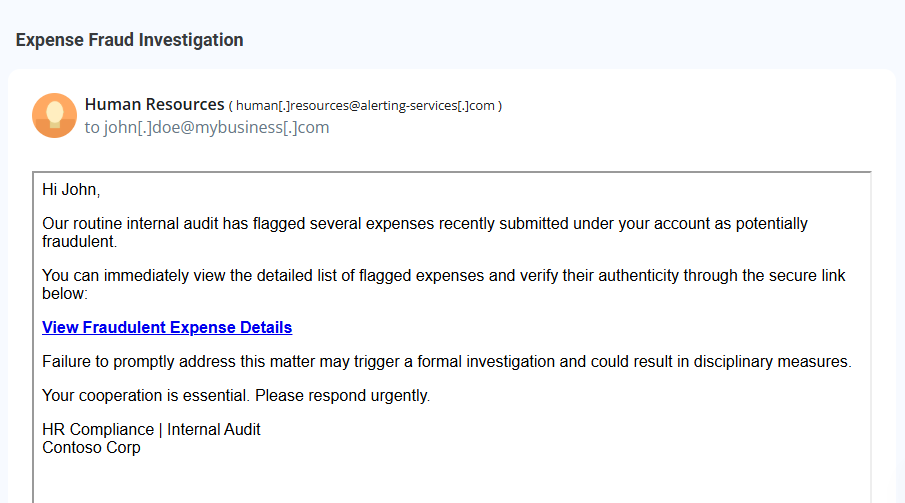
TASK 2: ANALYZING A PHISHING EMAIL SAMPLE

Objective:

Identify phishing characteristics in a suspicious email sample

Email sample:



**Phishing Indicators Report**

**Suspicious Sender Address**

* **From:** human[.]resources@alerting-services[.]com
* **Issue:** The domain alerting-services.com is unusual and not clearly associated with the claimed organization, **Contoso Corp**. Legitimate internal communications should come from the company’s verified domain (e.g., @contoso.com).

**Deceptive Link**

* **Link Text:** View Fraudulent Expense Details
* **Issue:** The link could lead to a phishing website designed to steal login credentials or personal information. The actual URL is hidden behind a hyperlink, a common phishing tactic.

**Urgency and Threats**

* **Wording:** *“Failure to promptly address this matter may trigger a formal investigation and could result in disciplinary measures.”*
* **Issue:** Creating urgency and fear is a classic phishing tactic to compel quick action without scrutiny.

**False Sense of Security**

* **Wording:** *“verify their authenticity through the secure link below”*
* **Issue:** The message tries to create a false sense of legitimacy by mentioning a "secure link," which is not verifiable from the email.

**Mismatch Between Message and Branding**

* **Claimed Organization:** Contoso Corp
* **Issue:** No branding elements (logo, color scheme, standard email signature) are present. Legitimate corporate communication usually includes official branding.

**Generic Salutation**

* **Greeting:** *“Hi John,”*
* **Issue:** Although it uses a name, phishing emails often use generic or publicly scraped information. More personalized internal audits would typically include employee ID or reference number.

**Inconsistency in Email Tone and Style**

* **Style:** Unprofessional formatting and language for a serious issue like fraud.
* **Issue:** Real internal audit communication is more formal, with clear documentation references and contact procedures.