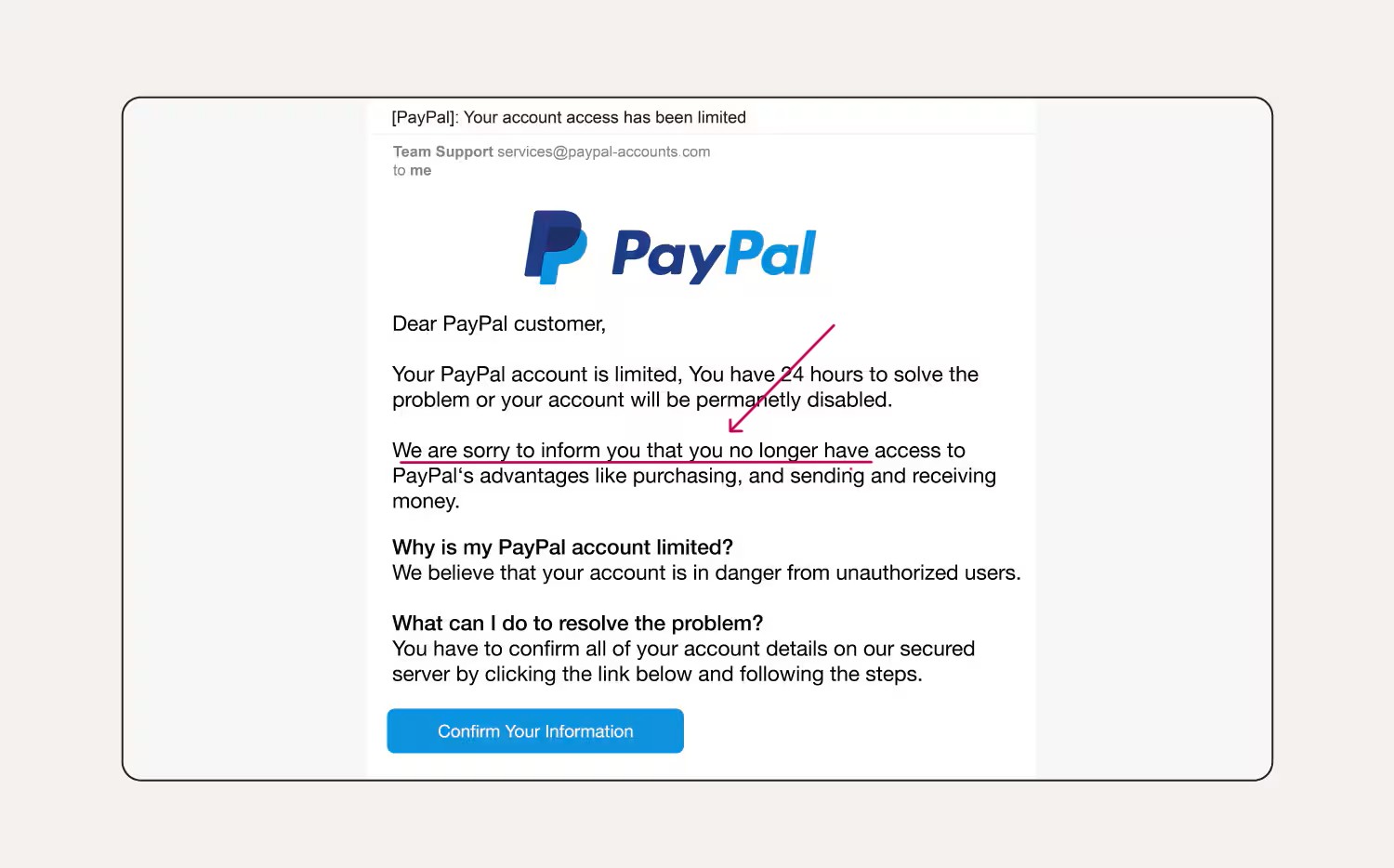
