Phishing Email Investigation SOP

Do’s & Don’ts

1) Do not click on any URL, Image with payload in the email body.
2) Do not click on any attachment.
3) Do be cautious about opening attachments, even from trusted senders
4) DON’T click on “verify your account” or “login” links in any email.
5) Do not revert back to the email.
6) Do not submit your infra email id users on any URL/attachment during investigation.

Investigation Steps

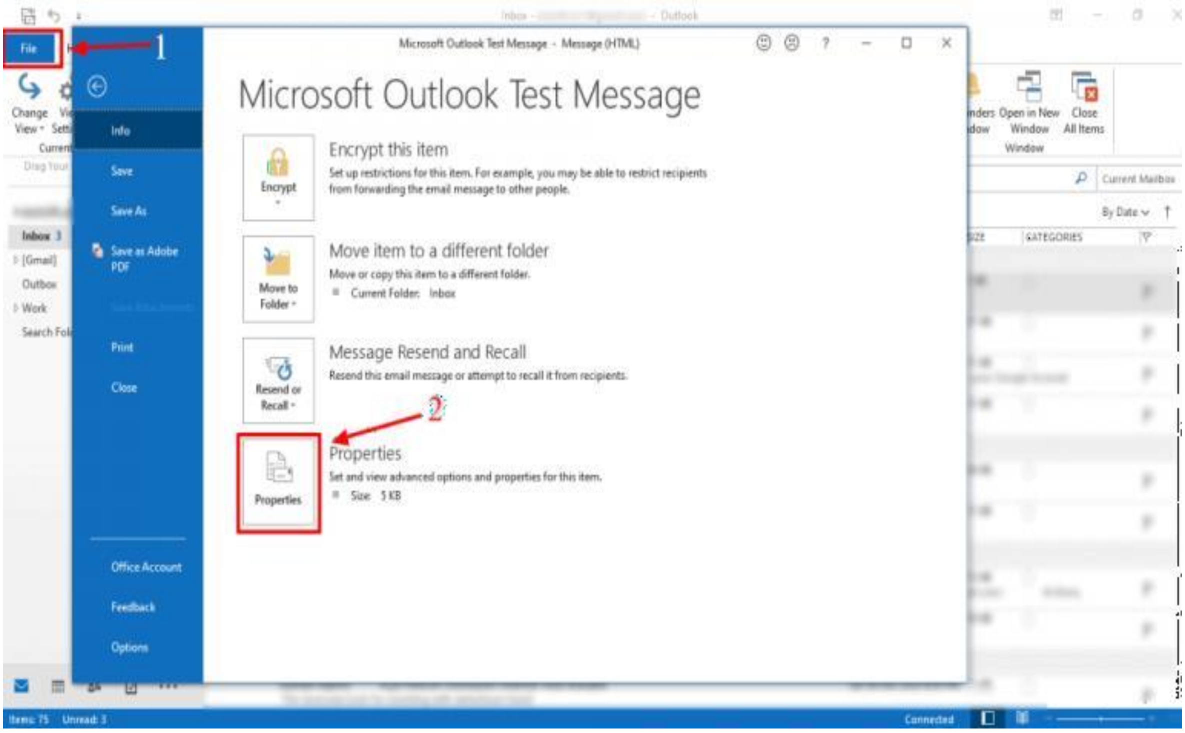
1) Email may contain URL, attachment such as pdf, word, excel, images with hidden URL payload etc. Below are some OSINT Tools which will help to investigate and to check the reputation of email.

