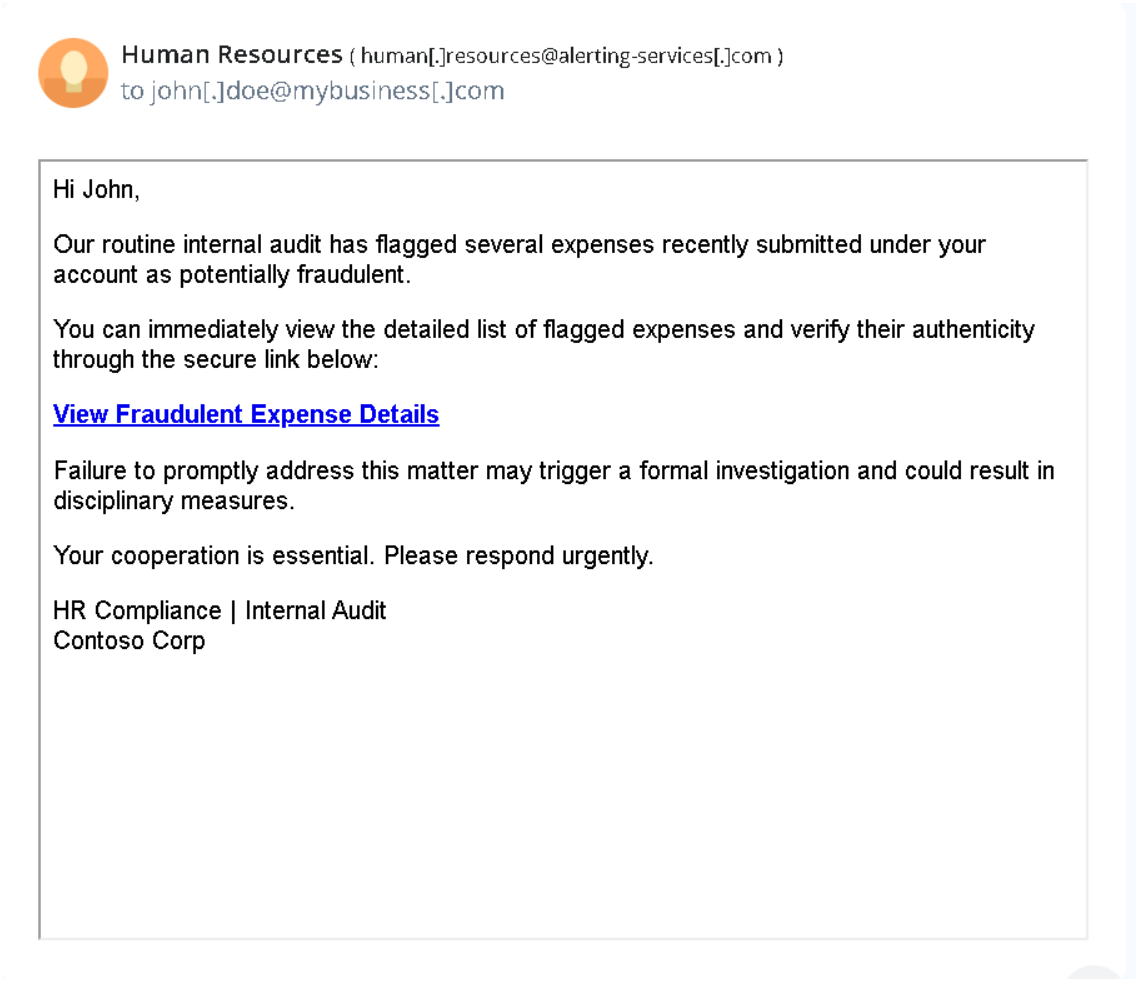
Task 2:

By Niranjan Manoj

Using a free sample available online I am examining the email address for spoofing.



Human Resources (human[.]resources@alerting-services[.]com)
to john[.]doe@mybusiness[.]com

Hi John,

Our routine internal audit has flagged several expenses recently submitted under your account as potentially fraudulent.

You can immediately view the detailed list of flagged expenses and verify their authenticity through the secure link below:

View Fraudulent Expense Details

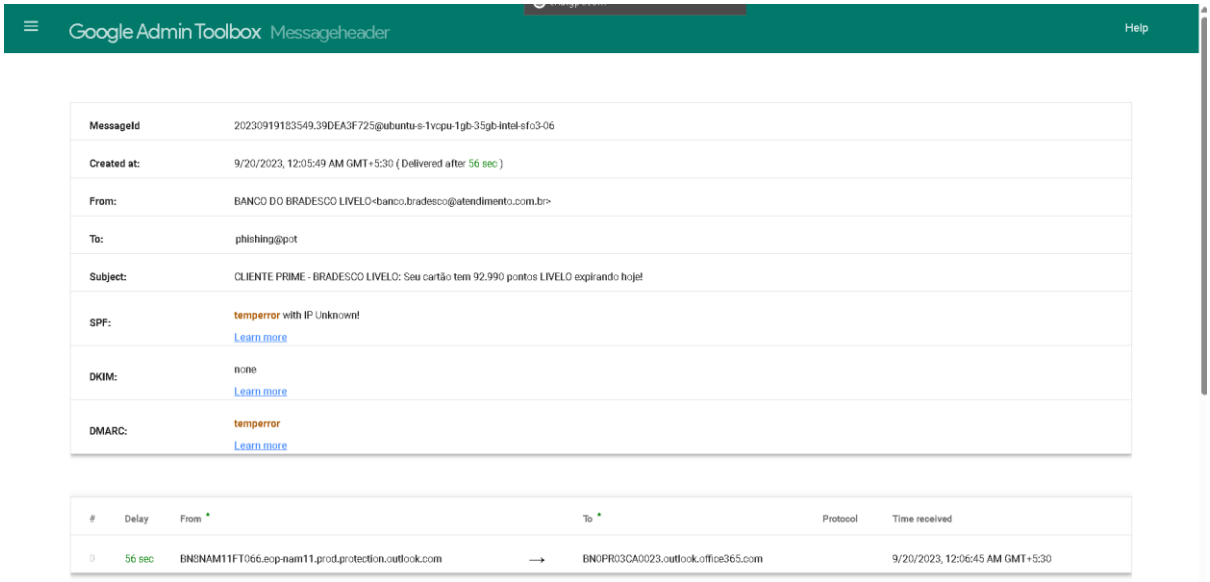
Failure to promptly address this matter may trigger a formal investigation and could result in disciplinary measures.

Your cooperation is essential. Please respond urgently.

HR Compliance | Internal Audit
Contoso Corp

2. upon examining we see that the sender uses [.] instead of using the actual domain which is a common way to fool senders into thinking it is the original domain.

3. using google online header analyzer I checked the email for discrepancies which included an spf and DMARC errors which highlights that the mail is spoof.



5. threatening language such as formal investigation and disciplinary measures are used so as to create a fake sense of urgency.

6. a misleading url is also present in the email.

A summary of all the phising traits in this mail are as follows:

Suspicious sender domain (doesn’t match company name)

Urgent and threatening tone

Suspicious link with potentially mismatched URL

No attachments but clickable link to a likely malicious site