Task 2

1. Let's start by obtaining ourselves a sample phishing email (search online for free phishing email samples and it will list you many websites that provide them for free just like in fig1.

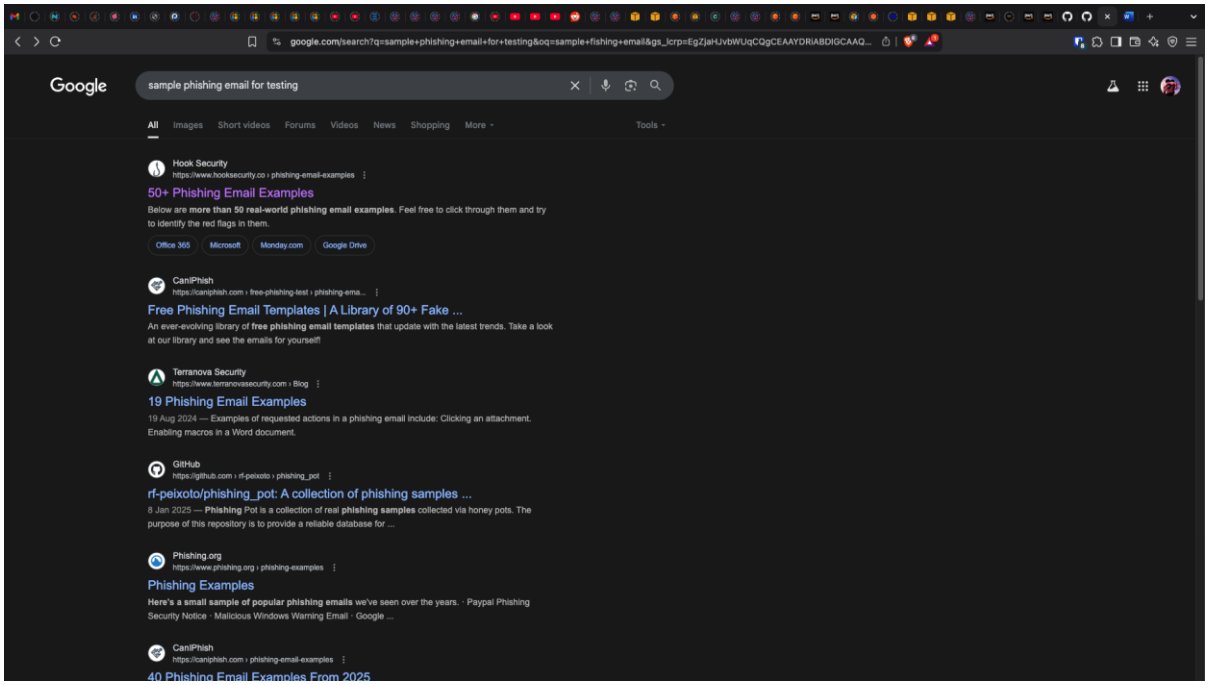

Fig1

2. Let's go with support@micr0soft-support.com for our example provided by the first link of our google search.
3. This was the email provided by the website:

From: support@micr0soft-support.com

Subject: Urgent: Your Microsoft Account Will Be Locked!

Dear User,

We have detected suspicious activity on your Microsoft account. To protect your information, we will temporarily lock your account if you do not verify it within 24 hours.

Please click the link below to verify your account:

https://microsoftsupport.verify-now.com

Failure to act now may lead to permanent account suspension.

Thank you, Microsoft Account Security Team

Attachment: SecurityUpdate.zip

4. Now with the first look this does not look phishy at all but when we examine the sender's email address closely we find that the email address is not right as it contains a '0' instead of 'o'. This means this is a spoofed domain attempting to impersonate Microsoft.
5. Now since we didn't actually receive an email we cannot check for headers directly but we do have a sample header file attached with the sample mail so lest check it instead. The sample header is:

Return-Path: <support@micr0soft-support.com>
Received: from unknown123.isp.fake ([192.0.2.55])
by mail.example.com with ESMTP;
Mon, 27 May 2025 10:00:00 +0000
Message-ID: <20250527100000.12345@mail.example.com>
Subject: Urgent: Your Microsoft Account Will Be Locked!
From: Microsoft Support <support@micr0soft-support.com>
To: victim@example.com
Content-Type: text/html; charset="UTF-8"
Date: Mon, 27 May 2025 10:00:00 +0000
DKIM-Signature: none
Authentication-Results: spf=fail smtp.mailfrom=micr0soft-support.com

