

## Social Engineering Write-Up

Name: ZAHIDAH AZ-ZAHRA BINTI SAFARIZAM

ID: 52215226218

Platform: TryHackMe

### Exercise: Phishing Analysis Fundamentals

#### 1. Objective

To identify the components involved in sending an email and to understand how to analyze email headers.

#### 2. Tools/Platform Used

- TryHackMe
- CyberChef
- Base64.Guru

#### 3. Steps Taken

1. Identified the email headers and email body.
2. Analyzed key email header fields such as From, Subject, Date, and To.
3. Viewed the raw email content to examine detailed header information.
4. Identified suspicious elements within the email details.
5. Analyzed the email body for attachments and content types.
6. Interacted with attachments by decoding files and defanging URLs.

#### 4. Findings/What I learned

- Learned how to view the raw source of an email, including the header and body.
- Understood the importance of analyzing email content for attachments, encoded data, and other suspicious elements.
- Gained a better understanding of the relationship between the email sender and recipient information.

#### 5. Conclusion

This exercise strengthened my understanding of email structure and phishing analysis techniques. It showed how attackers can also manipulate email elements and emphasized the need to analyse email headers, email content and email attachments attentively to identify phishing attacks.

## 6. Evidence

7.

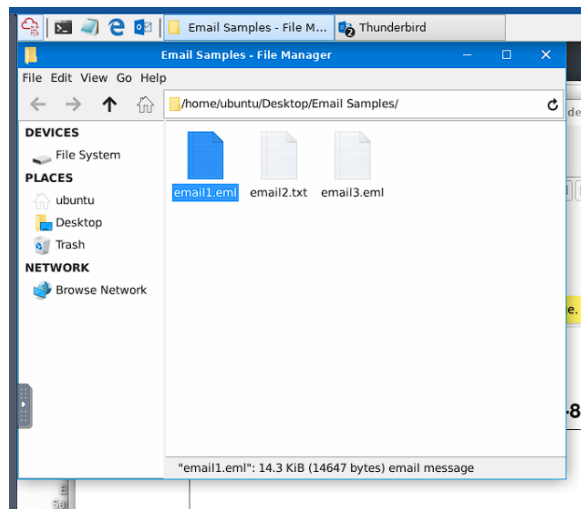


Figure 1: Types of email

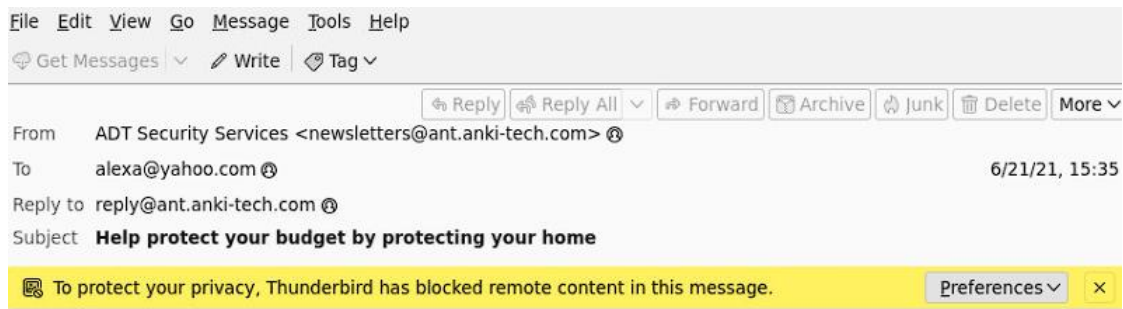


Figure 2: email1.eml

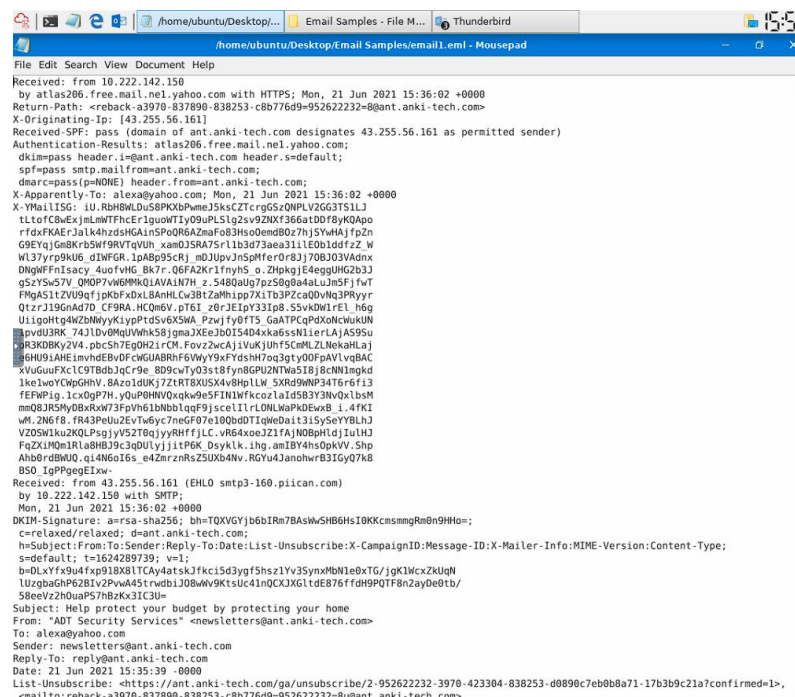


Figure 3: email1.eml raw details

