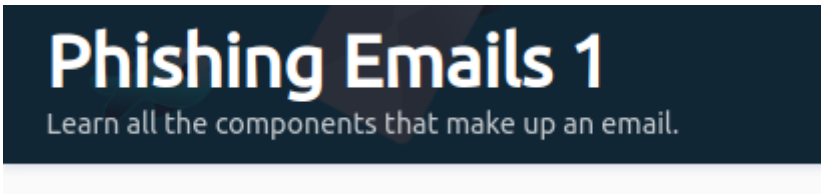
TRY HACK ME: Phishing Emails 1 Write-Up



Task 1 Introduction-

Spam and Phishing are common social engineering attacks. In social engineering, phishing attack vectors can be a phone call, a text message, or an email. As you should have already guessed, our focus is on email as the attack vector.

We all should be somewhat familiar with what spam is. No matter what, these emails somehow find their way into our inboxes.

The first email classified as spam dates back to 1978, and it's still thriving today.

Phishing is a serious attack vector that you, as a defender, will have to defend against.

An organization can follow all the recommended guidelines when it comes to building a layered defense strategy. Still, all it takes is an inexperienced and unsuspecting user within your corporate environment to click on a link or download and run a malicious attachment which may provide an attacker a foothold into the network.

Many products help combat spam and phishing, but realistically these emails still can get through. When they do, as a Security Analyst, you need to know how to analyze these emails to determine if they're malicious or benign.

Furthermore, you will need to gather information about the email to update your security products to prevent malicious emails from making their way back into a user's inbox.

Answer to the questions of this section-

No Answer needed

Task 2 The Email Address-

The invention of the email dates back to the 1970s for ARPANET. So, what makes up an email address?

1. User Mailbox (or Username)
2. @
3. Domain

Let's look at the following email address, billy@johndoe.com.

1. The user mailbox is billy
2. @ (thanks Ray)
3. The domain is johndoe.com

To simplify this even further, think about the street on which you live on.

1. You can think of your street as the domain.
2. The recipient's first/last name, along with the house number in this scenario, represents the user mailbox.
3.

Answer to the questions of this section-

Email dates back to what time frame?

1970s | Correct Answer

Task 3 Email Delivery –

There are 3 specific protocols involved to facilitate the outgoing and incoming email messages, and they are briefly listed below.

SMTP (Simple Mail Transfer Protocol) - It is utilized to handle the sending of emails.

POP3 (Post Office Protocol) - Is responsible transferring email between a client and a mail server.

IMAP (Internet Message Access Protocol) - Is responsible transferring email between a client and a mail server.

You should have noticed that both POP3 and IMAP have the same definition. But there are differences between the two.

