

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.

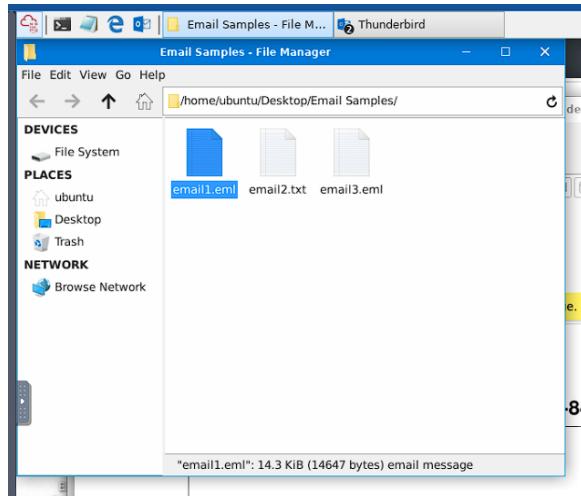


Figure 1: Types of email



Figure 2: email1.eml

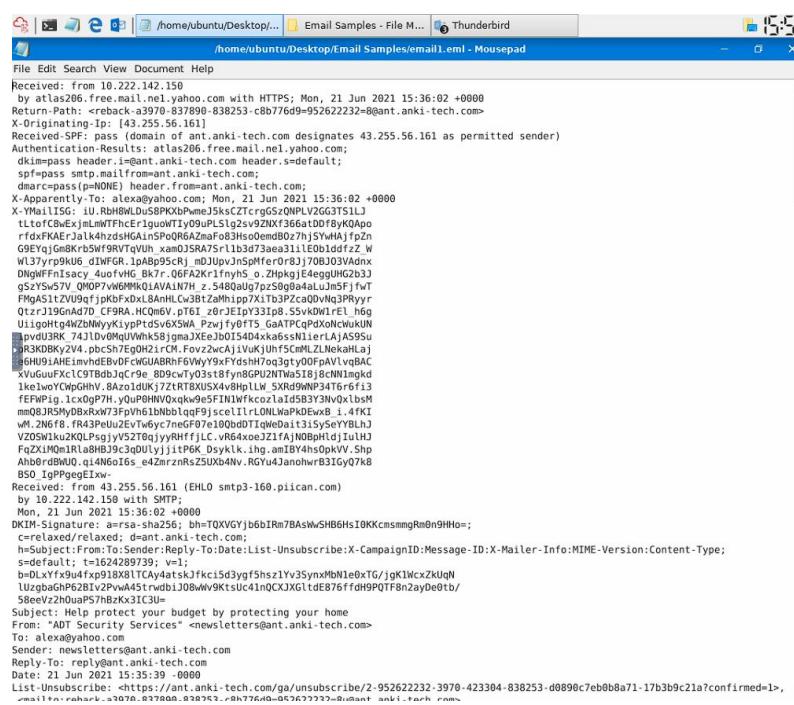


Figure 3: email1.eml raw details

Figure 4: email2.eml

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

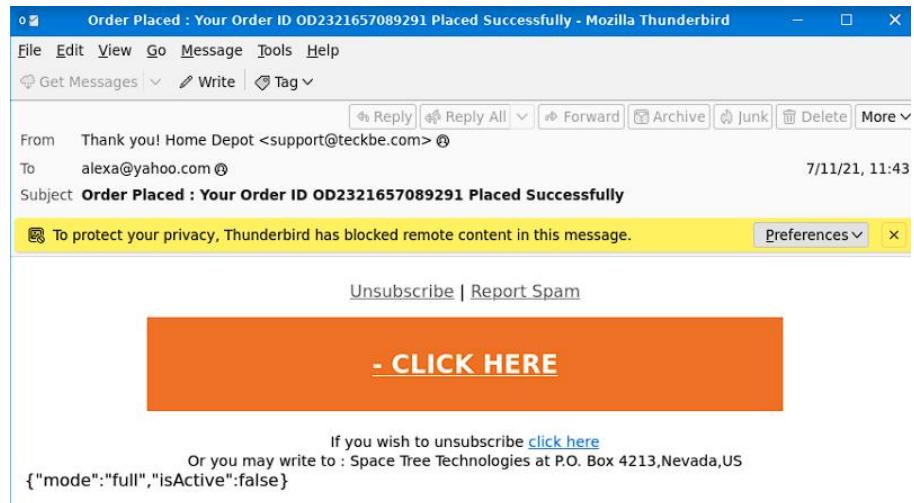


Figure 6: email3.eml

```
/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(pNONE) header.from=teckbe.com;
K-Apparently-To: alexa@yahoo.com; Sun, 11 Jul 2021 11:48:13 +0000
K-YMailISG: Pcp93_0WLDS17n7VAEQNtYkM0dxkhTU7phGw048do12xbE6
GtW2BzR4_EbK_9AXnvitLaw5vIEjKjYj0pdGtzUNCsEv4L8wXy3dH_YR0a
Iav1uK208z7qg6DGtbXvionKGt0f1Lyq10jq, mo_GxL_A_v8Jnun3AEzT3Co
WVJUf1UM7mXYt1Jfz2JEds6aHUR1xfpsQ0V1FoLH_GvWHiq2bp10x058ebjZ
P0f22tbs6cMy9mfeE7L5_dpFRKKLT4y44vtQ2XEJp_TBQx1d2BhG7_jx1l1w
o_FkjLsuktJL_p03zEcvhBMdBD851LwRkf19y0mxece0NNq5HcpJVPPYEcM
pRw0W0MnetlebnphyzTV0z2t_6H1t2JdKd8Ca_Fywpt0MCy8m77GwZj01jws3
FV15wGNgF7gsWo3pe0CSK6B_gja.QAGUUb7edzcbo1CdfbsmkJ78w5DxqqyA
XyZ1IK3Zi0z14pAqWC0gSCrkJiT2wzytloaxvn81bu1Nw_76VBnLefqoSb
K60eEfhu4xnUFSKG6BIMFvrls32yDx_C2dURxH7mgB6wDuTvhdX_GPI4Ys
k0a0qpuU2KEn59phJqUAEGTpVHhJvIyxVcb1UM_Z1NTv5cp3lweftZm1Quv
j2PEVe0q0X9OHQ0etIZMT2GLBmEqY27fj_fC5WU_gp99f72U2d0AahpLa7sac