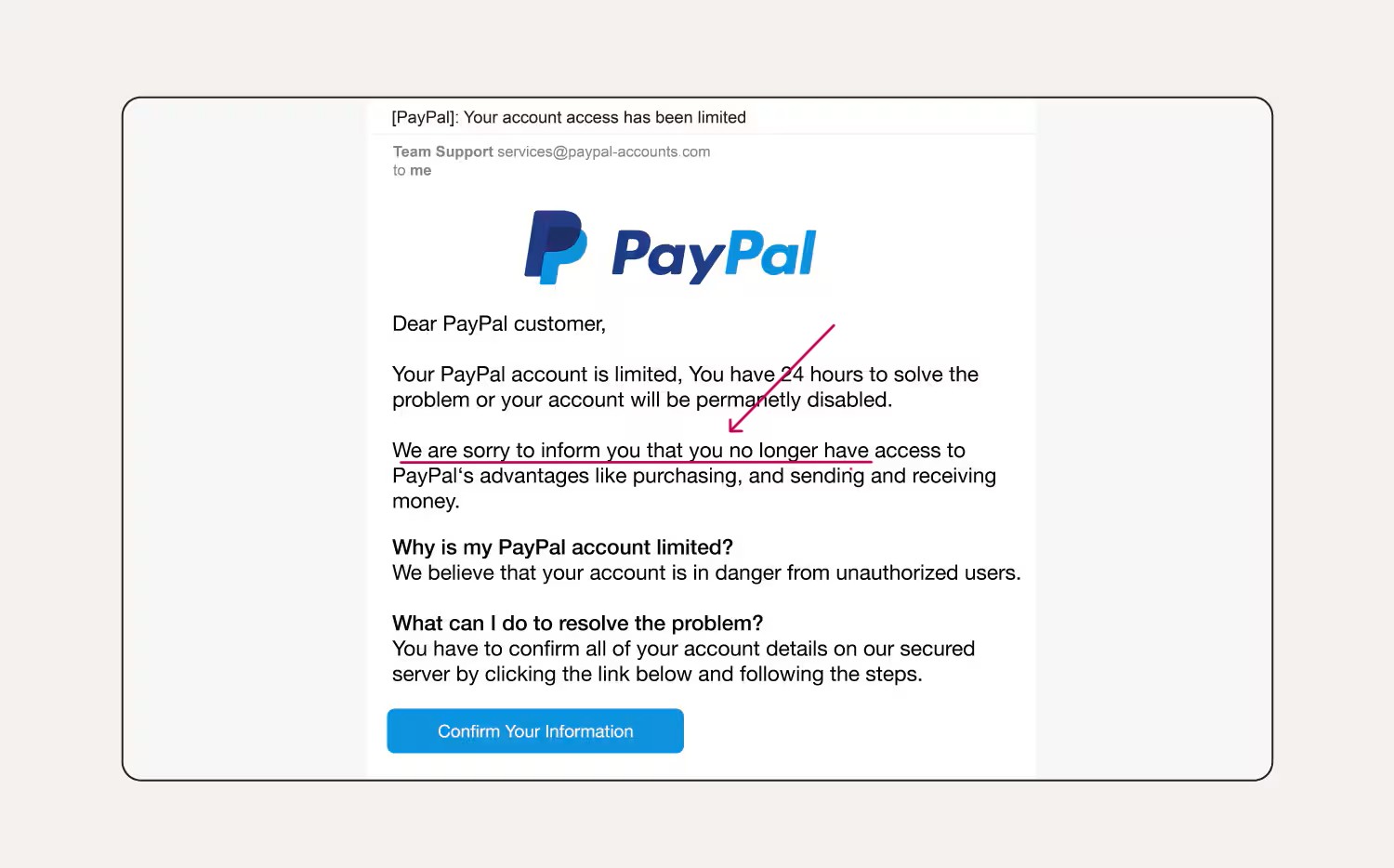
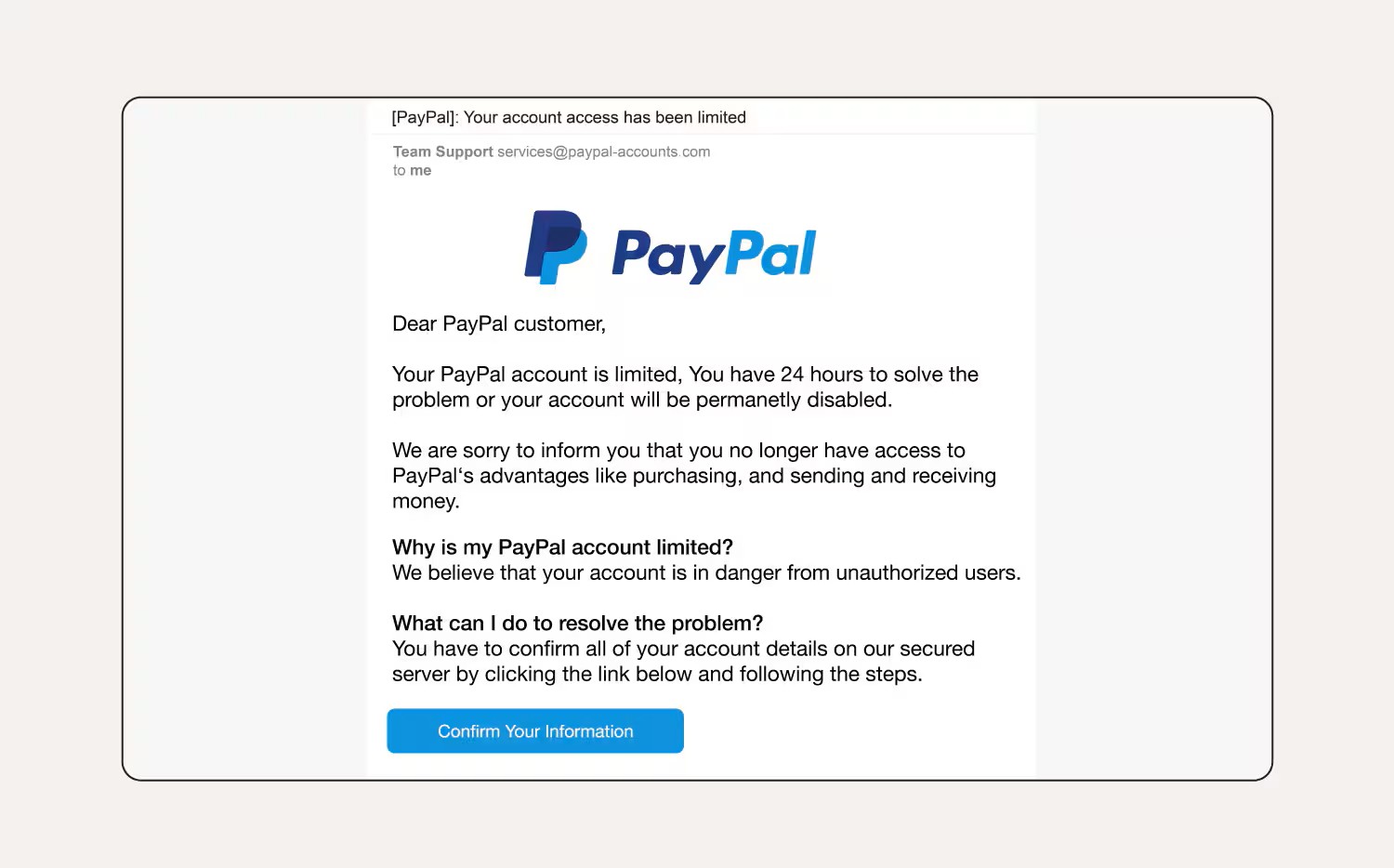
**Non-Specific Recipient Addressing:**

**the email begins with a generic greeting like "Dear PayPal Customer", instead of using the recipient’s actual name. Legitimate companies usually personalize emails, so this lack of personalization is a common phishing red flag.**

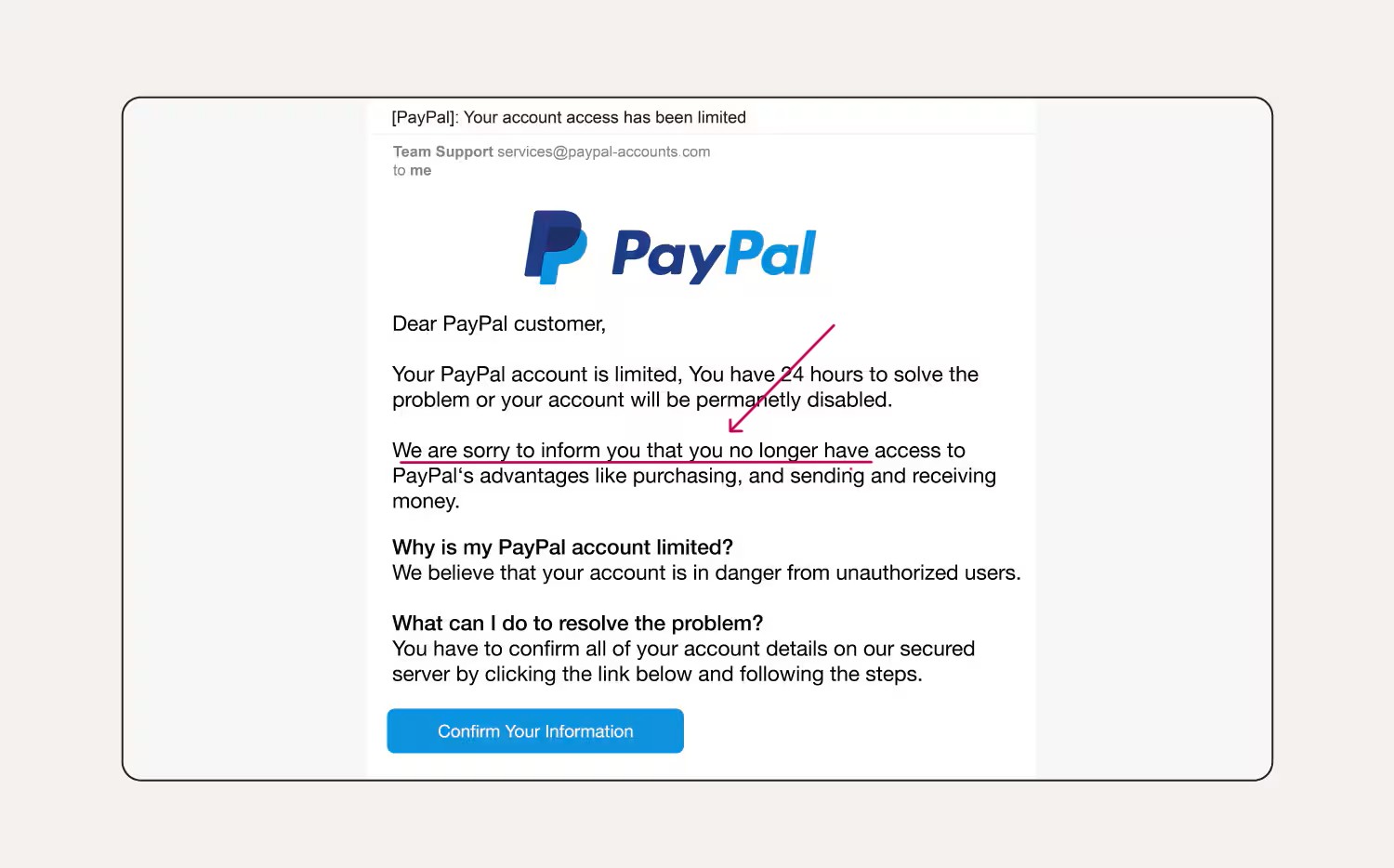
****

**Grammatical Red Flags:**

**The email contains awkward phrasing such as “Failure to comply will result in permanent suspension,” which sounds unprofessional and overly aggressive. Minor spelling or grammar mistakes like missing punctuation or unusual sentence structure are often signs of a phishing attempt.Top of Form**

