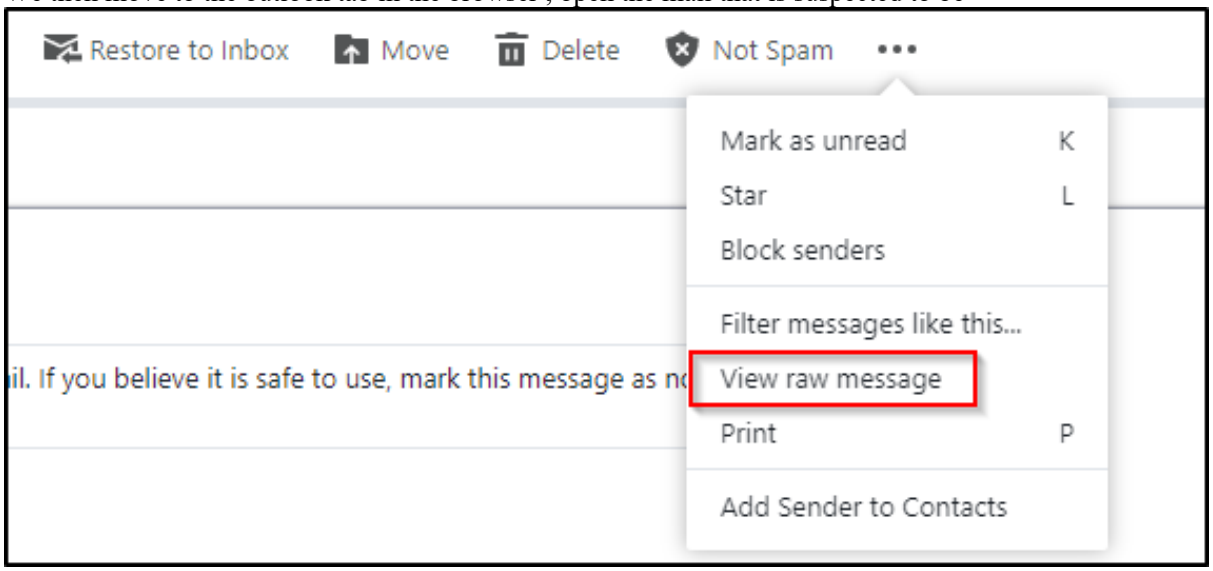
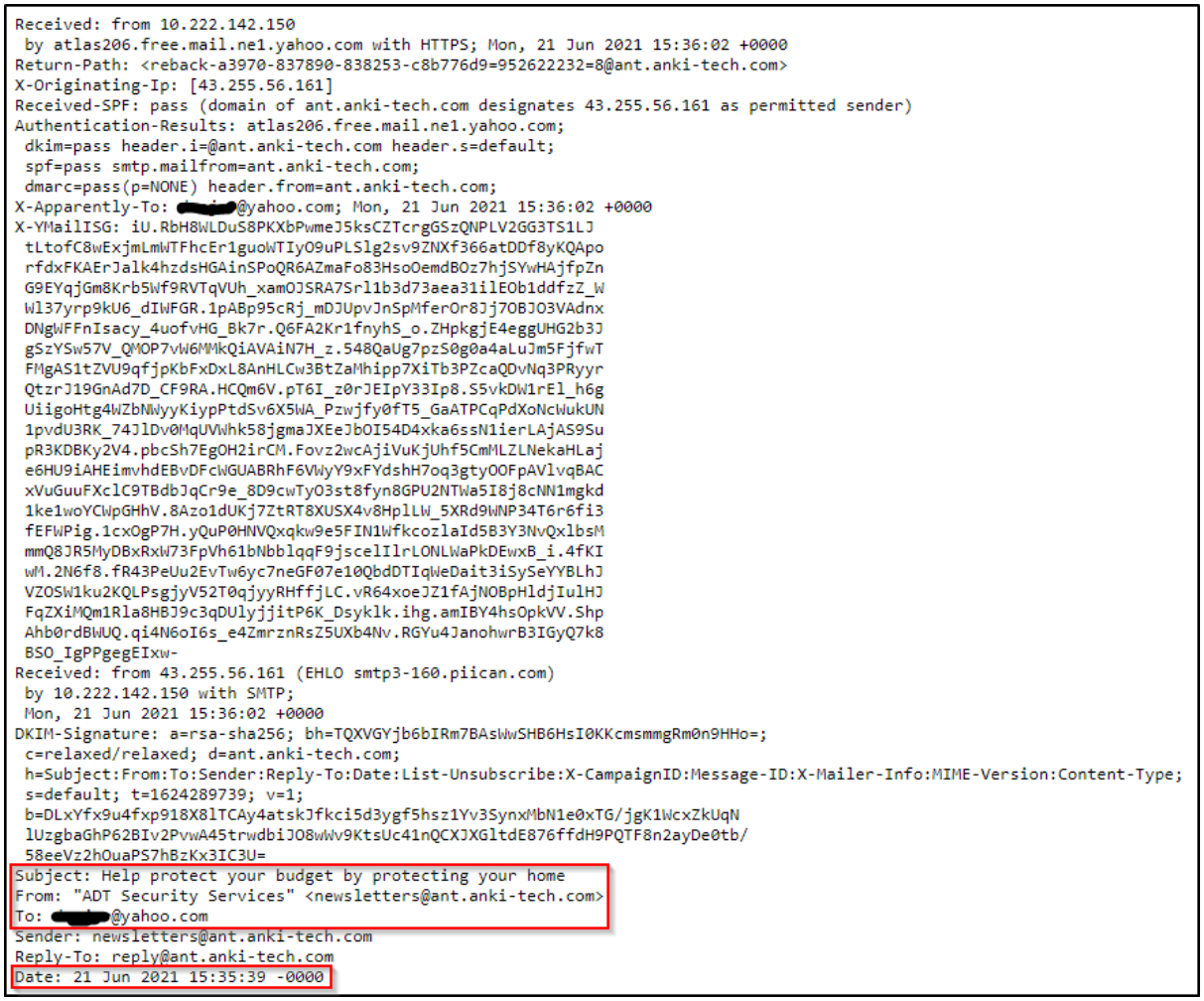
Elevate Labs Internship Task 2