uL_kxpFtYCuL4HRWSB10ipaJv0xxAf1nnH20Uyv24y_6EwqN9kxz20y6g0v
qjXTvGnBneC_KmEq7g2a_GA7D_2uRDTeffpxb1_ISw2tYoJtITUYvxosEjpr
pyV10_1P0mAgXaMoqj05Z1c4uLcMt0YcwOoKNHnBfLoXpzt88EZISH_9A1x
vpV_C4e_bqHFg4vETVu_i_y16m860YxkLYTvatkun1Dy9HulJwG0f7bm7Dp
uXjsgNo_1N923Rp9u50i_xAUcLc3jIVjv5_wq06JgYhymsoMoH_6y_d010Dg
vkRPm93iuFu9LuqfFLqMGoNw0s5a_9n5MwZfxNH3yC5mNNNx3.CP_xldIwMK
1h9z0V1y5Z2V1d6gkwnatsSRTkTSJNvUfhl0vCebC5mNNNx3.CP_xldIwMK
NDDu1FBVPNCmQy2PlameveQLR6TpPd)SgfYEJR6A0xufkbh0fWdcwJCgIf9
Sw0R5Wx1Vqow55dX_DfzphB8NmpPM0vZBT055TrG9njEw@1Y85xg --
Received: from 103.234.236.83 (EHL0_tcbe-236083.teckbe.com)
by 10.253.62.157 with SMTP;
Sun, 11 Jul 2021 11:48:13 +0000
OKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=teckbe.com;
q=dns/txt; s=dk2048; bh=Rt+hu+u7yxCX30Z1Hx9KSFWFNdRxFc16/V54F4VuI=;
h=from:reply-to:subject:to:mime-version:content-type:content-transfer-encoding:list-unsubscribe;
b=Hq19g7comz8ABzHkUYUnXlnLhksUBky1IE1nhysFNPo5Yl0B60dn9/jCc+JUXDNp0o4W6
K0g2okdM28Xp1vNeq5yAwb0BtB1og+8gYcOPbrjCEt04kwqd21D9neK2R/eiaidneR6qjL+Rx
YXjvAk1AbD1JHBzFhx5TakL0Hrjz5f80/JMVq7KzV0s6UDAw1U1:tS06SSCIktw0c76MzqHC1bk
ZGEH20m5Z6KpcQULBHj4Kkynb1j3_BRRU5ax/aqGCMC9U1Qn+YqyzMqfsz02oKd8hf8Az8pl5lwX
g41Fc4+rhJwLNhScA9bc09jZeziYaBopsaMr080p5XA==
```

