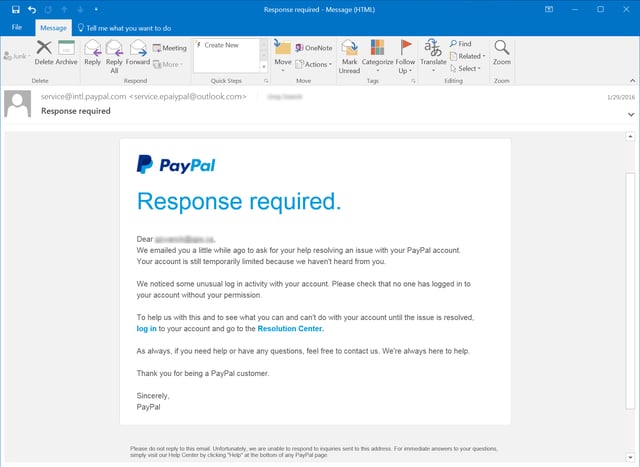
1.This is an example phishing email downloaded from online. Here it appares to be sent from PayPal, a famous payment website used widely in foreign countries. Now lets analyze this to confirm that it is not a real one and is a phishing email.



2. Now let’s analyse the sender’s email address. Here, it is [service@epaiypal@outlook.com](mailto:service@epaiypal@outlook.com). As you can see the spelling of PayPal is written mistakenly as paiypal, from this itself we can confirm that it is a spoof mail. No reputed company would make a mistake in their brand name while sending mails like these.

3. In the header of this mail, we can see that it contains [service@intl.paypal.com](mailto:service@intl.paypal.com) which looks more like a legitimate one and it is a trick by the sender to deceive us but if you look closely on the senders email we can come to know that this is a fake one. Also, the subject of this mail is “Response required” which is used to create a state of urgency on users and it is a common trick used by the attackers.

4. Here in this email, we can see there are some suspicious links, there is an login link and a resolution centre link, if we go inside the log in link and enter our paypal login credentials there it may lead to loss of our data. So this is very dangerous to enter into the links present in these type of phishing emails.

5. Now let us look for urgent or threatening language in this email. This email says that they have already contacted the user seeking help for resolving issue in their PayPal account and also it stated that the account is temporarily limited as they haven’t heard back from the user. So this type of message threatens the user and make them nervous and also as said earlier the Response required subject in the email makes the user to act urgently.

6. As this is just an image, I used chatgpt to give me a sample url that would be present if the link was clicked. So the given sample url by chatgpt is <http://secure-paypal-login.com/verify> and it also shows what the real url of paypal would look like and which is <https://www.paypal.com/login> and we can see that the real paypal login link has the paypal.com keyword and the legitimate url will always have that whereas in case of malicious link it is present as secure-paypal-login.com, so if we see some extra words like these in the domain name we can know that it is a fake one.

7. Yes, there are many mistakes that make this mail standout from the original paypal mail because in the first line they have used log in instead of login and paypal would always use login without having a space between them. Also they have used more casual way in writing the lines in the mail like “you can let us know everything is okay by logging in to your account” but paypal would use sentence like “Please verify your identity by logging in to your account”. Also there is a punctuation error in one of the sentence, “We’ll review your response and if we can confirm your identity, we’ll restore your account”, here there should be a comma(,) after the word response and before the word and. So there are these type of grammatical, logical and spelling mistakes in this email which makes this email to be known as a fake one by analyzing it thoroughly.

8. In summary, there are various phishing traits like Fake sender address, mismatched domain, Urgent/Threatening language, Spelling/Grammar issues, Suspicious links and informal tone. So these traits make this email a fake one and easy to differentiate it from the real one.