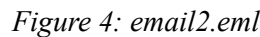


Figure 5: Decode email2.eml .pdf content-type

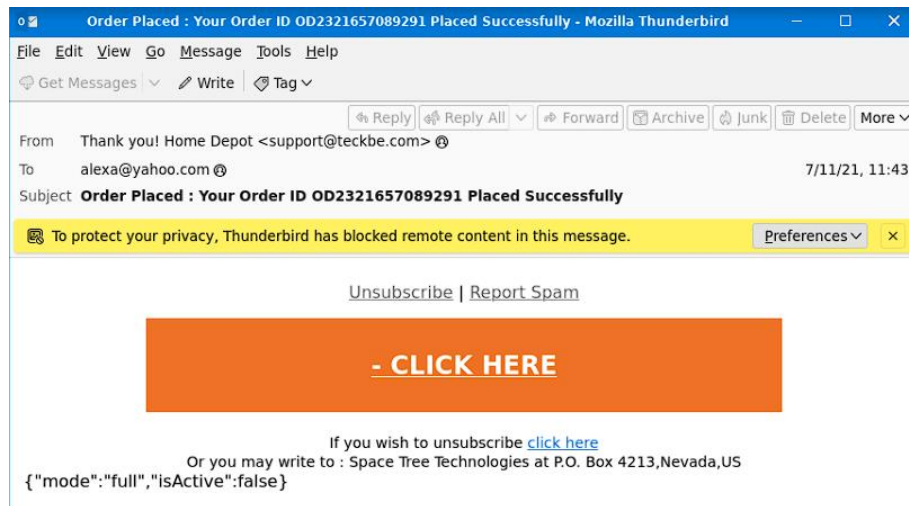


Figure 6: email3.eml

```

/home/ubuntu/Desktop/Email Samples/email3.eml - Mousepad
File Edit Search View Document Help
Received: from 10.253.62.157
  by atlas102.free.mail.gql.yahoo.com with HTTPS; Sun, 11 Jul 2021 11:48:13 +0000
Return-Path: <support@teckbe.com>
X-Originating-Ip: [103.234.236.83]
Received-SPF: pass (domain of teckbe.com designates 103.234.236.83 as permitted sender)
Authentication-Results: atlas102.free.mail.gql.yahoo.com;
  dkim=pass header.i=@teckbe.com header.s=dk2048;
  spf=pass smtp.mailfrom=teckbe.com;
  dmarc=pass(p=NONE) header.from=teckbe.com;
X-Apparently-To: alexa@yahoo.com; Sun, 11 Jul 2021 11:48:13 +0000
X-YMailISG: Pcp93.8WLDsI7m7VAEQNtYkM8dxkhTUX7phGw048do12XbE6
  Gltw2BzR4.Ebk.9AXnvt1nLaw55vIEJkyJo0dGtzUNCsEv4L8wY3dH_YRDa
  IavIwK20Bzfqo6DGTBXvbnKtoFlyNq10|bq.mo.GxL.A.v8Jnun3AEzT3Co
  WUJfU7m7mYoTL3fzJEds6ahURlxPps00v1FolH.GWwlg2p10xQ58ebjz
  P0F22ts66ChyP9mfE7L5.DpFRkKLT4y44wtQzXEP.TBQx1dZBHG7jvXIiW
  o.FK1jsUktrJL.p03zEcVhBMhD8D5lWkrf19y0mxECeNNq5HCpJVPPEcM
  pRw0W0MnetIebnbhyzTV0zh.6Gh172Kd8Ca.Fywpt0MCyW8m7TGwZ01jws3
  FV15WqNGF7g5Wo9peDCSBWg_Jga.QAGUib7edzcb0ICdfbsmkJ78w5DxqyqA
  XyZJIKJ3ZioZt4pLAqWC0Q5CrtJ3TzwyLtoaxvn81bU1NQ.76VBnLEef0sB
  K60eEhu4xnUFSK6Bh1MFlvrlsJ2ydX.C2dUrnXH7mG6BwGduTvhDx.GPI4Ys
  k0A0qoU2KE59DhJqUAGETpvhHjvIyxVcbiUM.ZiNTv5cp3lweFzXnIQVuv
  02PEVe9X0HJQetIZQMT2GLBmEqoY27fjTfC5WU.go99f2U2dDAahpAla7sac
  uU.kXpWfYCuL4HRW5Bi0upaJvQxxAFUnmHzOUymx24yG.6EwqN0kxZ0y6g0v
  qjXTvGnBhec.KmEqv7g2a.GA7D.2uRDTEfpXbI.15w2tYoJtITUYVxosEjpr
