# Task 6: Evaluate Generated Emails

Goal: Assess the quality and risk level of AI-generated phishing emails.

## Evaluation Criteria

1. Realism – Does it resemble a legitimate email in tone, formatting, and language?  
2. Persuasiveness – How convincing is the phishing content (urgency, call to action)?  
3. Category Matching – Does it align with known phishing types (banking, job scam, etc.)?  
4. Linguistic Quality – Grammar, spelling, and fluency of content.  
5. Phishing Indicators – Are there signs like suspicious links, urgent tone, or spoofed domains?

## Sample Evaluation Table

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Email ID | Category | Realism | Persuasiveness | Indicators Found | Risk Score (1–5) |
| #1 | Banking Phish | High | High | Suspicious URL, urgency | 5 |
| #2 | Job Scam | Medium | Medium | Vague company name | 3 |
| #3 | Tech Support Scam | High | High | Phone number, fake domain | 5 |