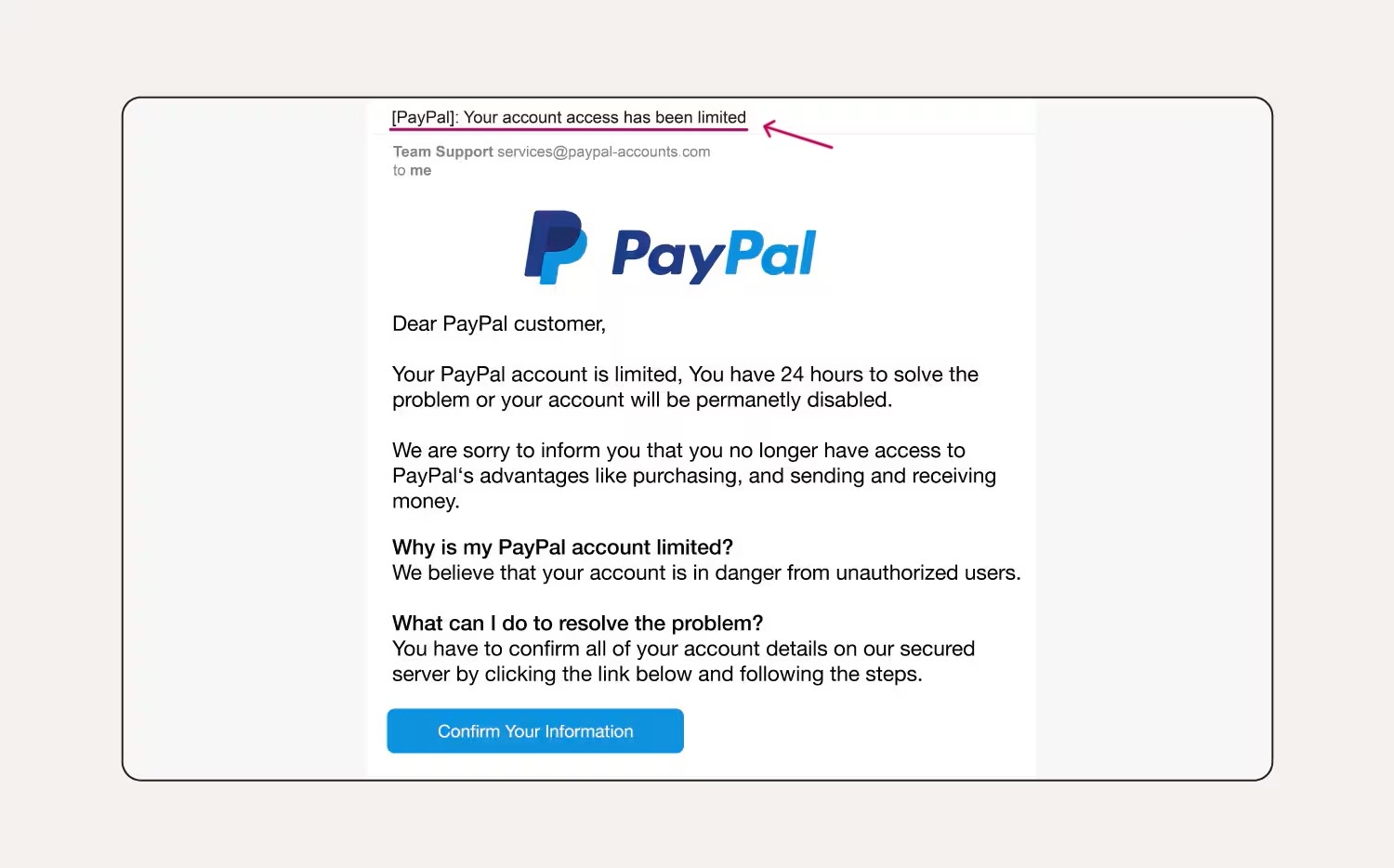
****

**Bottom of Form**



**False Account Restriction Notice:**

**The subject line claims that your account access has been “limeted,” clearly showing a spelling error in a serious alert. Scammers use such fake restriction warnings to create panic and trick users into clicking malicious links.**

****

**Summary of Phishing Traits Found in the Email**

* ✅ **Spoofed Sender Address:** Domain mimics a legitimate one (e.g., paypa1.com instead of paypal.com).
* 🔗 **Suspicious Links:** URLs redirect to fake websites designed to steal credentials.
* 🧾 **Generic Greeting:** Uses "Dear Customer" instead of your name — lacks personalization.
* ⚠️ **Urgent or Threatening Language:** Creates pressure with messages like “Account will be suspended in 24 hours.”
* ❌ **Spelling and Grammar Errors:** Words like “limeted” and awkward sentence structure reduce credibility.
* 🕵️ **Mismatched URLs:** Hovered links do not match the visible link text.
* 📎 **Unusual Attachments:** Includes suspicious HTML file or forms designed to capture sensitive data.
* 📬 **Fake Account Notifications:** Claims of access restrictions without any real verification.
* 🚨 **Lack of Security Signs:** No official branding, secure HTTPS links, or verified contact info.