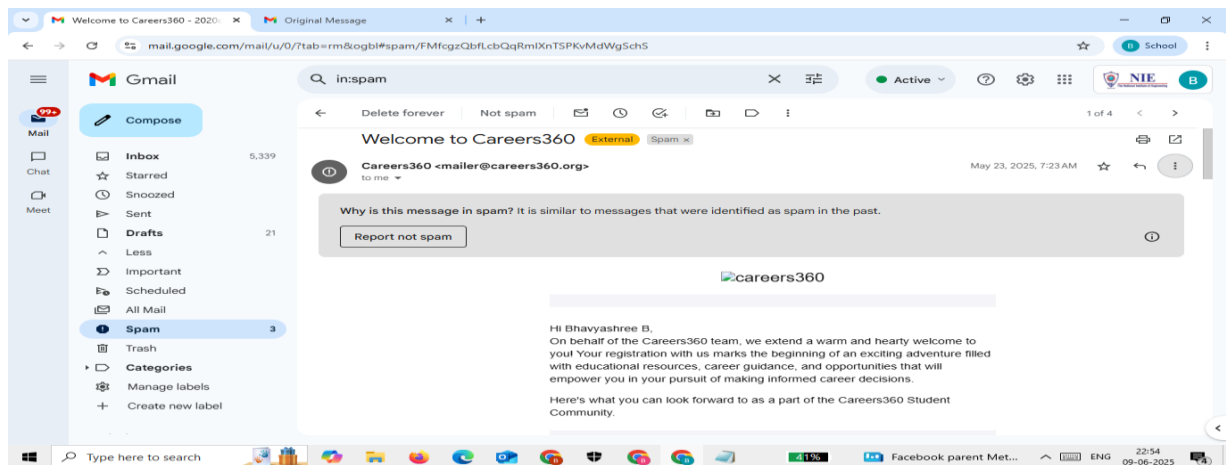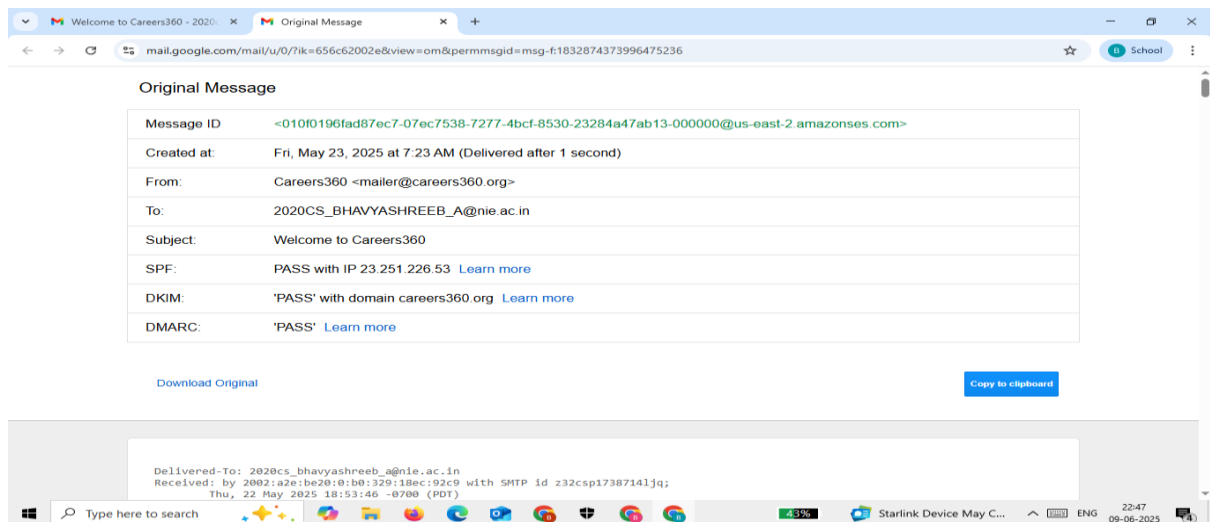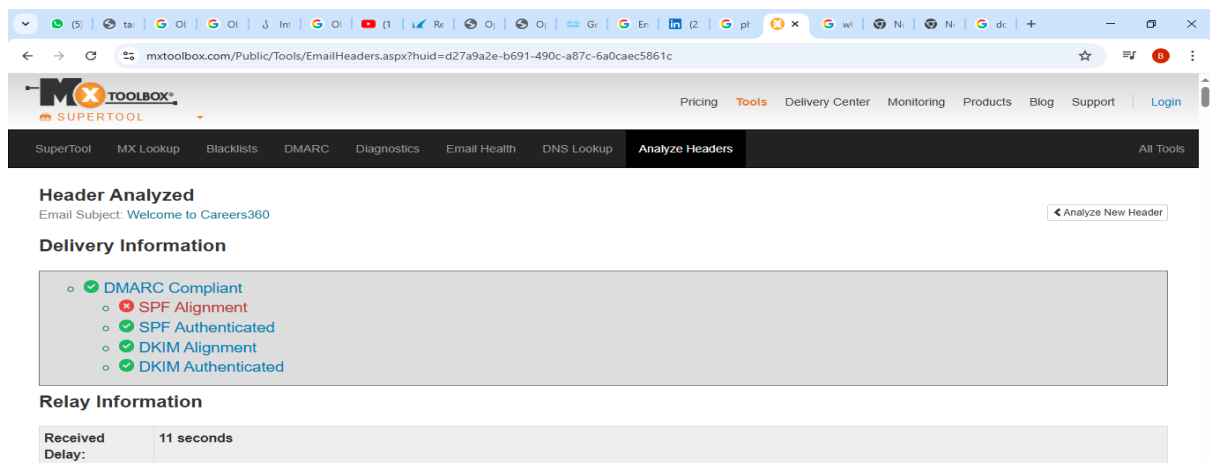# 1.Obtain a sample phishing email.