IP Reputation	**URL Analysis**	**Redirection checker**	**Domain Lookup**	**Header Analyzers**	**Sandbox**
AbuseIPDB - IP	Urlscan.io	Where Goes	Who.is	Manual Analysis (Recommended)	Manual Analysis (Recommended)
IBM X-Force Exchange	Symantec Site review	Redirect Detective	SecurityTrails	Mx Toolbox	ANY.RUN
Virus Total	Check Phish	Urlscan.io	Virus Total	Azure Message Header Analyzer	Hybrid Analysis
Cyren IP Reputation Check	Phish Tank	Virus Total	ViewDNS.info	Messageheader	Browserling
Maltiverse	Maltiverse		Domain.com	WhatIsMyIP email header	
Cisco Talos Intelligence	Palo Alto URL filtering		ICANN Lookup		
IP Void	URL Void				
IP quality Score	Browserling				

2) Open the email and check the sender domain reputation, it might possible that sender domain look like legitimate but there might be a spelling error. For ex example@micorsoft.com

Header Analysis

1) Go to File→ Click on Properties→Internet Headers



Microsoft Outlook Test Message - Message (HTML)

Microsoft Outlook Test Message

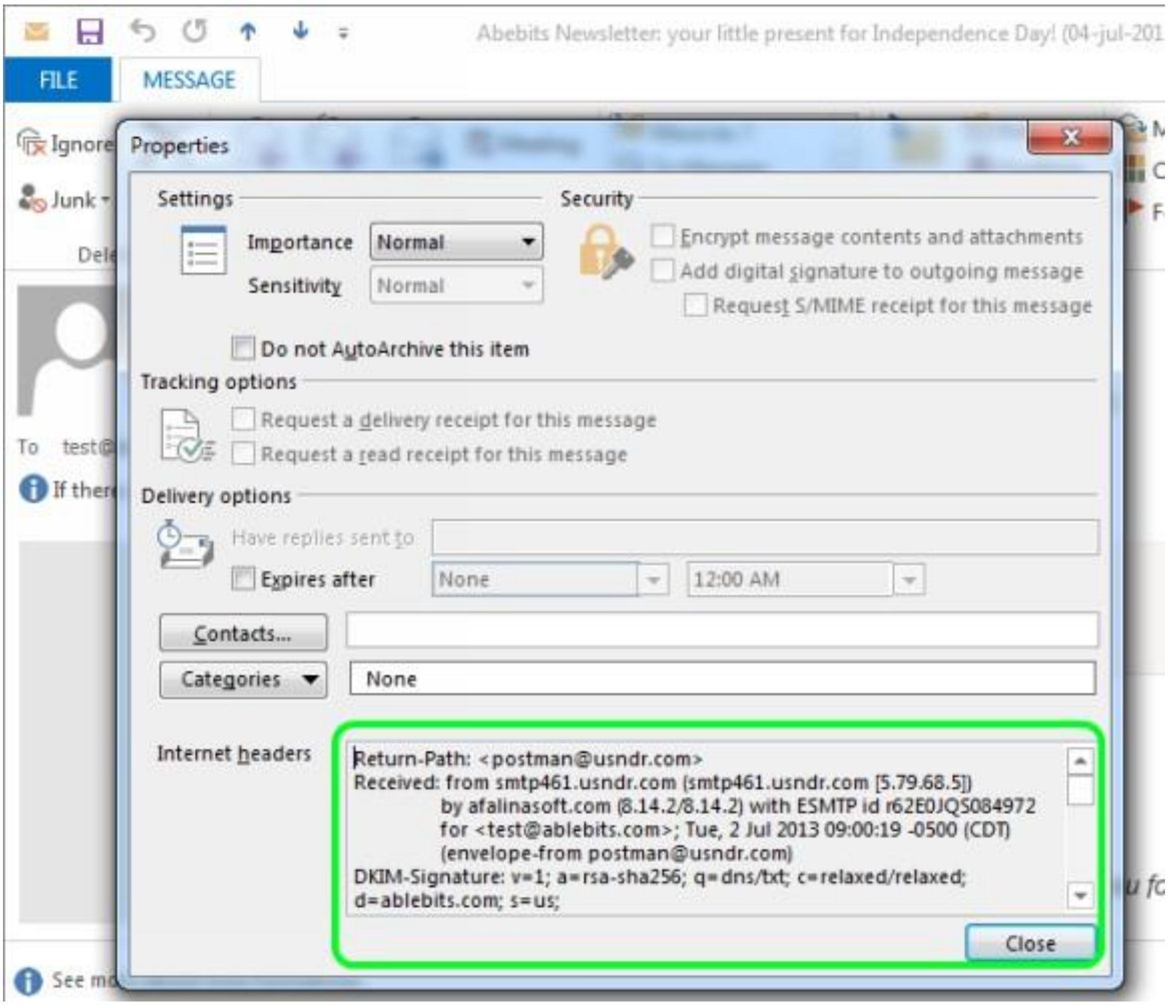
Encrypt this item
Set up restrictions for this item. For example, you may be able to restrict recipients from forwarding the email message to other people.