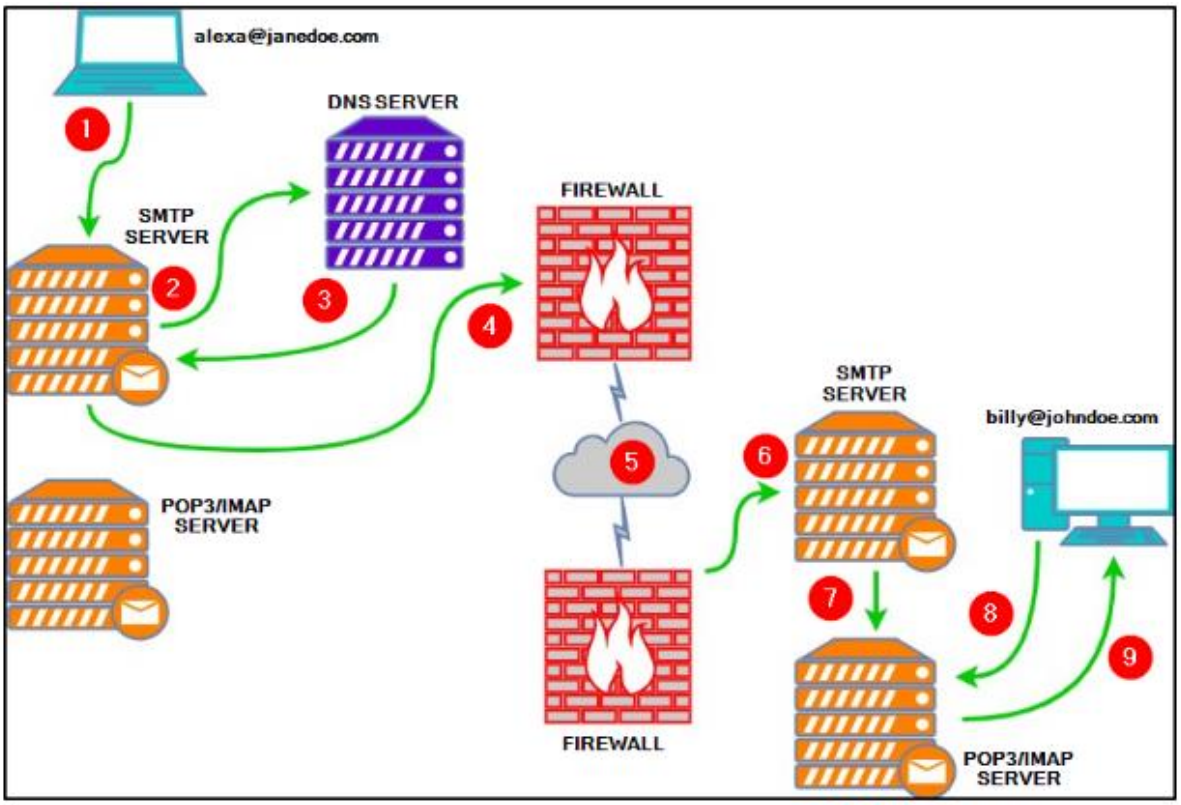
POP3

1. Emails are downloaded and stored on a single device.
2. Sent messages are stored on the single device from which the email was sent.
3. Emails can only be accessed from the single device the emails were downloaded to.
4. If you want to keep messages on the server, make sure the setting "Keep email on server" is enabled, or all messages are deleted from the server once downloaded to the single device's app or software.

IMAP

1. Emails are stored on the server and can be downloaded to multiple devices.
2. Sent messages are stored on the server.
3. Messages can be synced and accessed across multiple devices

EMAIL ARCHITECTURE-



Explanation of the email architecture-

1. Alexa composes an email to Billy (billy@johndoe.com) in her favorite email client. After she's done, she hits the send button.
2. The SMTP server needs to determine where to send Alexa's email. It queries DNS for information associated with johndoe.com.
3. The DNS server obtains the information johndoe.com and sends that information to the SMTP server.
4. The SMTP server sends Alexa's email across the Internet to Billy's mailbox at johndoe.com.
5. In this stage, Alexa's email passes through various SMTP servers and is finally relayed to the destination SMTP server.
6. Alexa's email finally reached the destination SMTP server.
7. Alexa's email is forwarded and is now sitting in the local POP3/IMAP server waiting for Billy.
8. Billy logs into his email client, which queries the local POP3/IMAP server for new emails in his mailbox.
9. Alexa's email is copied (IMAP) or downloaded (POP3) to Billy's email client.

Lastly, each protocol has its associated default ports and recommended ports. For example,

Port numbers when Protocols are Unencrypted -

SMTP is port 25

POP3 is port 110

IMAP is port 143

Port numbers when Protocols are encrypted – **over SSL/TLS**

SMTP is port 465

POP3 is port 995

IMAP is port 993

Answer to the questions of this section-

What port is classified as Secure Transport for SMTP?

465 | Correct Answer

What port is classified as Secure Transport for IMAP?

993 | Correct Answer

What port is classified as Secure Transport for POP3?

995 | Correct Answer

Task 4 Email Headers –

This task is to understand the components of what makes up an email message when it arrives in an inbox.

This understanding is necessary if you wish to analyze potentially malicious emails manually.

Before we begin, we need to understand that there are two parts to an email:

1. the email header (information about the email, such as the email servers that relayed the email)
2. the email body (text and/or HTML formatted text)

The syntax for email messages is known as the Internet Message Format (IMF).

Let's look at email headers first.

What do you look for when analyzing a potentially malicious email?

Let's start with the following email header fields:

1. From - the sender's email address
2. Subject - the email's subject line
3. Date - the date when the email was sent
4. To - the recipient's email address

This is usually clearly visible in any email client. Let's look at an example of these fields in the below image.