Objective: Identify phishing characteristics in a suspicious email sample.

The below photograph is a sample of a phishing email which was forwarded on the mail of a victim. The victim's mail was actually honeypot mail which was designed to catch the phishing email red handed .

We then move to the outlook tab in the browser , open the mail that is suspected to be





```
Received: from 10.222.142.150
 by atlas206.free.mail.ne1.yahoo.com with HTTPS; Mon, 21 Jun 2021 15:36:02 +0000
Return-Path: <reback-a3970-837890-838253-c8b776d9=952622232=8@ant.anki-tech.com>
X-Originating-Ip: [43.255.56.161]
Received-SPF: pass (domain of ant.anki-tech.com designates 43.255.56.161 as permitted sender)
Authentication-Results: atlas206.free.mail.ne1.yahoo.com;
 dkim=pass header.i=@ant.anki-tech.com header.s=default;
 spf=pass smtp.mailfrom=ant.anki-tech.com;
 dmarc=pass(p=NONE) header.from=ant.anki-tech.com;
X-Apparently-To: [redacted]@yahoo.com; Mon, 21 Jun 2021 15:36:02 +0000
X-YMailISG: iU.RbH8WLDuS8PKXbPwmeJ5ksCZTcrgGSzQNPLV2GG3TS1LJ
 tLtofC8wExjmLmWTFhcEr1guoWTIyO9uPLSlg2sv9ZNXf366atDDf8yKQApo
 rfdxFKAErJalk4hzdsHGAinSPoQR6AZmaFo83HsoOemdBOz7hjSYwHAjfpZn
 G9EYqjGm8Krb5Wf9RVTqVUh_xamOJSRA7Srl1b3d73aea31ilEOb1ddfzZ_W
 Wl37yrp9kU6_dIWFGR.1pABp95cRj_mDJUpvJnSpMferOr8Jj7OBJO3VAdnx
 DNgWFFnIsacy_4uofvHG_Bk7r.Q6FA2Kr1fnyhS_o.ZHpkgjE4eggUHG2b3J
 gSzYSw57V_QMOP7vW6MMkQiAVAiN7H_z.548QaUg7pzS0g0a4aLuJm5FjfwT
 FMgAS1tZVU9qfjpKbFxDxL8AnHLCw3BtZaMhipp7XiTb3PZcaQDvNq3PRyyr
 QtzrJ19GnAd7D_CF9RA.HCQm6V.pT6I_z0rJEIpY33Ip8.S5vkDW1rEl_h6g
 UiigoHtg4WZbNWyyKiypPtdSv6X5WA_Pzwjfy0fT5_GaATPCqPdXoNcWukUN
 1pvdU3RK_74JlDv0MqUVWhk58jgmaJXEeJbOI54D4xka6ssN1ierLAjAS9Su
 pR3KDBKy2V4.pbcSh7EgOH2irCM.Fovz2wcAjiVuKjUhf5CmMLZLNekaHLaj
 e6HU9iAHEimvhdEBvDFcWGUABRhF6VWyY9xFYdshH7oq3gtyOOFpAVlvqBAC
 xVuGuuFXclC9TBdbJqCr9e_8D9cwTyO3st8fyn8GPU2NTWa5I8j8cNN1mgkd
 1ke1woYCWpGHhV.8Azo1dUKj7ZtRT8XUSX4v8HplLW_5XRd9WNP34T6r6fi3
 fEFWPig.1cxOgP7H.yQuP0HNVQxqkw9e5FIN1WfkcozlaId5B3Y3NvQxlbsM
 mmQ8JR5MyDBxRxW73FpVh61bNbblqqF9jscelIlrLONLWaPkDEwxB_i.4fKI
 wM.2N6f8.fR43PeUu2EvTw6yc7neGF07e10QbdDTIqWeDait3iSySeYYBLhJ
 VZOSW1ku2KQLPsgjyV52T0qjyyRHffjLC.vR64xoeJZ1fAjNOBpHldjIulHJ
 FqZXiMQm1Rla8HBJ9c3qDUlyjjitP6K_Dsyklk.ihg.amIBY4hsOpkVV.Shp
 Ahb0rdBWUQ.qi4N6oI6s_e4ZmrznRsZ5UXb4Nv.RGYu4JanohwrB3IGyQ7k8
 BSO_IgPPgegEIxw-
Received: from 43.255.56.161 (EHLO smtp3-160.piican.com)
