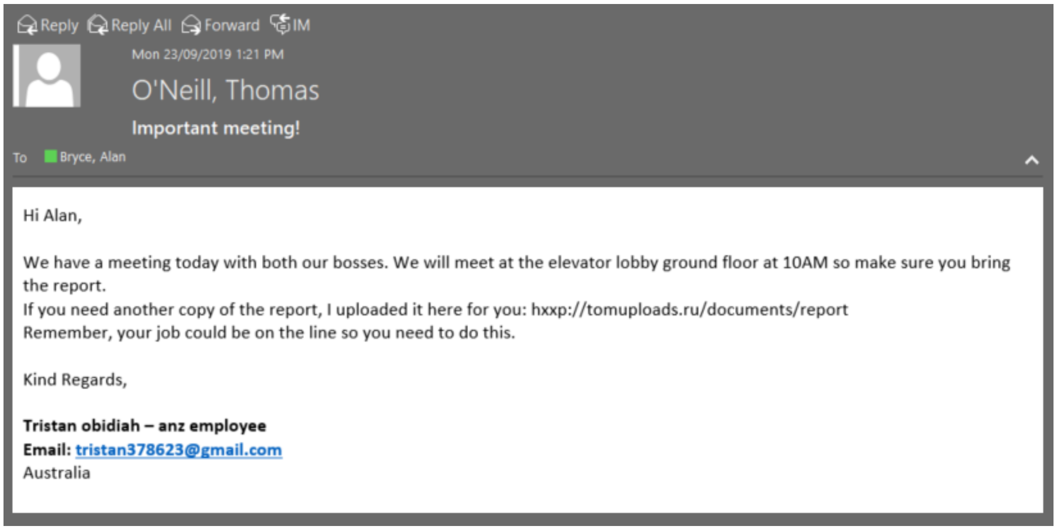
Please download the pdf document in the resources section to view the emails you will need to investigate.

In your investigation of the emails, what signs did you find to indicate whether each email was malicious or safe? Give your opinion and analysis on these emails in this document, then upload it as your submission.

Here is an example to use as a reference point:



Mon 23/09/2019 1:21 PM

O'Neill, Thomas

Important meeting!

To 🟩 Bryce, Alan

Hi Alan,

We have a meeting today with both our bosses. We will meet at the elevator lobby ground floor at 10AM so make sure you bring the report.
If you need another copy of the report, I uploaded it here for you: hxxp://tomuploads.ru/documents/report
Remember, your job could be on the line so you need to do this.

Kind Regards,

Tristan obidiah – anz employee
Email: tristan378623@gmail.com
Australia

Example Answer (Please note this is not part of the Task and is an example only. Please remove this section from your task submission):

Is this email Safe or Malicious?	My Analysis
Malicious	• *The attached URL is from Russia.* • *The email sender is requesting the user download a file with fairly generic justification.* • *This is enough indicators for us to assume that the link is probably malicious and should be treated as such.* • *Overall the email is not very professional. It is far too generic using terms that could apply to almost anyone and anywhere such as “the report” and the job title of “anz employee”. Also ‘anz’ is not capitalized, and the email provided is not a business email.* • *The name the email uses isn’t consistent with the display name.* • *Finally the email tries to instill a sense of urgency and dread by mentioning that the person’s job is on the line, and mentioning their bosses to provide some sort of authority to what they are saying. This is a common form of social engineering.*

Email 1:

Is this email Safe or Malicious?	My Analysis
Safe	• There is no attached file or any link to make the mail malicious. • Its just normal conversation between two persons. • Hence, the Email is safe

Email 2:

Is this email Safe or Malicious?	My Analysis
Malicious	• Email is sent from Russia • The URL is made using Hyperlinked Texts • Sender doesn’t mention the name of the user. • One driver never sends any mail like this • The attached link might be a suspect for a phishing link to steal users data • Without clicking the link, directly open log in to the office account and check if any problem is there.

Email 3:

Is this email Safe or Malicious?	My Analysis
Malicious	• The URL attached is a fake URL This is a clear phishing mail to steal users data (username, password) • The sender is genuinely asking if the facebook is down or not, but the attached link is malicious as the letter “b” in facebook is of different format. • The extension .opt (Optinal Practical Training) is commony used by STEM students only.

Email 4:

Is this email Safe or Malicious?	My Analysis
Safe	- This is a forwarded mail by Adam Marcus - Moreover it's a marketing email, and does not contain any malicious link or attached that could lead to any phishing attack. - Hence the mail is Safe

Email 5:

Is this email Safe or Malicious?	My Analysis
Malicious	- The email is sent by an FBI undercover agent, and none of the government spy or agents sends any mail to a normal civilian. - The mail asks the user to send the account details to contact further, which is a potential phishing attack to steal data.

Email 6:

Is this email Safe or Malicious?	My Analysis
Safe	- There is no attachments or links that could lead to any phishing site or malware. - This is a normal conversation between sender and reciever. - The signature in the mail defines the mail is genuine and sent by ANZ employee - Morever, the logo and name is capitalized and correct. - Hence the mail is genuine.

Email 7:

Is this email Safe or Malicious?	My Analysis
Malicious	- The URL attached is "http" instead of "https" - This is an ad phishing mail - The sender mail id is suspicious - The attached link is a php webpage, which is a potential phsihing webpage.