Phishing Emails 1

* Task 1
  + Start VM
* Task 2
  + Email dates back to what time frame?
    - 1970s
* Task 3
  + What port is classified as Secure Transport for SMPT?
    - 465
  + What port is classified as Secure Transport for IMAP?
    - 993
  + What port is classified as Secure Transport for POP3?
    - 995
* Task 4
  + What email header is the same as “Reply-to”?
    - Return-Path
  + Once you find the email sender’s IP address, where can you retrieve more information about the IP?
    - http://www.arin.net
* Task 5
  + In the above screenshots, what is the URI of the blocked image?
    - https://i.imgur.com/LSWOtDI.png
  + In the above screenshots, what is the name of the PDF attachment?
    - Payment-updatedid.pdf
  + 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?
    - Open text file and delete first part leaving only base64 data. Copy all and paste into input in Cyber Chef. Save output to pdf file. Open pdf file
      * THM{BENING\_PDF\_ATTACHMENT}
* Task 6
  + What trusted entity is this email masquerading as?
    - Home Depot
  + What is the sender’s email?
  + What is the subject line?
    - Order Placed : Your Order ID OD2321657089291 Placed Successfully
  + What is the URL link for CLICK HERE
    - hxxp[://]t[.]teckbe[.]com/p/?j3=EOowFcEwFHl6EOAyFcoUFVTVEchwFHlUFOo6lVTTDcATE7oUE7AUET==
* Task 7
  + What is BEC?
    - Business Email Compromise