Move item to a different folder
Move or copy this item to a different folder.
- Current Folder: Inbox

Message Resend and Recall
Resend this email message or attempt to recall it from recipients.

Properties
Set and view advanced options and properties for this item.
- Size: 5 KB

2) Copy the headers and paste in notepad to analyze.



Abebits Newsletter: your little present for Independence Day! (04-jul-201

Importance: Normal

Sensitivity: Normal

☐ Encrypt message contents and attachments

☐ Add digital signature to outgoing message

☐ Request S/MIME receipt for this message

☐ Do not AutoArchive this item

☐ Request a delivery receipt for this message

☐ Request a read receipt for this message

Have replies sent to

☐ Expires after: None 12:00 AM

Categories: None

Internet headers

```
Return-Path: <postman@usndr.com>
Received: from smtp461.usndr.com (smtp461.usndr.com [5.79.68.5])
          by afalinasoft.com (8.14.2/8.14.2) with ESMTP id r62E0JQS084972
          for <test@ablebits.com>; Tue, 2 Jul 2013 09:00:19 -0500 (CDT)
          (envelope-from postman@usndr.com)
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
d=ablebits.com; s=us;
```

3) Check below things in message header

   a. Authentication check
   b. Return Path
   c. Envelop sender
   d. Received from

4) It might happen that email is spoofed. To know whether sender is spoofed or not, check sender id and reply-to/envelope sender if both are different then the sender might be spoofed.

URL Analysis

1) Copy the URL, make sure that you don't click on it. Paste the URL in notepad.
2) If there is any your organization user email id in the URL then replace it with test.hello@gmail.com.
3) Check reputation of the URL. The URL might be a spam, legitimate, malicious.
4) In case of malicious, the category might be related to credential harvesting or malware phishing. Identify the threat category.

Attachment Analysis

1) Save the attachment and open it in notepad only. Analyze the code in that file and check for the https/http or any url which might be present in the file.
2) If URL found then repeat the process of "URL Analysis". If not proceed with step 3.
3) Open the sandbox provide by organization and analyze the file in that. If no sandbox from organization, then check in OSINT sandbox and make sure the you have replaced the user email id with fake email id.
4) It might happen that attachment can be an image having some payload in that. Be cautious and save the file and extract it through utility tools such as 7zip. You should get the html file or any other file in that.
5) Analyze that file in sandbox or manually.

Mitigation:

1) Check the clickers who clicked/open the URL/attachment
2) Check with same subject and sender if any other user has received the same email.
3) Reset the password of user's who clicked on the URL/Attachment.
4) Isolate the machine if system is compromised.
5) Check whether the malicious email is forwarded from compromised machine to other users or not.
6) If yes then proceed to isolate them and after doing all mitigation take them into the network.
7) Block the sender id if it is malicious
8) Block The URL in your Infra
9) Block other IOC's such as hash, IP etc.

Notification To the user

SPAM Emails	Legitimate Email	Malicious Emails
Hello, Thankyou for reporting this email. SOC Team have	Hello, Thank you for reporting this email.	Hello, Thank you for reporting this email.

investigated the email and found this email as SPAM. Please do not click/open any URL/attachment. Kindly do not revert back to that email.	Soc Team have investigated the email and found it as Legitimate email.	SOC Team have investigated this email and found it as Malicious email Kindly do not click on any URL and do not open any attachment. Please do not revert back to that email.

Summary: The email contains an attachment/URL which is spam/malicious/legitimate. After checking the URL/Attachment we found it as non-malicious/malicious. There are 12 user who received the same email and 1 clicker observed.

Investigation References: