Task 2 Report: Phishing Email Analysis

Objective:

To analyze a potentially suspicious domain (fresherjobsz.com) and identify phishing characteristics using email header and DNS inspection.

Tool Used:

- MXToolbox SuperTool (https://mxtoolbox.com)

Analysis Summary:

- Domain Analyzed: fresherjobsz.com
- Mail Servers:
  - mx10.antispam.mailbamp.com
  - mx20.antispam.mailbamp.com
  - mx30.antispam.mailbamp.com
- IPs belong to Google Cloud (used for email routing).

Key Findings:

1. DMARC Policy Not Enabled - This makes the domain vulnerable to spoofing, allowing attackers to send forged emails.
2. DNS and DMARC Records Found - While records are published, policy enforcement is lacking.
3. SPF and MX Records Exist - These are correctly configured.

Conclusion:

The domain has basic DNS protection, but the lack of a strict DMARC policy significantly weakens

its defense against phishing and spoofing attacks. This is a potential security issue and should be addressed by domain administrators.

Evidence: