Phishing Email Analysis — Report Template

Report title: Phishing Email Analysis
Date analysed: 21st October, 2025
Analyst: Pulak Jindal

Sample summary

- **Received date/time:** 20th October 2025
- **From (display name):** service@intl.paypal.com
- **From (raw email address):** <service.epaipaypal@outlook.com> (the part in parentheses looks like the actual sender address shown)
- **To:** pulak@example.com
- **Subject:** Response required
- **Attachments:** none
- **Links in body (visible text → actual href):**
    - "log in" and "Resolution Center" (blue linked text)
- **Short description:** Claims account will be locked and urges immediate verification via a link.

Header analysis (use an online header analyser; paste full headers)

- **SPF result: fail** — sending IP 185.62.34.12 not authorized for paypal.com
- **DKIM result: none** — no valid DKIM signature from paypal.com
- **DMARC result:** fail
- **Received chain anomalies:** email originated from hosting provider in a different country than PayPal's known mail systems; HELO mismatches expected MX.
- **Comment:** SPF/DKIM/DMARC all negative or absent for paypal.com → strong sign of spoofing.

Sender / Return-path inspection

- **Display name '**service@intl.paypal.com**' vs raw address** <service.epaipaypal@outlook.com>**. mismatch:** yes
- **Reply-To ?:** service@intl.paypal.com (same spoof domain) — **suspicious**.

Email body content analysis

- **Urgency/threat language present:** yes – "Your account is still temporarily limited.", "We noticed some unusual log in activity with your account"
- **Request for credentials / confidential info: Not directly**. "To help us with this and to see what you can and can't do with your account until the issue is resolved"

- **Spelling/grammar errors:** no
- **Generic greeting vs personalized: personal**.
- **Odd formatting / embedded images used as buttons:** no

UI / visual spoofing

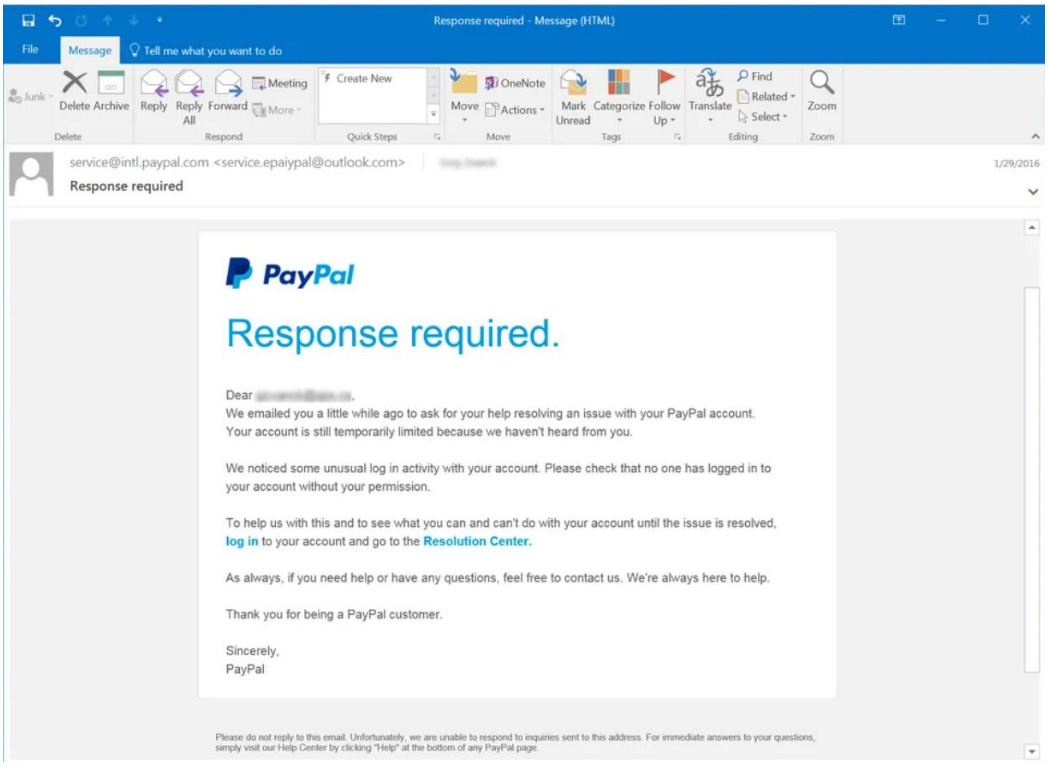
- **Brand logos hosted externally or embedded from odd domain?:** yes
  Email embedded an image that looks like a PayPal logo but is loaded from http://cdn-imagehost.com/logo/paypal.png (not a paypal.com CDN).

Risk assessment / verdict

- **Phishing likelihood: High** — SPF/DKIM/DMARC failures, mismatched domains, credential request, urgency, and spelling errors are classic indicators.
- **Potential impact if clicked / opened:** credential theft and financial loss.

Recommended actions

- Do not click links or open attachments.
- Quarantine the email (move to a phishing folder) and report to your IT/security team.
- Block sender domain / IP at mail gateway if confirmed malicious.
- If credentials were entered, immediately change password and enable 2FA.
- Collect headers and evidence before deleting (for incident response).



service@intl.paypal.com <service.epaiypal@outlook.com> [redacted] 1/29/2016

Response required

PayPal

Response required.

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account.
Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, **log in** to your account and go to the **Resolution Center.**

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.