Warning: This is a snippet from an actual email. The email in the below image is from a honeypot Yahoo email address. Don't engage/interact with the email addresses or IP addresses revealed in this room.

Note: The numbers in the above image correspond to the email header fields bullet list above.

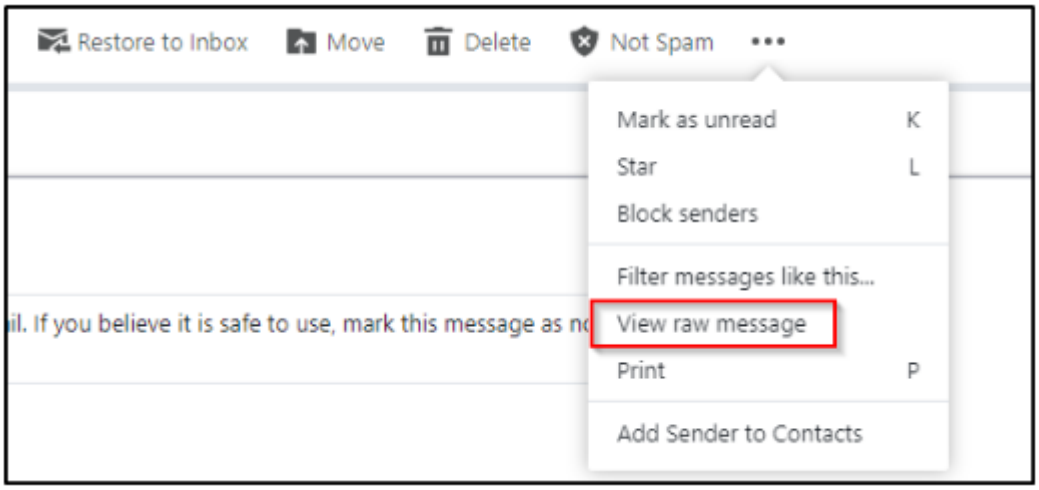
Another method to obtain the same email header information, and more, is by viewing the 'raw' email details.

When looking at an email header in detail, it can be intimidating at first, but it's not so bad if you know what to look for.

Note: Depending on your email client, whether a web client or a desktop app, the steps to view these email header fields will vary, but the concept is the same.

Review this Knowledge Base (KB) article from Media Temple on viewing the raw/full email headers in various email clients here.

In the below image, you can see how to view this information within Yahoo.



Below is a snippet of the raw message for the email sample.

```
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
 Qtzr319GnAd7D_CF9RA.HCQm6V.pT6I_z0rJEIpY33Ip8.S5vkDW1rEl_h6g
 UiigoHtg4WZbNWyyKiypPtdSv6X5WA_Pzwjfy0fTS_GaATPCqPdXoNcWukUN
 1pvdU3RK_74JlDv0MqUVWhk58jgmaJXEeJbOI54D4xka6ssN1ierLAjAS9Su
 pR3KDBKy2V4.pbcSh7EgOH2irCM.Fovz2wcAjiVuKjUhf5CmMLZLNekaHLaj
 e6HU9iAHEimvhdEBvDFcWGUABRhF6VWyY9xFYdshH7oq3gtyOOFpAVlvqBAC
 xVuGuuFXclC9TBdbJqCr9e_BD9cwTyO3stBfyn8GPU2NTWa5I8j8cNN1mgkd
 1ke1woYCWpGHhV.8Azo1dUKj7ZtRT8XUSX4v8HplLW_5XRd9WNP34T6r6fi3
 fEFWPig.1cxOgP7H.yQuP0HNVQxqkw9e5FIN1WfkcozlaId583Y3NvQxlbsM
 mmQ8JR5MyDBxRxW73FpVh61bNbblqqF9jscelIlrLONLWaPkDEwxB_i.4fKI
 wM.2N6f8.fR43PeUu2EvTw6yc7neGF07e10QbdDTIqWeDait3iSySeYYBLhJ
 VZOSW1ku2KQLPsgjyV52T0qjyyRHffjLC.vR64xoeJZ1fAjNO8pHldjIulHJ
 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
```

Note: The above image shows some, not all, of the information within an email's header.

You can review this email in the Email Samples directory on the Desktop within the attached virtual machine. The email is titled email1.eml.

From the above image, there are other email header fields of interest.