6. **Now let's understand the header file through an online header analyzer (the one I used is " https://mxtoolbox.com/EmailHeaders.aspx ") which will automate the analyzing process for us and seperate out all the important stuff from the useless stuff. The output of the header file is in fig2.**

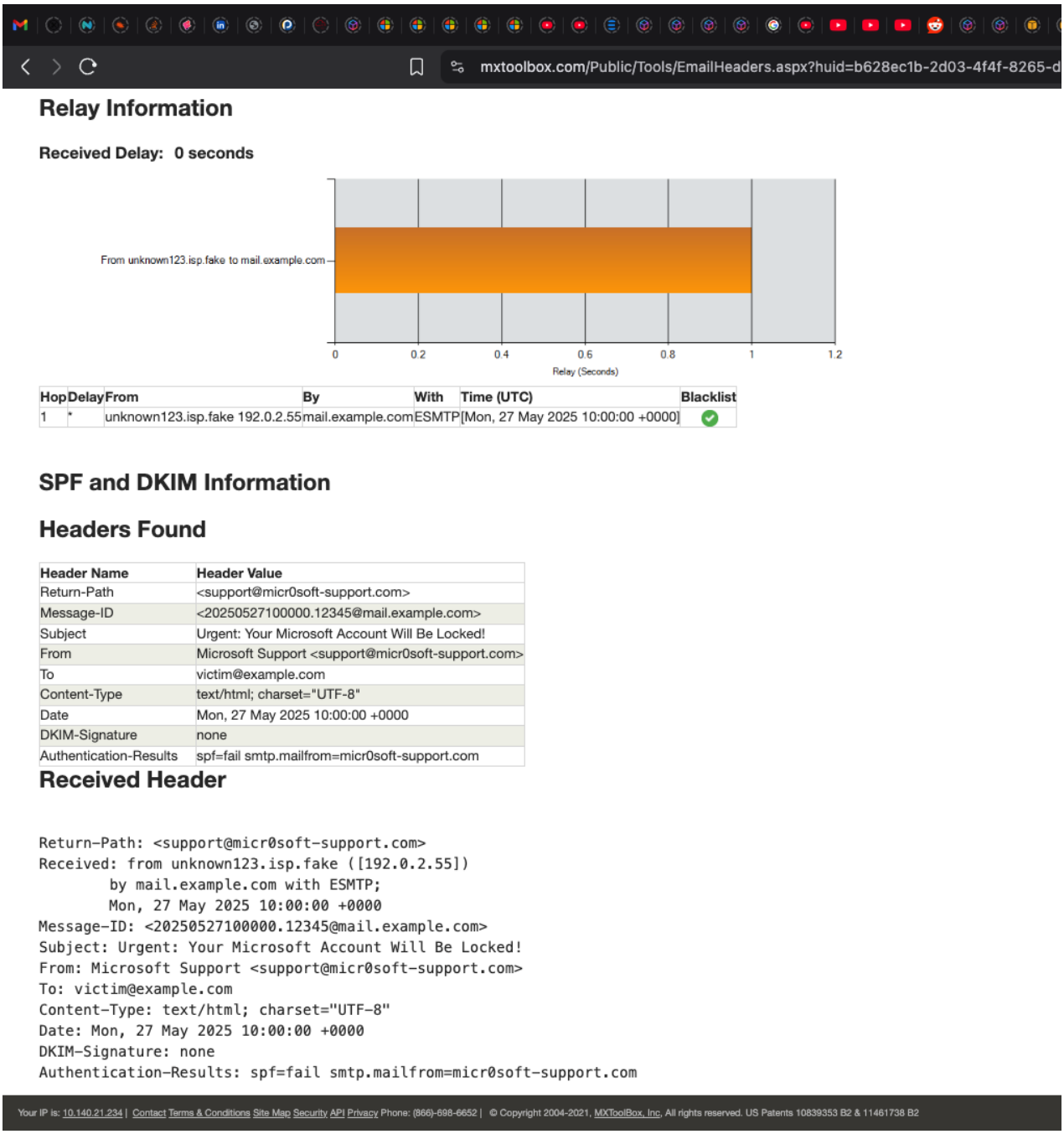

Fig2

7. **From this output we can infer:**
   - Domain has a zero “0” in “micr0soft” which means it is spoofed
   - IP 192.0.2.55 is not a known Microsoft server (see fig3 for detail)

