Phishing Analysis Fundamentals

Introduction

- spam and phishing are common social engineering attacks
- first email classified as spam dates back to 1978

The Email Address

Makeup of an email address (billy@johndoe.com)

1. User mailbox - billy
2. @
3. Domain – johndoe.com

Email Delivery

- protocol are used to send email
- protocols were created to handle specific network related tasks

3 specific protocols involved to facilitate the outgoing and incoming email messages

- SMTP / Simple Mail Transfer Protocol : utilized to handle the sending of emails
- POP3 / Post Office Protocol : responsible for transferring email between a client and mail server
- IMAP / Internet Message Access Protocol : responsible for transferring email between a client and mail server

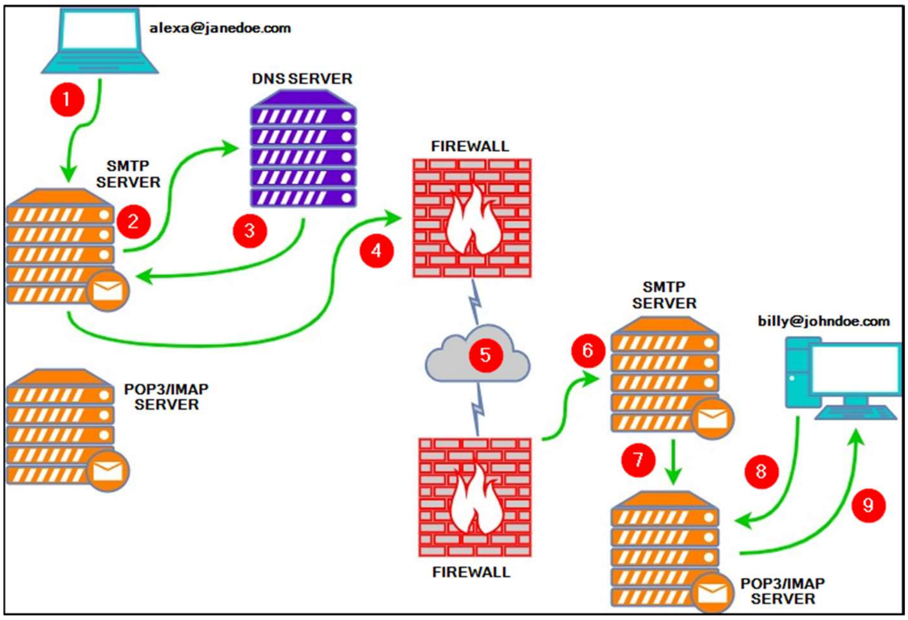
Difference between POP3/IMAP

POP3

- emails are downloaded and stored on a single device
- sent messages are stored on the single device from which the email was sent
- emails can only be accessed from the single device the emails were download to

IMAP

- emails are stored on the server and can be downloaded to multiple devices
- sent messages are stored on the server
- messages can be synced and accessed across multiple devices



1. Alexa composes an email to Billy (billy@johndoe.com) in her favourite email client.
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.1

Port Numbers
SMTP
- default port + does not provide encryption: 25
- secure port + TLS/SSL encryption: 465

IMAP
- default port + does not provide encryption: 143
- secure port + TLS/SSL encryption: 993

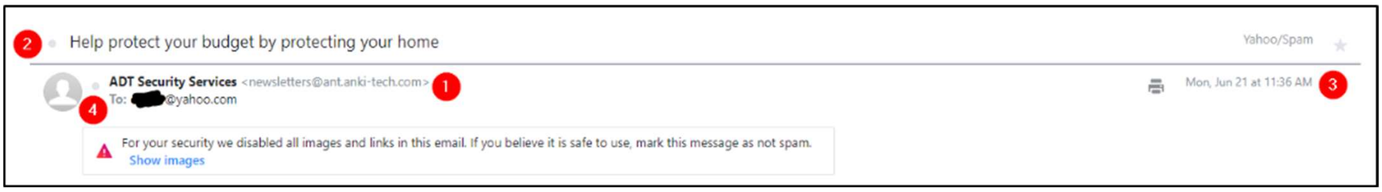
POP3
- default port + does not provide encryption: 110
- secure port + TLS/SSL encryption: 995

Email Headers

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

2 parts to an email:
- email header (information about the email, such as the email servers that relayed the email)
- email body (text and/or HTML formatted text)

- syntax for email messages is known as the Internet Message Format / IMF



Help protect your budget by protecting your home

Yahoo/Spam

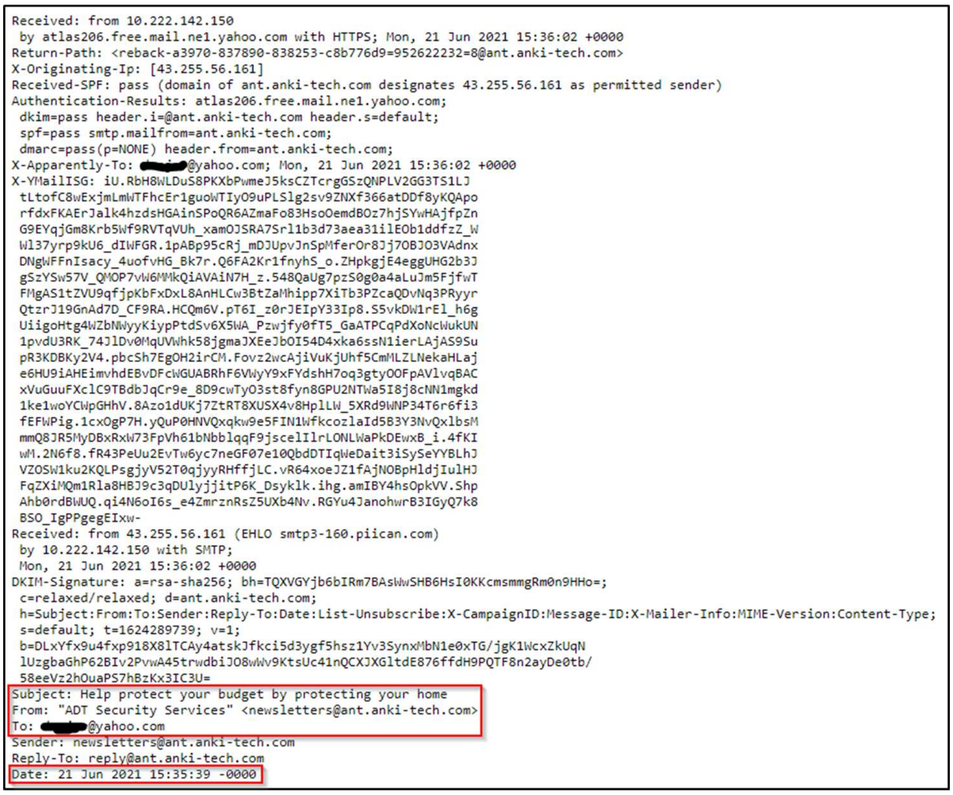
ADT Security Services <newsletters@ant.anki-tech.com>
To: [redacted]@yahoo.com

Mon, Jun 21 at 11:36 AM

For your security we disabled all images and links in this email. If you believe it is safe to use, mark this message as not spam.
Show images