1. X-Originating-IP - The IP address of the email was sent from (this is known as an X-header)
2. Smtp.mailfrom/header.from - The domain the email was sent from (these headers are within Authentication-Results)
3. Reply-To - This is the email address a reply email will be sent to instead of the From email address

To clarify, in the email in the sample above, the Sender is newsletters@ant.anki-tech.com, but if a recipient replies to the email, the response will go to reply@ant.anki-tech.com, which is the Reply-To, and NOT to newsletters@ant.anki-tech.com.

Below is an additional resource from Media Temple on how to analyze email headers:

https://mediatemple.net/community/products/all/204643950/understanding-an-email-header

Answer to the questions of this section-

What email header is the same as "Reply-to"?

Return-Path	Correct Answer

Once you find the email sender's IP address, where can you retrieve more information about the IP?

http://www.arin.net	Correct Answer

Task 5 Email Body –

The email body is the part of the email which contains the text (plain or HTML formatted) the sender wants you to view.

Below is an example of a text-only email.

Hi John,

I hope you had a good weekend!

Could you please send over a few date/times that you're available this week to discuss your work?

Thanks,
THM

Below is an example of the HTML formatted email.

A message from TryHackMe!

Hi heavenraiza,

You have a new writeup submission: https://tryhackme.com/room/manage/windowsfundamentals1xbx

Go To TryHackMe »

For support, reply to this email.

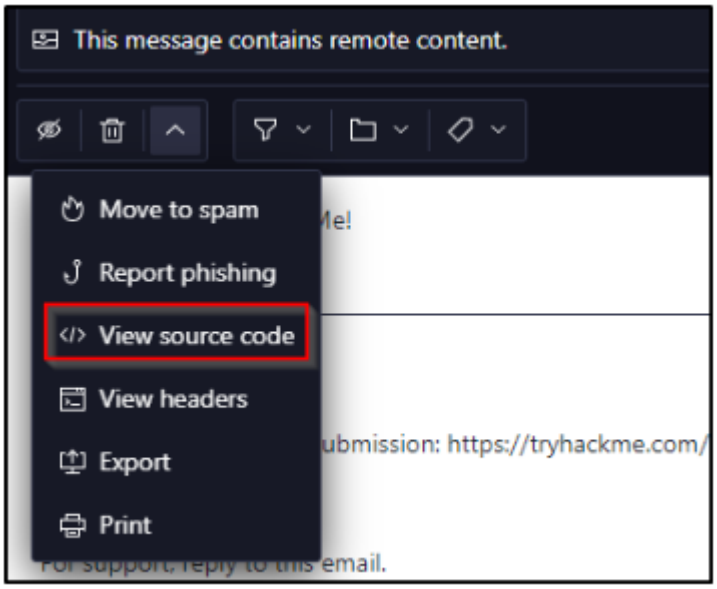
A registered UK Company
Don't like these emails? Delete Account
@RealTryHackMe

The above email contains an image (which was blocked by the email client) and embedded hyperlinks.

HTML is what makes it possible to add these elements to an email

To view an email's HTML code is the same approach shown below, but it may vary depending on the webmail client.

In the example below, the screenshot is from Protonmail.



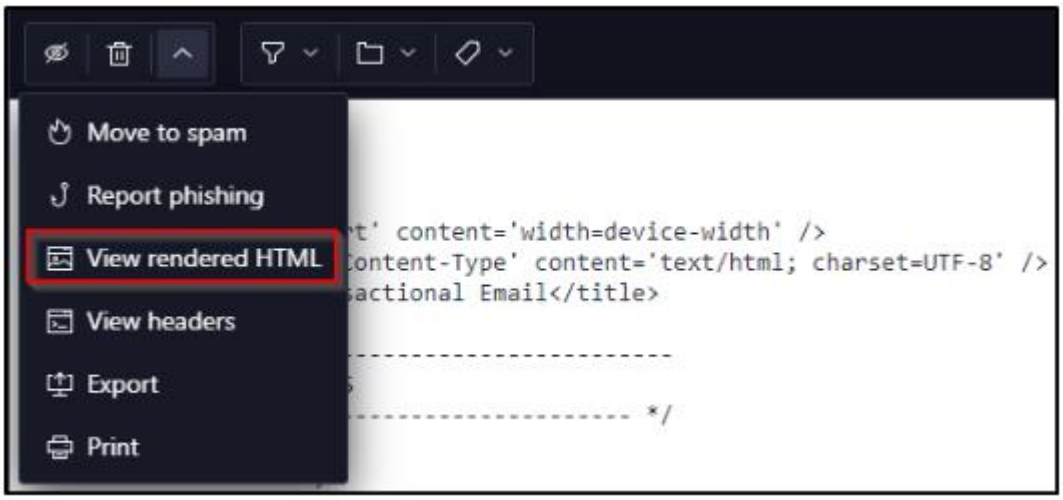
A snippet of the HTML code is shown below.

```
<body class='' >
  <table role='presentation' border='0' cellpadding='0' cellspacing='0' class='body'>
    <tr>
      <td> </td>
      <td class='container'>
        <div class='content'>

          <!-- START CENTERED WHITE CONTAINER -->
          <span class='preheader'>A message from TryHackMe!</span>
          <table role='presentation' class='main'>

            <!-- START MAIN CONTENT AREA -->
            <tr>
              <td class='wrapper'>
                <img class='logo' src='https://i.imgur.com/LSWOtDI.png'><hr>
                <table role='presentation' border='0' cellpadding='0' cellspacing='0'>
                  <tr>
                    <td>
                      <p>Hi heavenraiza,</p>
                      <p>You have a new writeup submission: https://tryhackme.com/room/manage/windowsfundamentals1xbx</p>
                      <table role='presentation' border='0' cellpadding='0' cellspacing='0' class='btn btn-primary'>
                        <tbody>
                          <tr>
                            <td align='left'>
                              <table role='presentation' border='0' cellpadding='0' cellspacing='0'>
                                <tbody>
                                  <tr>
                                    <td> <a href='https://tryhackme.com' target='_blank'>Go To TryHackMe &raquo;</a></td>
                                  </tr>
                                </tbody>
                              </table>
                            </td>
                          </tr>
                        </tbody>
                      </table>
                      <p>For support, reply to this email.</p>
```

In this specific email web client, Protonmail, the option to switch back to HTML is called "View rendered HTML".



Again, it will be different for other webmail clients.

Lastly, emails may contain attachments. The same premise applies; you can view an email's attachment from an email's HTML format or by viewing the source code.

Let's look at a few examples below.

The following example is an HTML formatted email from "Netflix" with an attachment. The web client is Yahoo!

1. The email body has an image.
2. The email attachment is a PDF document.

Now let's view this attachment within the source code.

```
Content-Type: application / pdf; name = "Payment-updateid.pdf"
Content-Disposition: attachment; filename = "Payment-updateid.pdf"
Content-Transfer-Encoding: base64
Content-ID: <f_km3inpml1>
X-Attachment-Id: f_km3inpml1

JVBERi0xLjcNCiW1tbW1DQoxIDAgb2JqDQo8PC9UeXBlL0NhdGFsb2cvUGFnZXMgMiAwIFIvTGFu
Zyhlbi1VUykgL1N0cnVjdFRyZWVSb290IDIwOCAwIFIvTWFya0luZm88PC9NYXJrZWQgdHJ1ZT4 +
L01ldGFkYXRhIDkxOSAwIFIvVmlld2VyUHJlZmVyZW5jZXMgOTIwIDAgUj4 + DQplbmRvYmoNCjIg
MCBvYmoNCjw8L1R5cGUvUGFnZXMvQ291bnQgMS9LaWRzWyAzIDAgUl0gPj4NCmVuZG9iag0KMyAw
IG9iag0KPDwvVHlwZS9QYWdlL1BhcmVudCAyIDAgUi9SZXNvdXJjZXM8PC9Gb250PDwvRjEgNSAw
IFIvRjIgMzIgMCBSL0YzIDQxIDAgUi9GNCA1MSAwIFIvRjUgNzYgMCBSL0Y2IDg0IDAgUi9GNyAx
NDYgMCBSL0Y4IDIwMyAwIFI + Pi9FeHRHU3RhdGU8PC9HUzcgNyAwIFIvR1M4IDggMCBSPj4vWE9i
amVjdDw8L0ltYWdlMjggMjggMCBSL0ltYWdlMzAgMzAgMCBSL0ltYWdlMzcgMzcgMCBSL0ltYWdl
MzkgMzkgMCBSL0ltYWdlNDMgNDMgMCBSL0ltYWdlNDUgNDUgMCBSL0ltYWdlNDcgNDcgMCBSL0lt
YWdlNDkgNDkgMCBSL0ltYWdlNTYgNTYgMCBSL0ltYWdlNTggNTggMCBSL0ltYWdlNjAgNjAgMCBS
```


From the above example, we can see the headers associated with this attachment:

1. Content-Type is application/pdf.
2. Content-Disposition specifies it's an attachment.
3. Content-Transfer-Encoding tells us it's base64 encoded.

With the base64 encoded data, you can decode it and save it to your machine.

Warning: When interacting with attachments, proceed with caution and make sure you don't double-click an email's attachment by accident.

Note: Headers specific to 'content' can be found in various locations within an email message source code, and they're not only associated with attachments. For example, Content-Type can be text/html, and Content-Transfer-Encoding can have other values, such as 8bit.

Answer to the questions of this section-

In the above screenshots, what is the URI of the blocked image?

https://i.imgur.com/LSWOtDI.png | Correct Answer

In the above screenshots, what is the name of the PDF attachment?

Payment-updateid.pdf | Correct Answer

In the attached virtual machine, view the information in email2.txt and reconstruct the PDF using the base64 data. What is the text within the PDF?

THM{BENIGN_PDF_ATTACHMENT} | Correct Answer | Hint

Copy the only base64 content from email2.txt file and use this site – https://www.ipvoid.com/base64-to-pdf/ to decode base64 content and view the flag.

ipvoid.com/base64-to-pdf/

IP Reputation API

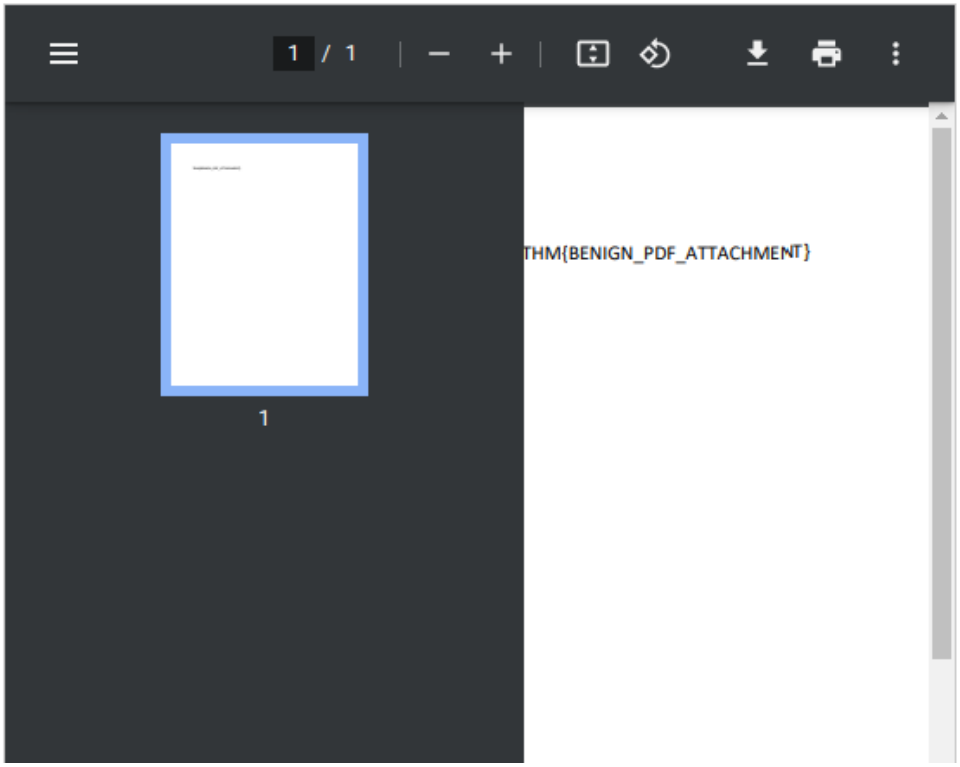
Base64 to PDF

Use this online base64 to PDF tool to convert a base64-encoded string to PDF, so you can preview it in your browser and download it as PDF file in your device. The simplest way to decode base64 as PDF online.


```
JVBERi0xLjYNJeLjz9MNCjE0IDAgb2JqDTw8L0xpbmVhcml6ZWQgMS9MI
MDE4MS9OIDEvVCAzNDk3My9IIFsgNDU3IDE1NF0+Pg1lbmRvYmoNICAgI
DQoyMSAwIG9iag08PC9EZWNvZGVQYXJtczw8L0NvbHVtbnMgNC9QcmVka
ZXIvRmxhdGVEZWNvZGUvSURbPDM2Qzc0RjkxRDgzMDdENDQ4MTQ5MjQ5O
QTYwN0I0NzJFQTQ5QUVDNTc3NUE0MTRENDM5Qz5dL0luZGV4WzE0IDExX
ZW5ndGggNTQvUHJldiAzNDk3NC9Sb290IDE1IDAgUi9TaXplIDI1L1R5c
```


ipvoid.com/base64-to-pdf/

IP Reputation API



Or you can also do

```
kali@kali:~$ base64 --decode email2.pdf > email2result.pdf
kali@kali:~$ ls
```

Where email2.pdf has base64 content and email2result.pdf has the decoded result of base64 in pdf format.

Task 6 Types of Phishing –

Different types of malicious emails can be classified as one of the following:

1. Spam - unsolicited junk emails sent out in bulk to a large number of recipients. The more malicious variant of Spam is known as MalSpam.
2. Phishing - emails sent to a target(s) purporting to be from a trusted entity to lure individuals into providing sensitive information.
3. Spear phishing - takes phishing a step further by targeting a specific individual(s) or organization seeking sensitive information.
4. Whaling - is similar to spear phishing, but it's targeted specifically to C-Level high-position individuals (CEO, CFO, etc.), and the objective is the same.
5. Smishing - takes phishing to mobile devices by targeting mobile users with specially crafted text messages.
6. Vishing - is similar to smishing, but instead of using text messages for the social engineering attack, the attacks are based on voice calls.
7. When it comes to phishing, the modus operandi is usually the same depending on the objective of the email.

For example, the objective can be to harvest credentials, and another is to gain access to the computer.

Below are typical characteristics phishing emails have in common:

1. The sender email name/address will masquerade as a trusted entity (email spoofing)
2. The email subject line and/or body (text) is written with a sense of urgency or uses certain keywords such as Invoice, Suspended, etc.
3. The email body (HTML) is designed to match a trusting entity (such as Amazon)
4. The email body (HTML) is poorly formatted or written (contrary from the previous point)
5. The email body uses generic content, such as Dear Sir/Madam.
6. Hyperlinks (oftentimes uses URL shortening services to hide its true origin)
7. A malicious attachment posing as a legitimate document

We'll look at each of these techniques (characteristics) in greater detail in the next room within the Phishing module.

Reminder: When dealing with hyperlinks and attachments, you need to be careful not to accidentally click on the hyperlink or the attachment.

Hyperlinks and IP addresses should be 'defanged'. You can read more about this technique here.

Analyze the email titled email3.eml within the virtual machine and answer the questions below.

Note: Alexa is the victim, and Billy is the analyst assigned to the case. Alexa forwarded the email to Billy for analysis.

Answer to the questions of this section-

What trusted entity is this email masquerading as?

Home Depot | Correct Answer

What is the sender's email?

