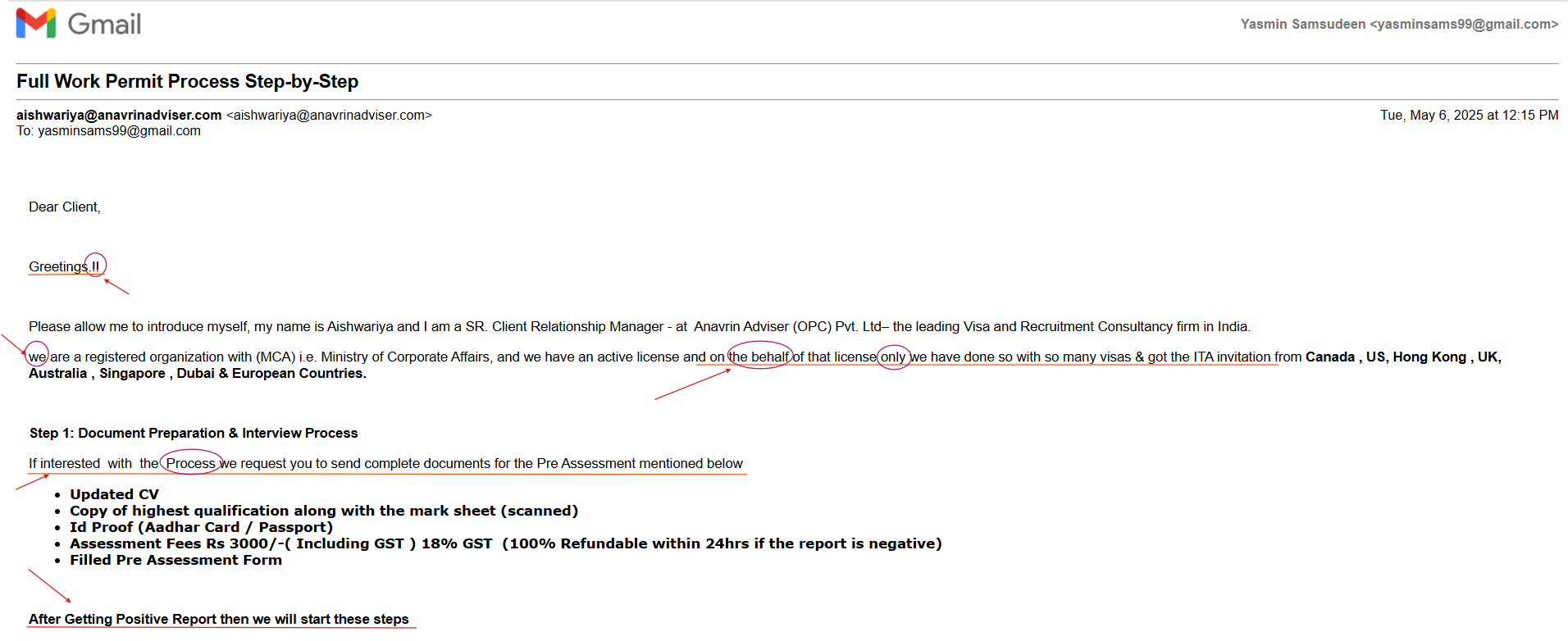
**Task-2 Analyzing a Phishing Email Sample**

**Analyzing a suspicious email**

There are so many grammatical and punctuation errors in the above email that indicate a strong red flag for phishing.

