Phishing Email Analysis

1. Obtain a Sample Phishing Email

- ✔ You've provided a complete sample with headers and content.

2. Examine Sender's Email Address for Spoofing

- **From:** kinaxis+autoreply@talent.icims.com
- **Reply-To:** Same as sender
- This looks **legitimate**, as icims.com is a known HR platform used by many companies (including Kinaxis).
- No spoofing detected from just the address.

3. Check Email Headers for Discrepancies

Key Header Findings:

Field	**Value**
Received:	from icims-talentplatform-166162.email.icims.tools (162.247.166.162)
Received-SPF:	pass (SPF verified)
Client IP:	162.247.166.162
Message-ID:	@ip-10-47-163-96.ec2.internal (internal AWS IP)

Analysis:

- IP 162.247.166.162 resolves to **iCIMS**, a trusted HR software vendor.
- SPF check passed → Google verified the domain is authorized to send on behalf of icims.com.
- Email routed through AWS (common for enterprise software).
- No header spoofing or malicious relay detected.

4. Identify Suspicious Links or Attachments

- No file attachments.

- **Embedded links (Base64 decoded)**:
    - https://tracking.icims.com/f/a/... → **a standard tracking link used by iCIMS**
    - https://www.kinaxis.com/sites/default/files/... → links to Kinaxis's official website
    - https://kinaxis.icims.com/icims2/?r=AAE... → personalized candidate portal

Analysis:

- All links are from trusted domains: icims.com, kinaxis.com
- No signs of redirection, shortened URLs, or mismatches
- Clean links

5. Look for Urgent or Threatening Language

- Language used:
    - "Thank you for your interest..."
    - "We want to be as transparent..."
    - "Here's what's next..."
- **No urgency or threats detected**
- Professional and informational tone

6. Note Any Mismatched URLs

- No mismatched or misleading URLs.
- Hover text (if viewed in HTML email) would match destination link.
- No obfuscation or redirect

7. Verify Presence of Spelling or Grammar Errors

- Example text:
    - "We understand that applying for a job can be very exciting but also challenging..."
    - "Here's what's next..."

- Language is grammatically correct and professional.

Final Conclusion:

This **does NOT appear to be a phishing email**.

Signs of Legitimacy:

- Proper SPF, domain alignment
- Recognized sender (icims.com)
- Clean headers and sending IP
- No threats, errors, or suspicious links
- Consistent branding (Kinaxis & iCIMS)