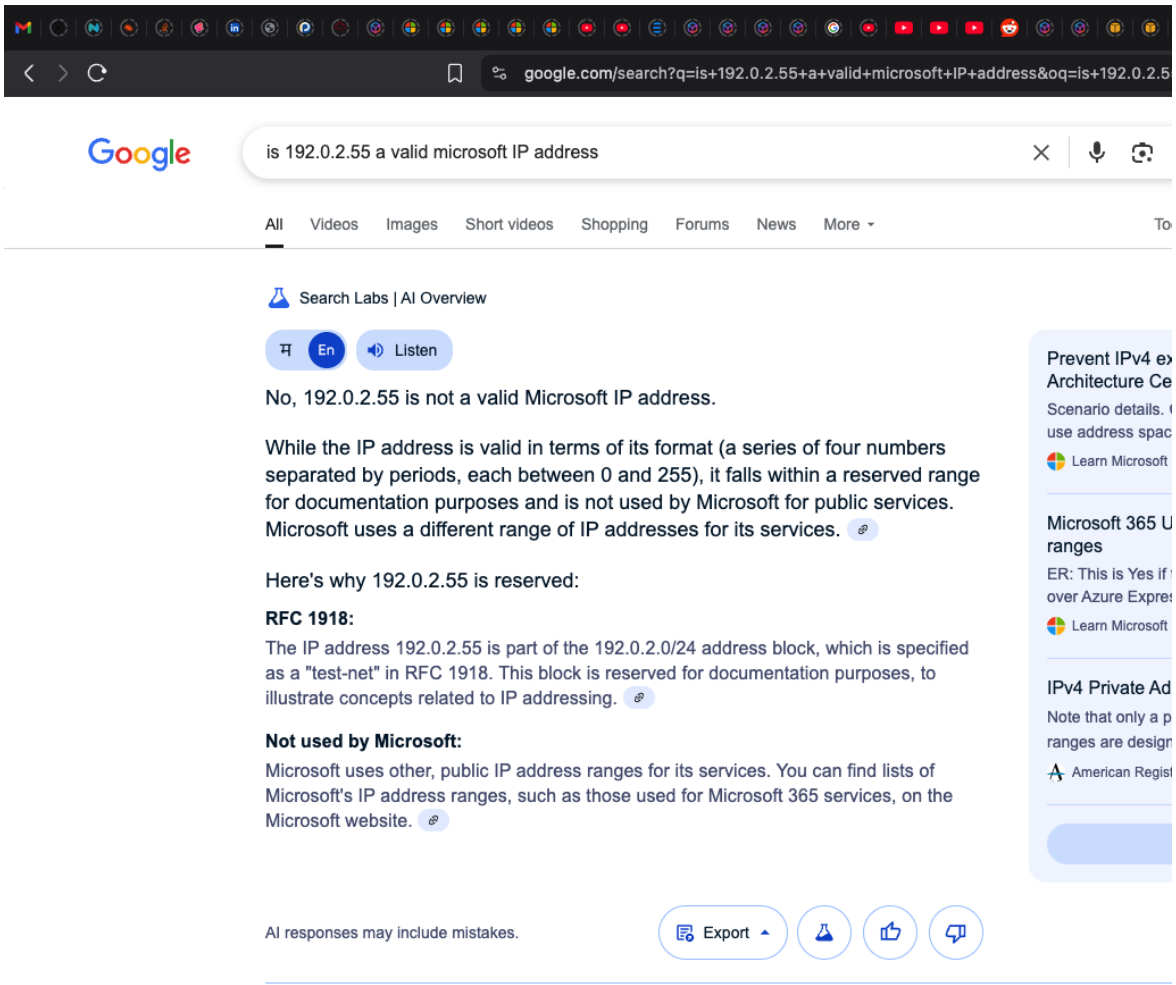

Fig3

- **SPF failure we get it from the last line of the header file**
  Authentication-Results: spf=fail smtp.mailfrom=micr0soft-support.com
  which means the sender that sent this email is not authorized to send emails from the domain its claiming to be
- **No DKIM signature meaning the email is not authorized by the service provider**
  A DKIM signature for context is a kind of digital signature provided by the sender's mail engine which uses a already built up record from the DNS server
- **The headers received are from a fake relay server**

8. **Now in our case we don't have the actual attachment of a phishing email, but we can still tell that it's probably fake since why a verification email from microsoft have a zip file attached to it.**
   Always think before you download anything from an email that's the best practice to avoid getting phished.