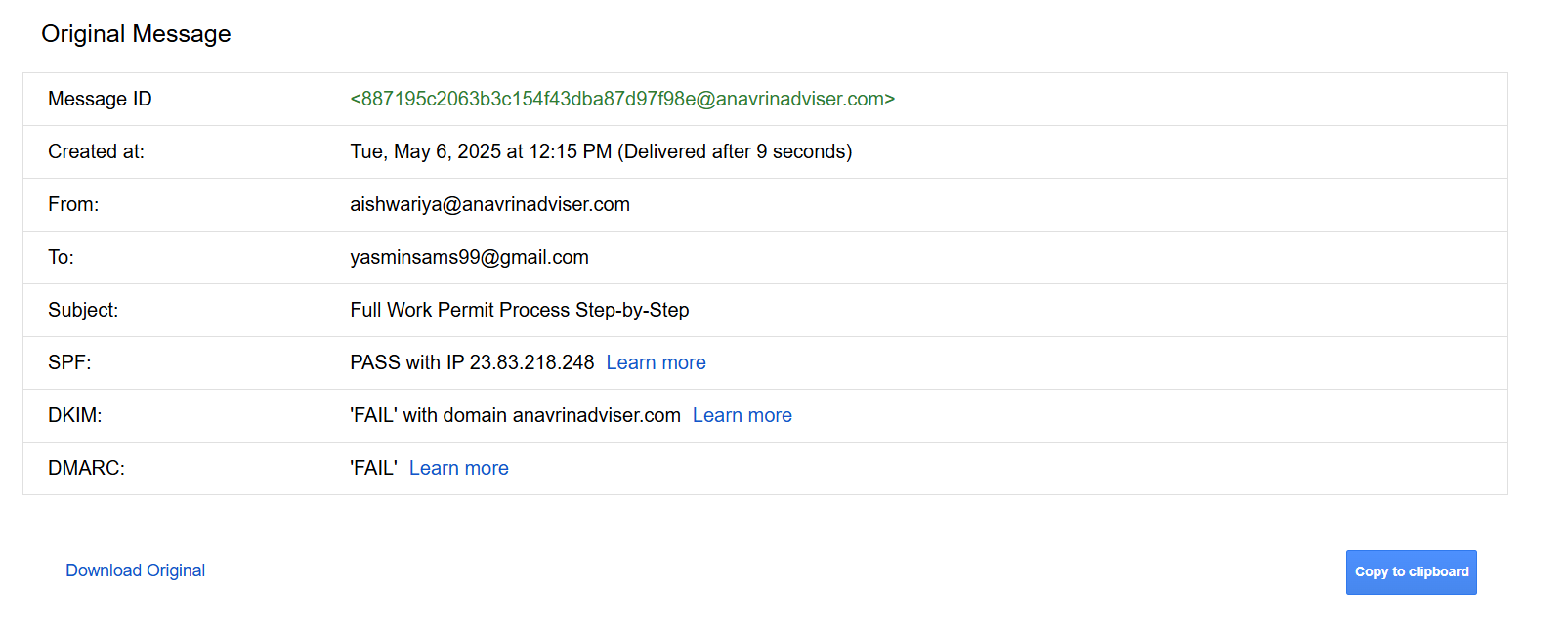
****

**Analyzing the email headers**

While analyzing the header, the sender address and Return-Path are same and have no discrepancies.

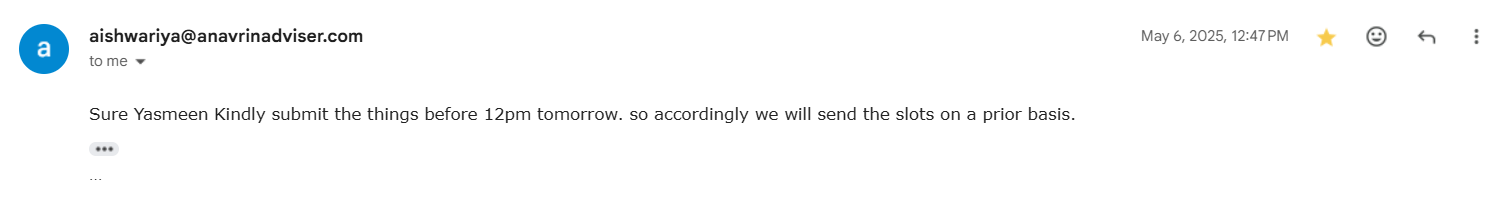


After clicking on the original message from the three dots on the right side of this email, it is found that the ***DKIM*** and ***DMARC*** show ***“FAIL”*** message which is a strong indication for a phishing or spoofing attempt.

****

**Follow-up email**

There is a sense of urgency in the follow-up email again with spelling and punctuation errors.

****

**Phishing traits found in this email:**

1. **Grammatical and punctuation error:** Professional organizations usually maintain a ***high standard*** for ***written communication***. Therefore, ***errors*** in ***grammar*** and ***punctuation*** indicate that the email sent is highly suspicious and has a high chance of being a phishing email.
2. **Psychological Manipulation:** In the current IT market, it is hard to land on interviews even for an experienced person. However, this email poses a “too good to be true” offer of sending people to several countries with ***Visa*** sponsorship. This offer is questionable as there is a certain amount to be paid for the process which again raises suspicions.
3. **Sense of urgency:** The phishing email usually creates a sense of ***urgency***, ***importance*** or ***curiosity*** to entice recipients to open the email, click any ***malicious links*** or ***act immediately*** in this case. As the subject includes topics like ***work permits***, they directly appeal to individuals seeking employment or legal status.
4. **DMARC and DKIM Authentication Failures:**

* The email clearly states ***DKIM: 'FAIL'*** and ***DMARC: 'FAIL'***. Despite an ***SPF: PASS***, these failures are critical. DKIM verifies the email's integrity and sender's authorization via a digital signature, while DMARC dictates actions based on SPF/DKIM alignment. A legitimate sender with proper email authentication configured would almost always pass all three checks.
* The failure of DKIM suggests the email content was either tampered with after being sent by the legitimate server, or it was outright forged and could not be correctly signed by the purported sender. DMARC's failure reinforces that this email does not align with the security policies set by anavrinadviser.com, making it highly suspicious.

**Points to Remember:**

* Always check email headers for SPF, DKIM, and DMARC results
* Be highly suspicious of emails demanding immediate action, threatening consequences, or containing obvious grammatical and punctuation mistakes
* Never click links or open attachments from unknown or suspicious senders. Always hover over links to verify the true destination URL before clicking
* If an email seems suspicious, do not reply or use provided contact info. Instead, directly visit the official website of the organization or use known, legitimate contact details
* Use your email provider's "Report Phishing" function for suspicious emails. This helps protect you and others by improving spam filters