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

- raw email message



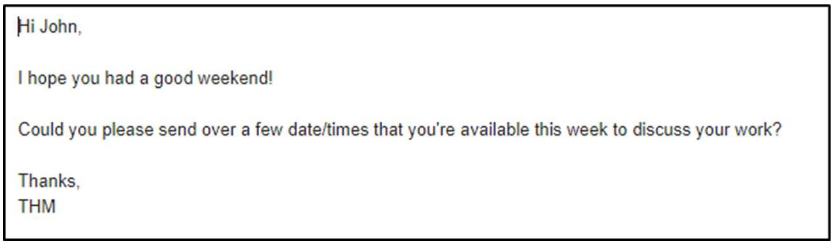
```
Received: from 10.222.142.150
 by atlas206.free.mail.ne1.yahoo.com with HTTPS; Mon, 21 Jun 2021 15:36:02 +0000
Return-Path: <reback-a3970-837890-838253-c8b776d9=952622232=8@ant.anki-tech.com>
X-Originating-Ip: [43.255.56.161]
Received-SPF: pass (domain of ant.anki-tech.com designates 43.255.56.161 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
 QtzrJ19GnAd7D_CF9RA.HCQm6V.pT6I_z0rJEIpY33Ip8.S5vkDW1rEl_h6g
 UiigoHtg4WZbNWyyKiypPtdSv6X5WA_Pzwjfy0fT5_GaATPCqPdXoNcWukUN
 1pvdU3RK_74JlDv0MqUVWhk58jgmaJXEeJbOI54D4xka6ssN1ierLAjAS9Su
 pR3KDBKy2V4.pbcSh7EgOH2irCM.Fovz2wcAjiVuKjUhf5CmMLZLNekaHLaj
 e6HU9iAHEimvhdEBvDFcWGUABRhF6VWyY9xFYdshH7oq3gtyOOFpAVlvqBAC
 xVuGuuFXclC9TBdbJqCr9e_8D9cwTyO3st8fyn8GPU2NTWa5I8j8cNN1mgkd
 1ke1woYCWpGHhV.8Azo1dUKj7ZtRT8XUSX4v8HplLW_5XRd9WNP34T6r6fi3
 fEFWPig.1cxOgP7H.yQuP0HNVQxqkw9e5FIN1WfkcozlaId5B3Y3NvQxlbsM
 mmQ8JR5MyDBxRxW73FpVh61bNbblqqF9jscelIlrLONLWaPkDEwxB_i.4fKI
 wM.2N6f8.fR43PeUu2EvTw6yc7neGF07e10QbdDTIqWeDait3iSySeYYBLhJ
 VZOSW1ku2KQLPsgjyV52T0qjyyRHffjLC.vR64xoeJZ1fAjNOBpHldjIulHJ
 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
```

1. X-Originating-IP - The IP address of the email was sent from (this is known as an X-header) [43.255.56.161]
2. Smtp.mailfrom/header.from - The domain the email was sent from [ant.anki-tech.com]
3. Reply-To - This is the email address a reply email will be sent to instead of the From email address [reply@ant.anki-tech.com]

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.

Email Body
- part of the email that contains the text the sender wants you to view

Text-only email:



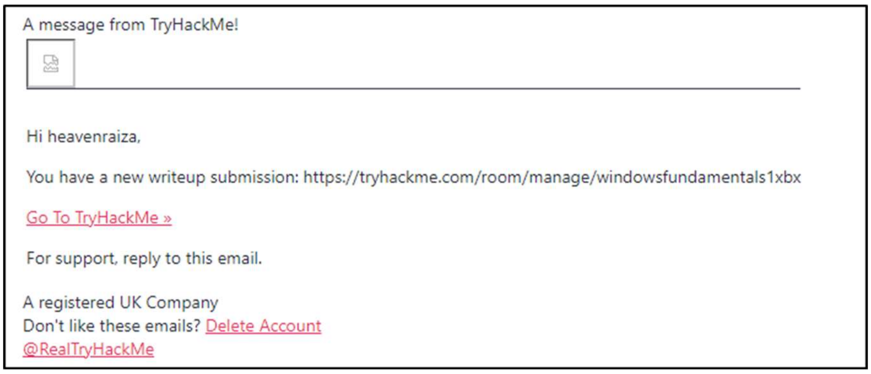
Hi John,

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

HTML format email:



A message from TryHackMe!