  pyVIO.tP0mAGXaMQvqr05Zlc4uLcMt0Ycw0oKNhN8FL0XpZrBBE2I5H.9A1x
  vpV.C4e.0qHfG4vETxu.i.yl6mm860YxkLTatkunIDy9HulJwrG0F7bm7DP
  uXjsmGo.LW923Rg9u50lx3AUclC3jIVuVS.wg06JgThymshoH.6y.d0100G
  vKRPM93iuFW9iufuqMG0mwsB.9nSMK2fxNH3yd.2RMwIVtB.45G7akd1D
  1h9z0Vi5Z2VldEGwkatmSKRtk5JNvUFlh0wVcebCs5m4NNXc.3P.xLdIWk
  NDOuLFBVPNCmzQyzP1aMveQLR6TpPdJsgFYEJRH6A0uFkbMOPWdcwJcGIf9
  5WoRSWxIVqowv55dX.DfzPh8N8mpPM0vZBT05STGr9nJEWn0IY85xg--
Received: from 103.234.236.83 (EHLO tcbe-236083.teckbe.com)
  by 10.253.62.157 with SMTP;
  Sun, 11 Jul 2021 11:48:13 +0000
X-IM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=teckbe.com;
  q=dns/txt; s=dk2048; bh=Rt+hu+u7yxCX30ZLHx9K5FWFNdrXFCi6/V54F4VuAI=;
  h=from:reply-to:subject:to:mime-version:content-type:content-transfer-encoding:list-unsubscribe;
  b=Hqh9q7comz8ABZkUYUyXnLxLhksUBky1IEInhysFNp05YL0B6ldn9/jCCe+rJUXDNp0o4W6
  KQq2okdM28xpIvNEq5yAWboBTlog+8qYcQpBrJcET0w4kwidq2ID9nekZr/aiadneR6gjl+RX
  YXjVaKA1b0JIHBFmX5TakL0hRjz5f8Q/JMvq7kZv056UDAw1U1TSQ6SSCIktwDc76MzqHC1bmK
  ZGEH2Qm5Z6KpcOULBHj4KKynb13jBRU05aX/aqGCM9U1Qn+YqyzMqfsz02oKd8hf8Az8p15LwX
  q4lF1c4rhhJwLWkScA9bc09jZezlVaBpsaMr00Ap5XA==
Content-Type: text/html; charset=UTF-8
From: =?UTF-8?B?VghhmsgeW91ISBib2llIERlCG90?= <support@teckbe.com>
To: alexa@yahoo.com
Reply-To: support@teckbe.com
Subject: =?UTF-8?B?7T3JkZXIuGxhY2VkdDogWw91ciBPCmRlcjBJRCBPRDIzMjE2NTcwODkyOTegUGxhY2VklFN1Y2Nlc3NmddXseQ==?=
Message-ID: <tkbe_204456168_28443456_28260243_2164817_269_520_5436.1626003191881.com.root@tcbe-236083.teckbe.com>
X-Mailer: <support@teckbe.com>
X-Complaints-To: <abuse@teckbe.com>