Content-Type: text/html; charset=UTF-8
From: =?UTF-8?B?7Ghbmsge9115B1b211ERlcG90?= <support@teckbe.com>
To: alexa@yahoo.com
Reply-To: support@teckbe.com
Subject: =?UTF-8?B?7T3JkZX1gUGxhY2VkJDogW91ciBPcmRlc1BJRCBPRDIzMjE2NTcw0Dky0TEgUGxhY2VkJFNIY2Nlc3Nmwdxse0==?
Message-ID: <tkb_204456168_2843456_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

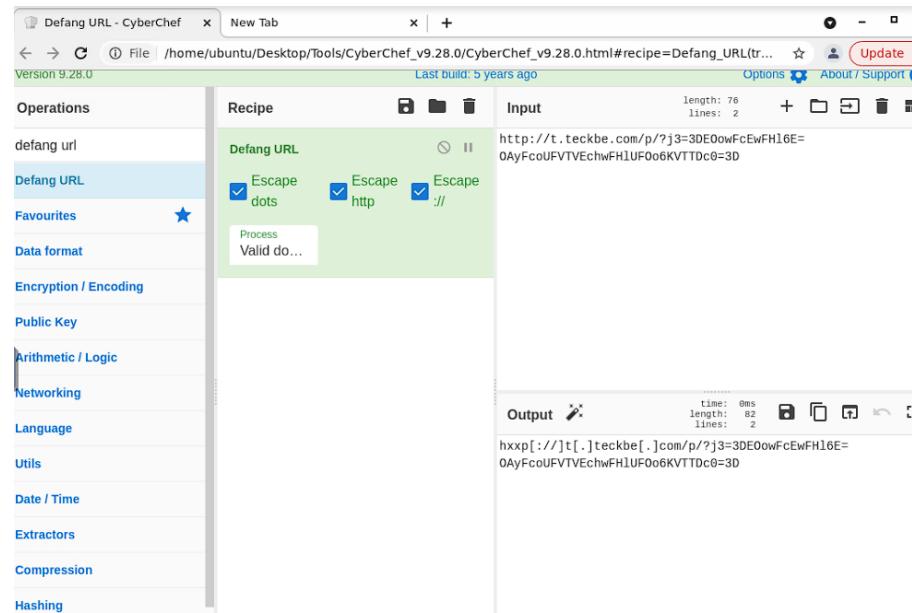


Figure 8: Defang URL for email3.eml

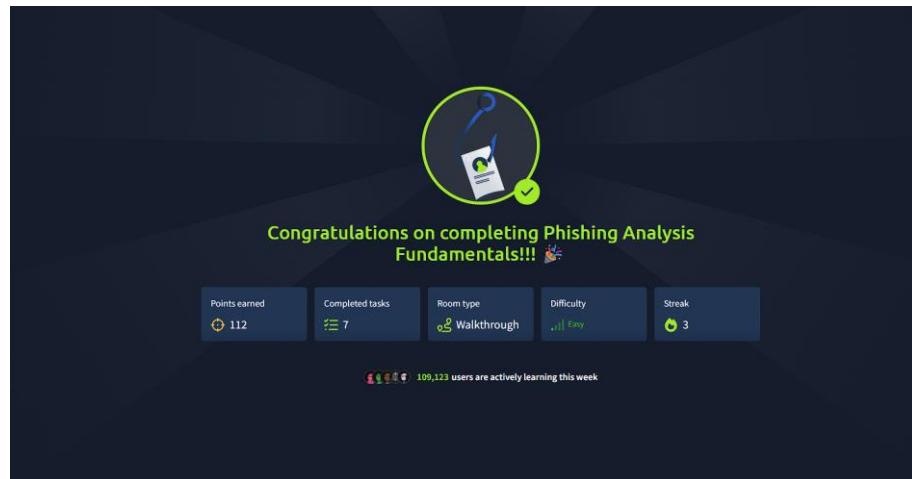


Figure 9: Complete Task