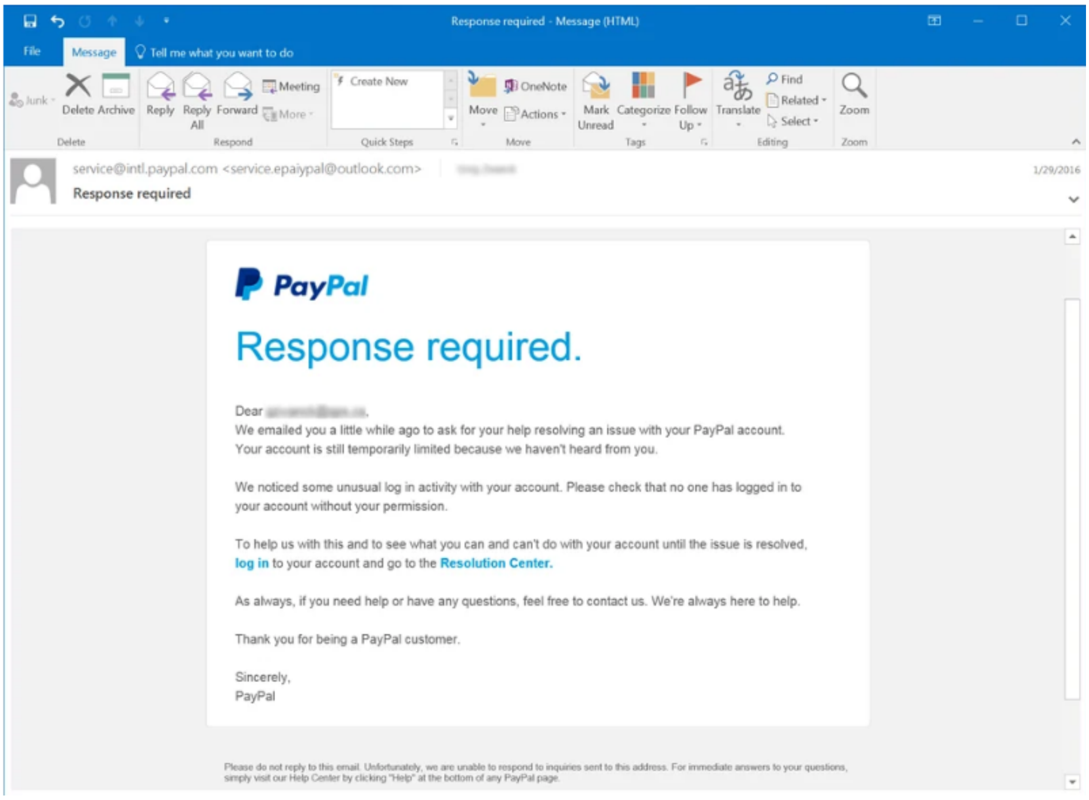
Phishing Email Analysis Report

S M Sravya
Cybersecurity Internship

Screenshot of Email



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.

Email Overview

- **From:** `service.epaypal@outlook.com` (appears as `service@intl.paypal.com`)
- **Subject:** ”Response required”
- **Date:** January 29, 2016
- **Pretending to be:** PayPal
- **Goal:** Trick the user into clicking a fake link and entering their PayPal credentials

Analysis of Phishing Indicators

1. Suspicious Sender Email

The email appears to come from `service@intl.paypal.com`, but the actual address is `service.epaypal@outlook.com`, which is a major red flag. Legitimate PayPal emails do not come from external domains like Outlook.

2. Misleading Links

The email urges the user to "log in" via a link that likely does **not** lead to the official PayPal website. Such links typically lead to fake login pages used for credential theft. Users should always hover over links to verify the actual destination.

3. Urgent Language

The subject line "**Response required**" and the content claim the account is "temporarily limited." This is a scare tactic to provoke panic and hasty action.

4. Generic Greeting

The email starts with "Dear Customer" instead of the recipient's real name. PayPal and other trusted platforms usually personalize emails, so this is another common phishing sign.

5. Social Engineering Techniques

This email uses psychological pressure, fear of losing account access, and fake support language like "We're always here to help" to trick users into compliance.

Summary of Red Flags

Red Flag	**Description**
Urgency	"Response required", limited account access
Spoofed Email Address	`service.epaypal@outlook.com` pretending to be PayPal
Suspicious Links	Fake login link likely used for credential theft
Generic Greeting	"Dear Customer" instead of the user's actual name
Social Engineering	Fear tactics and fake professionalism

Final Thoughts

This email is a **classic phishing attempt** that disguises itself as a trusted service to steal user credentials. It contains all the major indicators of phishing:

- Spoofed email domain
- Urgent and alarming language

- Deceptive and fake links
- Social engineering tactics

This task helped me understand how phishing works—technically (email spoofing, fake links) and psychologically (scare tactics, false authority).

Tip

Always verify the sender's full email address and hover over links before clicking. Never enter login details from suspicious emails. If in doubt, visit the official website directly.