```

Figure 7: email3.eml raw details

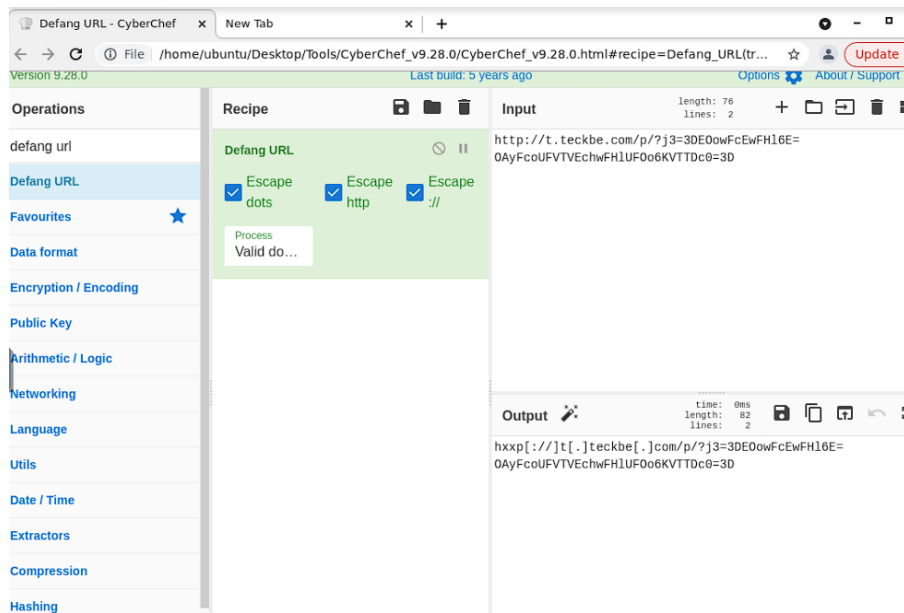


Figure 8: Defang URL for email3.eml

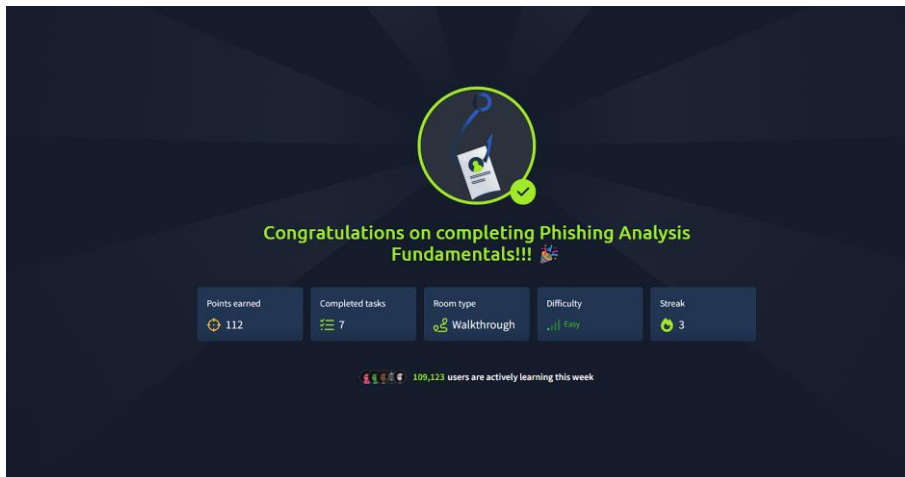


Figure 9: Complete Task