Hi heavenraiza,

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

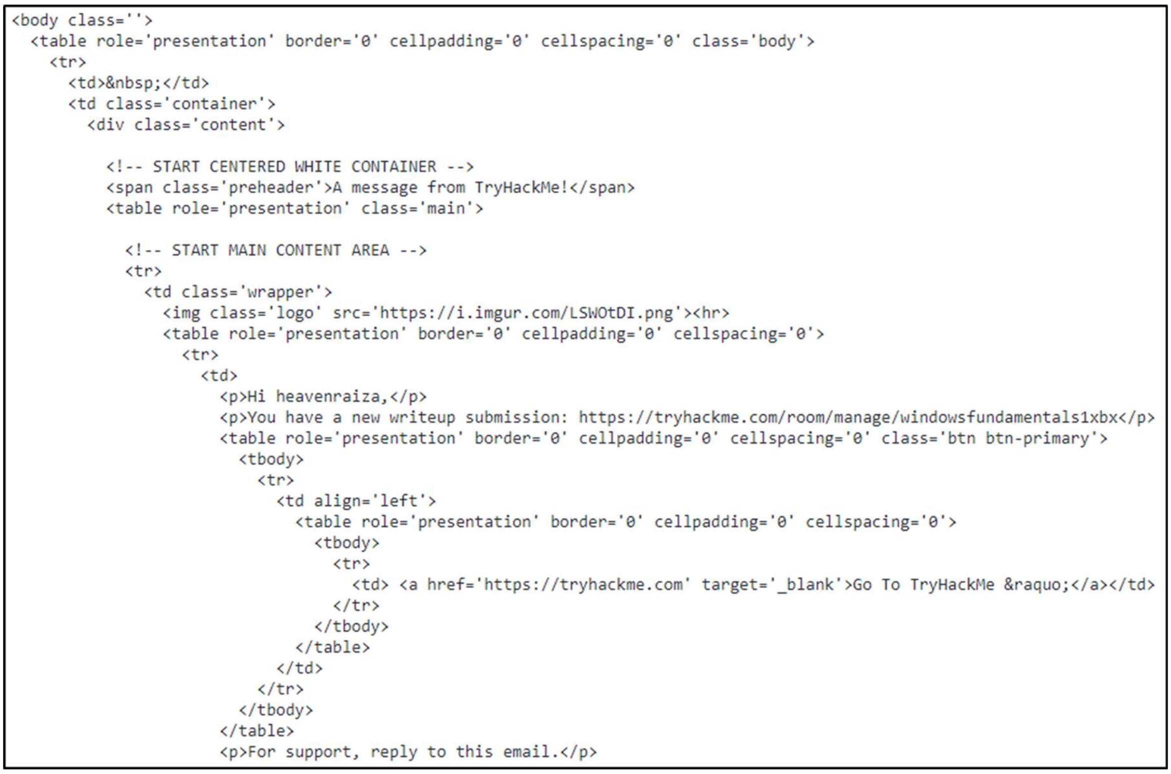
Go To TryHackMe »

For support, reply to this email.

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

- above email contains and image (blocked by the email client) and embedded hyperlinks
- HTML makes it possible to add these elements to an email

HTML code </>View source code:

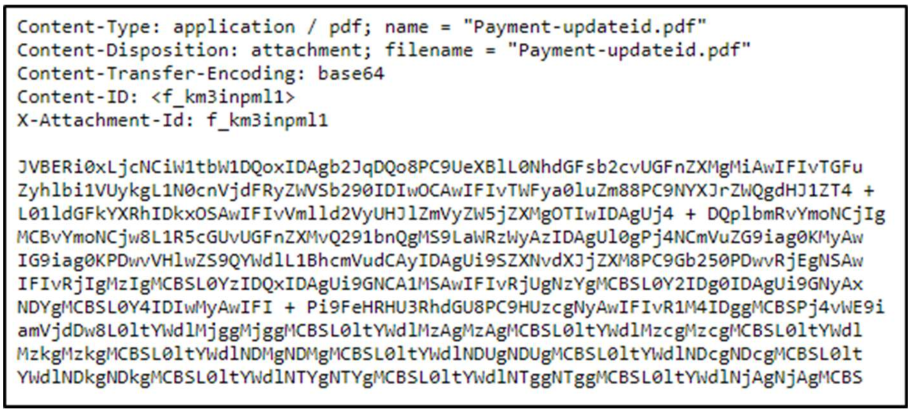


```
<body class=''>
  <table role='presentation' border='0' cellpadding='0' cellspacing='0' class='body'>
    <tr>
      <td>&nbsp;</td>
      <td class='container'>
        <div class='content'>

          <!-- 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>
```

- view the 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
```

Content-Type: application/pdf
Content-Disposition: specifies it’s an attachment
Content-Transfer-Encoding: base64 encoded

Types of Phishing

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

Characteristics phishing emails have in common:

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

*BEC – Business Email Compromise
[is when an adversary gains control of an internal employees account and then uses the compromised email account to convince other internal employees to perform unauthorised/fraudulent actions]