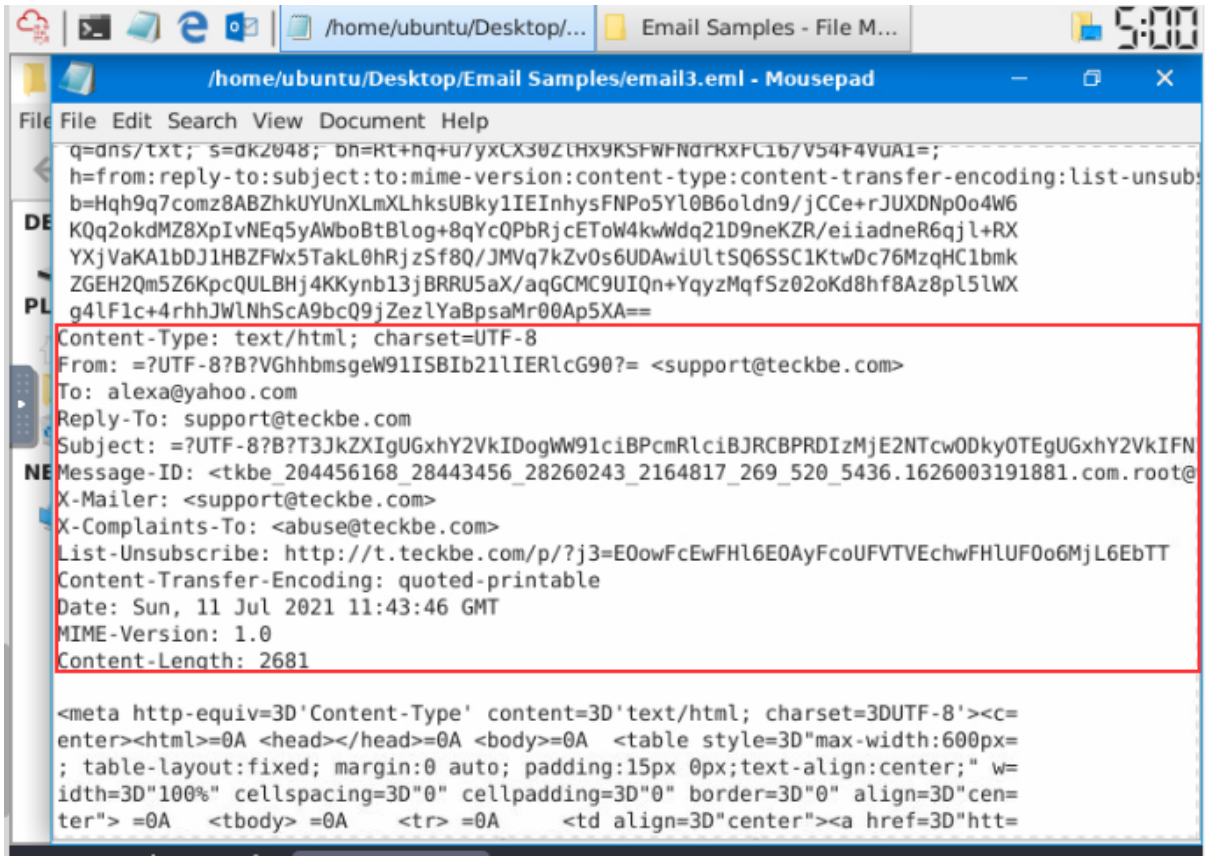
support@teckbe.com | Correct Answer

What is the subject line?

Order Placed : Your Order ID OD2321657089291 Placed ! | Correct Answer

What is the URL link for - CLICK HERE? (Enter the defanged URL)

hxxp[://]t[.]teckbe[.]com/p/?j3=EOowFcEwFHl6EOAyFcoU | Correct Answer | Hint



To read Subject Line- do base64 decoding of the UTF-8 content provided as Subject:

```
kali@kali:~$ base64 --decode email3.txt > emailresult.txt
kali@kali:~$ gedit emailresult.txt
kali@kali:~$ gedit email3.txt
```

Open email3.txt Save


```
1 T3JkZXIgUGxhY2VkIDogWW91ciBPcmRlciBJRCBPRDIzMjE2NTcwODkyOTEgUGxhY2VkIFN1Y2Nlc3NmdWxseQ==
2
```


TO READ and NOTE-

A BEC is when an adversary gains control of an internal employee's account and then uses the compromised email account to convince other internal employees to perform unauthorized or fraudulent actions.

Tip: You should be familiar with this term. I have heard this question asked before in a job interview.

Within this room, we covered the following:

1. What makes up an email address?
2. How an email travels from sender to recipient.
3. How to view the source code of an email header.
4. How to view the source code of an email body.
5. Understand the pertinent information we should obtain from an email we're analyzing.
6. Some common techniques attackers use in spam and phishing email campaigns.

That is all for this Write-up, hoping this will help you in solving the challenges of Phishing Emails 1. Have Fun and Enjoy Hacking! Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumai

For more cyber security learning follow me here-

https://github.com/ctf-time

https://www.youtube.com/channel/UCf-F-eATCUXYaUVk8Xl7OOQ

https://www.instagram.com/cybersecurity.cyber_seek/

https://twitter.com/Shefali37920461