9. **Now lets check the link sent to us in the email to verify ourselves.**
   Note : never click on the links provided in an email directly always check whether the link is correct or not by searching the link attached in google or chatgpt and asking it is real or not . Lets check wheather the email attached in the phishing mail was real or not?
   The output is in fig4.

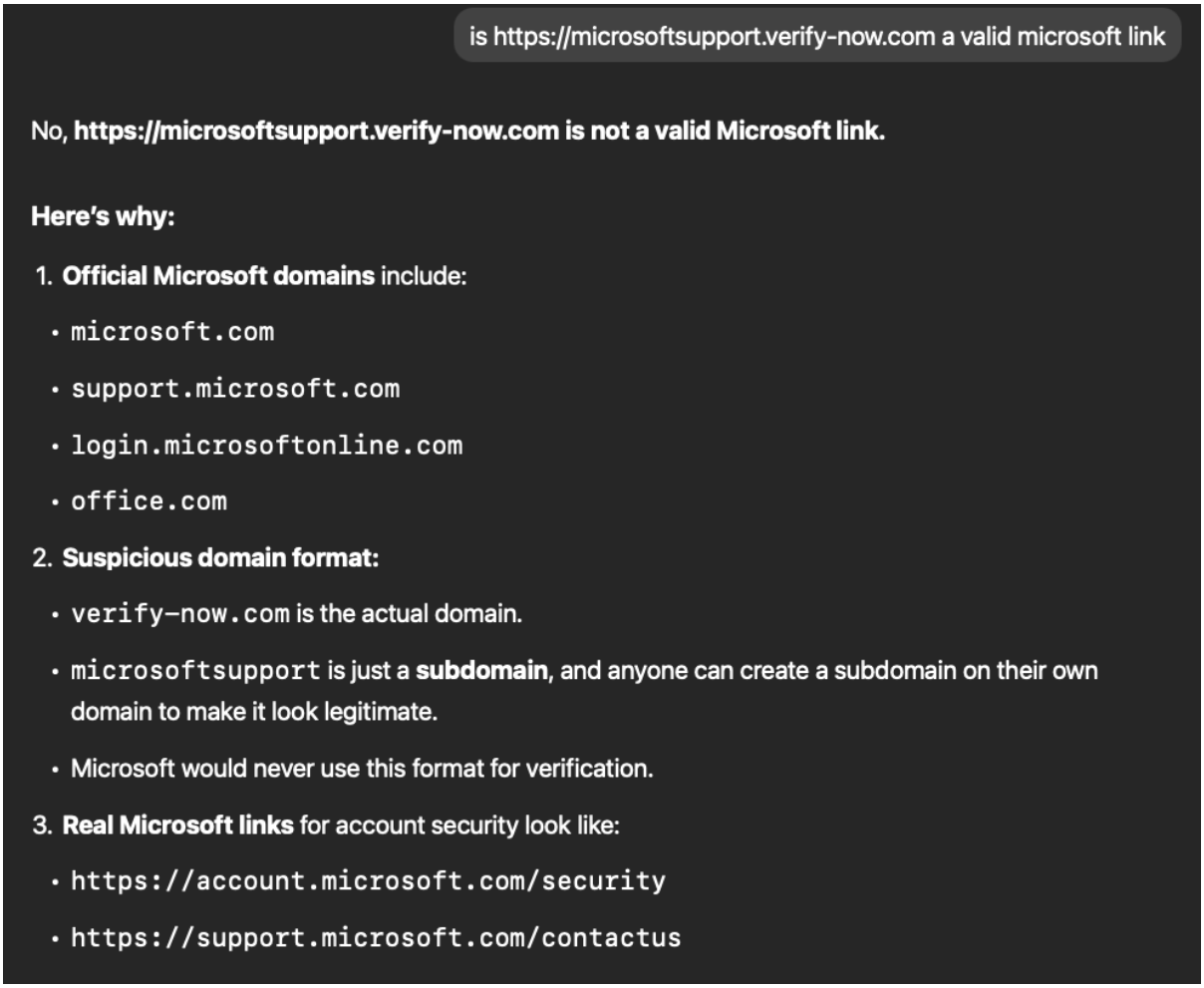

Fig4

   As you can see the link is not a legit one.

10. **Now to summarize the whole email spoofing check let's put it in a table format for it to be easy to understand.**

Phishing Trait	Observed
Spoofed sender address	✅
Fake/mismatched URL	✅
Urgency/threat	✅
Suspicious attachment	✅
Grammar/spelling issues	✅
Failed email headers check	✅

11. Now with the information we have gathered it's pretty clear the email was a phishing one.