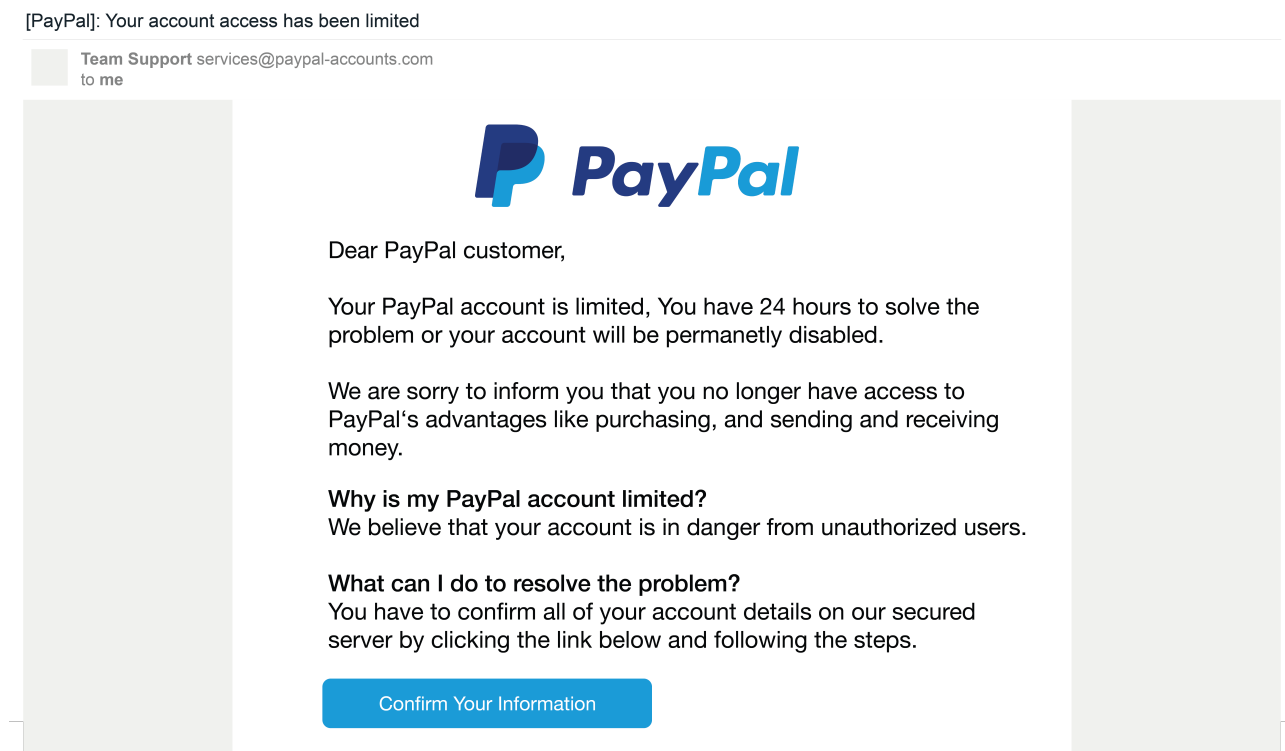




Email example






Email Details

- **Subject:** [PayPal]: Your account access has been limited
- **From:** services@paypal-accounts.com
- **Sender Name:** Team Support

1. Spoofed or Suspicious Sender

- **Email address:** services@paypal-accounts.com
-  Appears to impersonate PayPal.
-  **Red flag:** Not a legitimate PayPal domain (paypal.com). The domain paypal-accounts.com is likely registered to mimic the official brand.

2. Urgent or Threatening Language

-  "Your PayPal account is limited"
-  "You have 24 hours to solve the problem or your account will be permanently disabled."
-  **Red flag:** Creating a false sense of urgency is a hallmark phishing tactic to rush users into clicking malicious links.


3. Generic Greeting

- **Greeting:** “Dear PayPal customer”
- **✗ Red flag:** Legitimate companies like PayPal usually address you by your full name to confirm the message is intended for you.

4. Suspicious Link or CTA

- **Button:** “Confirm Your Information”
- **✗ Red flag:** The button likely links to a spoofed login page designed to steal credentials. (You should hover over it in a real email client to inspect the URL.)

5. Grammar/Spelling Errors

-  Several small grammatical issues:
 - “You have 24 hours to solve the problem” → awkward and unnatural phrasing.
 - “permanently” is a common typo in these scams (not in this image, but common).
 - Repetitive use of “PayPal” and odd capitalizations.
- **✗ Red flag:** Minor grammar flaws often appear in phishing emails created by non-native speakers or quickly generated scams.

6. Brand Misuse

- **PayPal logo** is used to increase legitimacy.
- **✗ Red flag:** Use of brand images doesn't validate authenticity. Anyone can copy/paste logos into scam emails.

7. Unverified or Unsafe Domain (Header Needed to Confirm)

- The domain in the “from” address is not PayPal-owned.
- If email headers were available, SPF/DKIM/DMARC failures would likely confirm this is not from an authorized source.

Summary

Trait	Evidence
Spoofed Sender	<code>services@paypal-accounts.com</code> – not a PayPal domain
Urgent/Threatening Language	24-hour time limit, account disable warning
Generic Greeting	"Dear PayPal customer" instead of using full name
Suspicious Link	“Confirm Your Information” button – destination unknown

Grammar Errors	Awkward phrasing, unnatural sentence flow
Brand Logo Misuse	Legitimate PayPal logo copied into a fake email