 by 10.222.142.150 with SMTP;
 Mon, 21 Jun 2021 15:36:02 +0000
DKIM-Signature: a=rsa-sha256; bh=TQXVGYjb6bIRm7BAsWwSHB6HsI0KKcmsmmgRm0n9HHo=;
 c=relaxed/relaxed; d=ant.anki-tech.com;
 h=Subject:From:To:Sender:Reply-To:Date:List-Unsubscribe:X-CampaignID:Message-ID:X-Mailer-Info:MIME-Version:Content-Type;
 s=default; t=1624289739; v=1;
 b=DLxYfx9u4fxp918X8lTCAy4atskJfkci5d3ygf5hsz1Yv3SynxMbN1e0xTG/jgK1WcxZkUqN
 lUzgbaGhP62BIv2PvwA45trwdbiJO8wWv9KtsUc41nQCXJXGltdE876ffdH9PQTF8n2ayDe0tb/
 58eeVz2hOuaPS7hBzKx3IC3U=
Subject: Help protect your budget by protecting your home
From: "ADT Security Services" <newsletters@ant.anki-tech.com>
To: [redacted]@yahoo.com
Sender: newsletters@ant.anki-tech.com
Reply-To: reply@ant.anki-tech.com
Date: 21 Jun 2021 15:35:39 -0000
```

Based on the sample email (email1.eml) and the header fields examined, we identified several classic **phishing traits**:

1. **Suspicious Sender Domain**

   The sender domain ant.anki-tech.com does not match any official or verified organization. This domain is likely spoofed to trick recipients.

2. **Reply-To Mismatch**

   The Reply-To field is reply@ant.anki-tech.com, which differs from the From address. This is commonly used to redirect replies to an attacker-controlled inbox.

3. **X-Originating-IP**

   The IP in the X-Originating-IP header can be traced to a location not associated with the claimed sender. Using tools like iplocation.net, you can identify the geographical mismatch.

4. **Urgent or Manipulative Language**

These emails usually contain language urging the user to “act now”, “verify immediately”, or threatening account suspension.

5. **Generic Greetings**

   Instead of personalized greetings, the email may begin with “Dear Customer” or “User”, a common trait in phishing attempts.

6. **Suspicious Links**

   Hyperlinks (if any) do not lead to the official domain. Always hover to preview the actual destination.

7. **Spelling and Grammar Issues**

   Phishing emails often include subtle grammatical errors or unusual sentence structure, further raising suspicion.

🛠️ Tools Used

- **Outlook Web Client** – To open and view raw email headers.
- **Email Header Analyzer** (MXToolbox) – To identify spoofed or misconfigured header fields.
- **WHOIS/IP Lookup Tools** – To trace domain registration or IP origin.