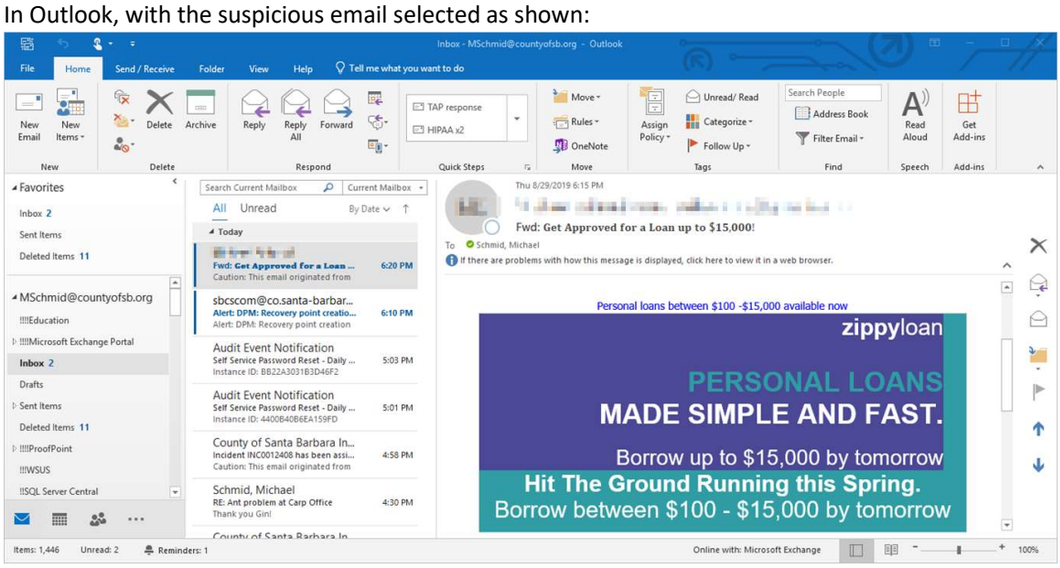
How to Report Suspicious Email

Suspicious email can be any email which looks like SPAM, phish, extortion, was unexpected, has an irrelevant context, seems too good to be true, extremely poor grammar, suspiciously vague and brief and seeming to come from a known VIP, usually comes from an external email address, and many other possibilities.

Suspicious emails should always be reported immediately by any employee who receives them in order to help stop email cybersecurity threats as soon as possible.

Instructions:

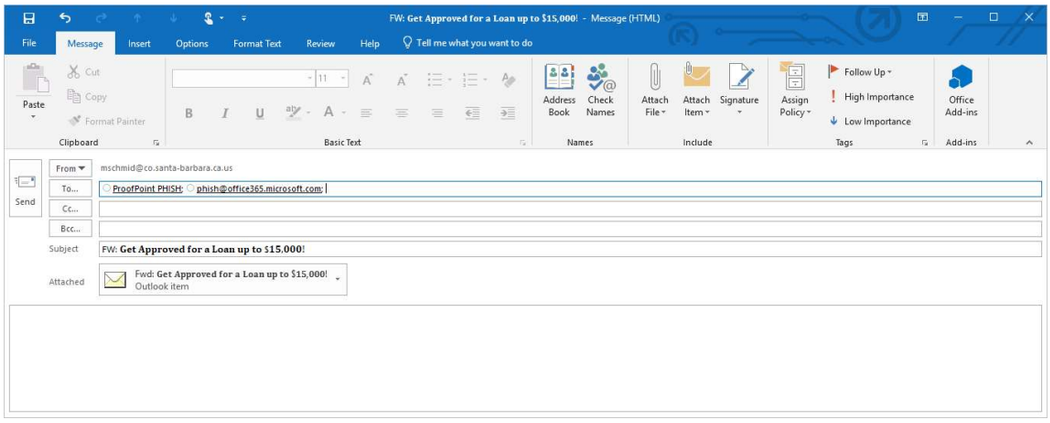
1. In Outlook, with the suspicious email selected as shown:



   Press the Ctrl, Alt, and F keys simultaneously. This keystroke combination will save the current email as a file, and attach it to a new email. This is the **best method** for sending in email to be analyzed.

2. Address this new email to both:
   a. proofpointphish@co.santa-barbara.ca.us and
   b. phish@office365.microsoft.com

   as shown below:



   There is no need to include any text in the body of the email.

3. Send the email.

Sending the email to our local proofpointphish@co.santa-barbara.ca.us mailbox will cause Proofpoint TAP to analyze the forwarded email. If it's determined to be malicious, Proofpoint TRAP will pull all copies of the email from all county mailboxes and hold them securely in quarantine.

Sending the email to phish@office365.microsoft.com will help reduce the chances of email like the one forwarded from arriving in the future without being stopped by the Office365 quarantine.

NOTE: This method is only known to work while using the Outlook client. When reporting from OWA or from a mobile device, simply forward the email.

NOTE: Internal county emails blasts such as retirement workshop announcements, EU training announcements, blood drive announcements, and any other authorized blasts typically do not qualify as "suspicious" and should not be reported. It is possible, however, that a sender's mailbox could be breached and used to send a malicious blast. If that were to happen, the usual indicators such as irrelevant context and poor grammar would be present. If that were to occur, please report it!

NOTE: Individual department policies may add to these instructions. Please be sure to comply with any additional instructions your department specifies for reporting suspicious email.