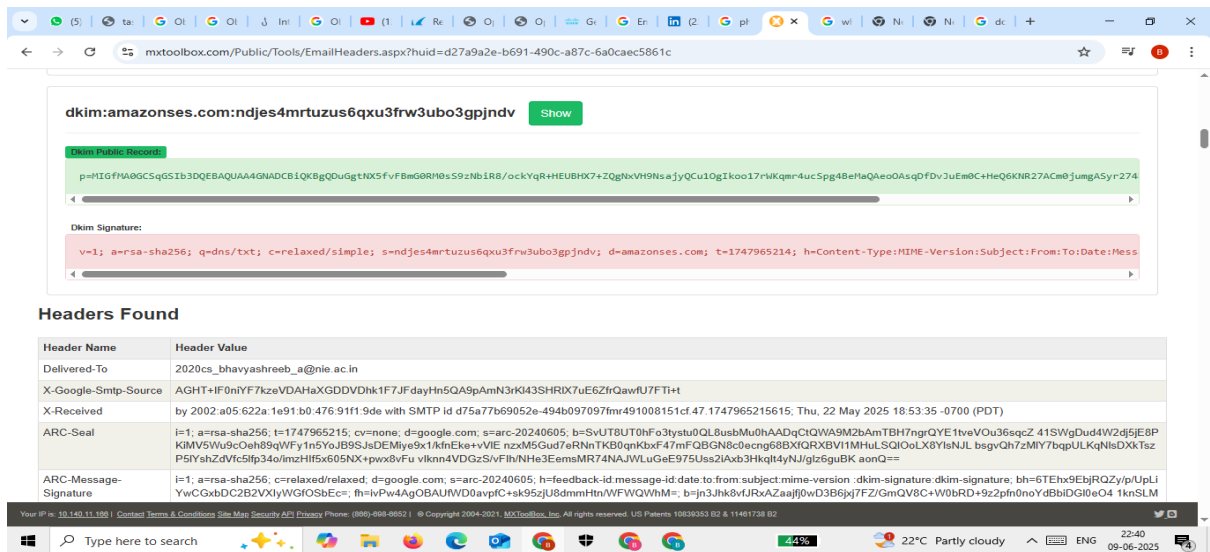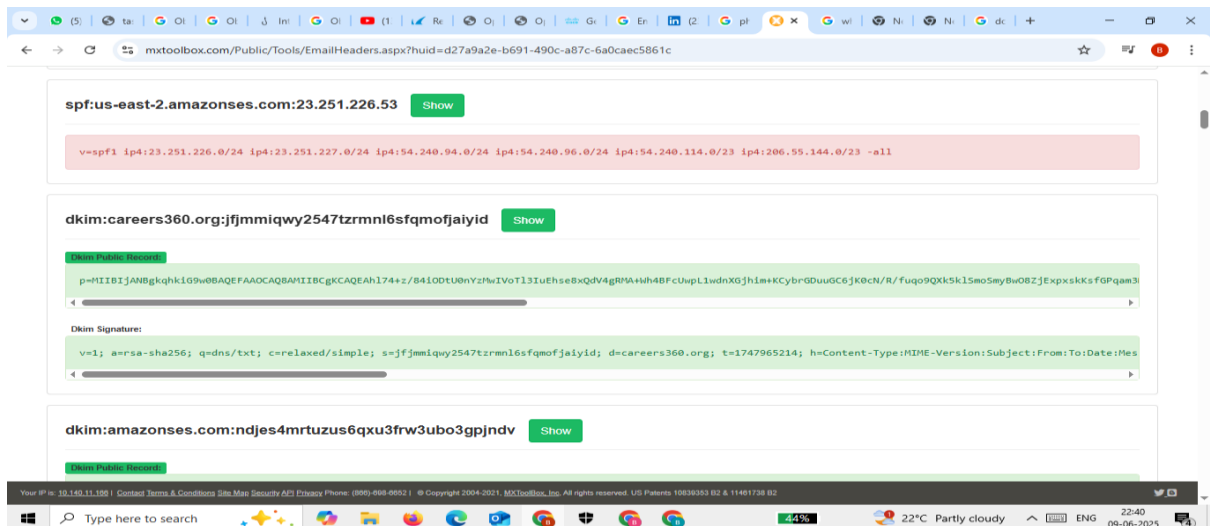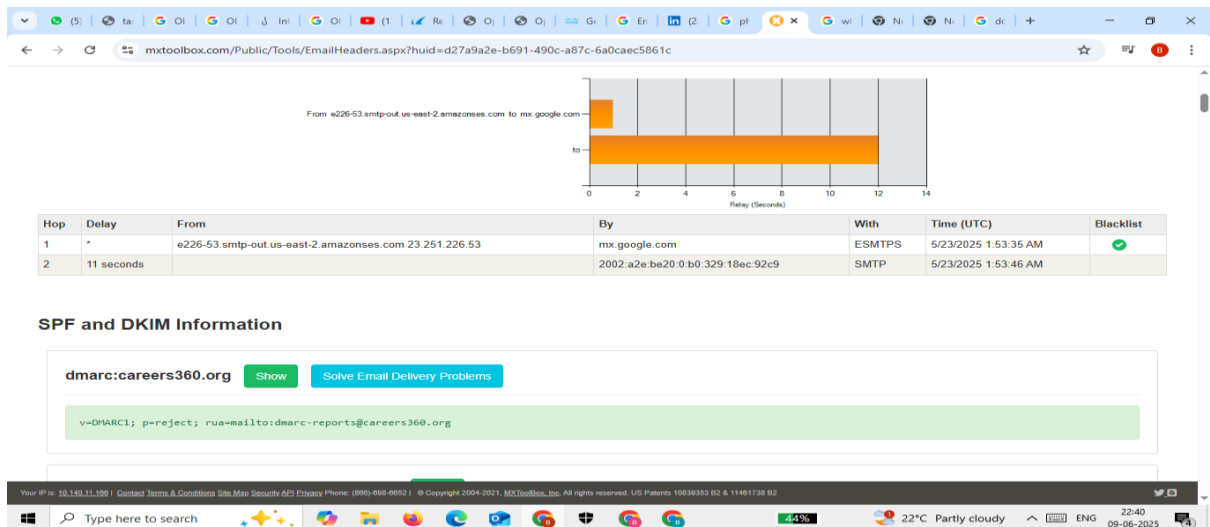
2.Examine sender's email address for spoofing.

3.Check email headers for discrepancies (using online header analyzer).

From e226-53.smtp-out.us-east-2.amazonses.com to mx.google.com

to

Relay (Seconds)

Hop	Delay	From	By	With	Time (UTC)	Blacklist
1	*	e226-53.smtp-out.us-east-2.amazonses.com 23.251.226.53	mx.google.com	ESMTPS	5/23/2025 1:53:35 AM	✓
2	11 seconds		2002:a2e:be20:0:b0:329:18ec:92c9	SMTP	5/23/2025 1:53:46 AM	

SPF and DKIM Information

dmarc:careers360.org [Show] [Solve Email Delivery Problems]

v=DMARC1; p=reject; rua=mailto:dmarc-reports@careers360.org

---

spf:us-east-2.amazonses.com:23.251.226.53 [Show]

v=spf1 ip4:23.251.226.0/24 ip4:23.251.227.0/24 ip4:54.240.94.0/24 ip4:54.240.96.0/24 ip4:54.240.114.0/23 ip4:206.55.144.0/23 -all

dkim:careers360.org:jfjmmiqwy2547tzrmnl6sfqmofjaiyid [Show]

Dkim Public Record:

p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAh174+z/84iODtU0nYzMwIVoTl3IuEhse8xQdV4gRMA+Wh4BFcUwpL1wdnXGjhim+KCybrGDuuGC6jK0cN/R/fuqo9QXk5kl5mo5myBwO8ZjExpxskKsfGPqam3i

Dkim Signature:

v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=jfjmmiqwy2547tzrmnl6sfqmofjaiyid; d=careers360.org; t=1747965214; h=Content-Type:MIME-Version:Subject:From:To:Date:Mes

dkim:amazonses.com:ndjes4mrtuzus6qxu3frw3ubo3gpjndv [Show]

Dkim Public Record:

---

dkim:amazonses.com:ndjes4mrtuzus6qxu3frw3ubo3gpjndv [Show]

Dkim Public Record:

p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDuGgtNX5fvFBmG0RM0sS9zNbiR8/ockYqR+HEUBHX7+ZQgNxVH9NsajyQCu1OgIkoo17rWKqmr4ucSpg4BeMaQAeoOAsqDfDvJuEm0C+HeQ6KNR27ACm0jumgASyr274

Dkim Signature:

v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; s=ndjes4mrtuzus6qxu3frw3ubo3gpjndv; d=amazonses.com; t=1747965214; h=Content-Type:MIME-Version:Subject:From:To:Date:Mess

Headers Found

Header Name	Header Value
Delivered-To	2020cs_bhavyashreeb_a@nie.ac.in
X-Google-Smtp-Source	AGHT+IF0niYF7kzeVDAHaXGDDVDhk1F7JFdayHn5QA9pAmN3rKI43SHRIX7uE6ZfrQawfU7FTi+t
X-Received	by 2002:a05:622a:1e91:b0:476:91f1:9de with SMTP id d75a77b69052e-494b097097fmr491008151cf.47.1747965215615; Thu, 22 May 2025 18:53:35 -0700 (PDT)
ARC-Seal	i=1; a=rsa-sha256; t=1747965215; cv=none; d=google.com; s=arc-20240605; b=SvUT8UT0hFo3tystu0QL8usbMu0hAADqCtQWA9M2bAmTBH7ngrQYE1tveVOu36sqcZ 41SWgDud4W2dj5jE8P KiMV5Wu9cOeh89qWFy1n5YoJB9SJsDEMiye9x1/kfnEke+vVIE nzxM5Gud7eRNnTKB0qnKbxF47mFQBGN8c0ecng68BXfQRXBVI1MHuLSQIOoLX8YIsNJL bsgvQh7zMlY7bqpULKqNlsDXkTsz P5lYshZdVfc5lfp34o/imzHlf5x605NX+pwx8vFu vIknn4VDGzS/vFih/NHe3EemsMR74NAJWLuGeE975Uss2iAxb3HkqIt4yNJ/glz6guBK aonQ==
ARC-Message-Signature	i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20240605; h=feedback-id:message-id:date:to:from:subject:mime-version :dkim-signature:dkim-signature; bh=6TEhx9EbjRQZy/p/UpLi YwCGxbDC2B2VXIyWGfOSbEc=; fh=ivPw4AgOBAUfWD0avpfC+sk95zjU8dmmHtn/WFWQWhM=; b=jn3Jhk8vfJRxAZaajfj0wD3B6jxj7FZ/GmQV8C+W0bRD+9z2pfn0noYdBbiDGl0eO4 1knSLM

4.Identify suspicious links or attachments

There are no suspicious links or attachments in his mail.

5.Look for urgent or threatening language in the email body.

There is no threatening language like "urgent action required" or "your account will be terminated", They are red flags that indicate a potential phishing attempt

6.Note any mismatched URLs (hover to see real link).

This email does not have a link where the displayed text or shortened URL differs from the actual destination, which is a sign of potential security risk. This happens when the link uses a redirect or a URL shortener, obscuring the real destination behind a seemingly legitimate link.

7.Verify presence of spelling or grammar errors.

The email contains 32 grammer suggestion and got 68 out of 100 writing score.

8.Summarize phishing traits found in the email.

The email likely failed SPF alignment because the email's sender IP address wasn't authorized in the domain's SPF record. Additionally, the email has 32 grammar mistakes, which need to be corrected for clarity and professional presentation.