

Email 3 Analysis Report :

The screenshot shows a Gmail inbox with the following details:

- Compose** button.
- Inbox** selected, with 3 new messages.
- Starred**, **Snoozed**, **Sent**, **Drafts**, **All Mail**, **Purchases**, and **More** buttons.
- Labels** section with a plus sign.
- Search mail** bar.
- Subject : Job Offer – Immediate Joining** (Inbox)
- to me** (dropdown)
- 18:45 (6 minutes ago)**
- Dear Applicant,**
- From: hr@amaz0n-careers.com**
- ⚠️ Congratulations....!**
- You have been shortlisted for the position of Remote Customer Support Executive.**
- Please download the attached offer letter and submit your ID proof along with your bank details for salary processing.**
- Complete the formalities within 24 hours to avoid cancellation of your offer.**
- Regards,
HR Team**
- Reply**, **Forward**, and **Smileys** buttons.

1. Subject Line :

⚠️ Job Offer – Immediate Joining ⚠️

⚠️ Creates urgency and opportunity.

2. Sender Email : hr@amaz0n-careers.com

Domain careers.com is not official.

Notice the word : **amaz0n** (zero instead of letter “o”).

This is called **domain spoofing**.

Real Amazon domain : amazon.com

3. Greeting:

Dear Applicant

Generic greeting i.e, Refers to da friendly wave

Legitimate companies use your real name.

4. Attachment Request:

The email asks to download an offer letter and send ID proof.

High risk of Phishing.

Attachments may contain malware.

Requesting ID proof is a data theft attempt.

5. Psychological Tactics Used:

- Career opportunity
- Urgency
- Trust in known brand name

6. Risk Classification : !!PHISHING – HIGH RISK !!

7. Simple Explanation:

This email impersonates Amazon using a fake domain. It tries to steal personal documents or install malware through attachments.