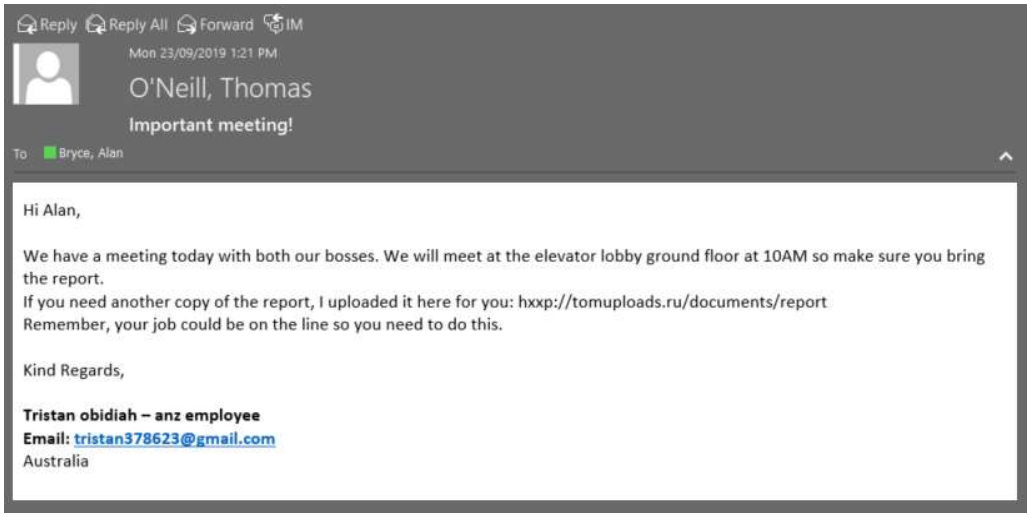
Please download the pdf document in the resources section to view the emails you will need to investigate.

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:



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	• **Consistent sender identity** – The name and email address match and align with expected sender details. • **Established relationship** – The conversation appears to be between two individuals who know each other well. • **No suspicious elements** – No unexpected links, attachments, or requests for sensitive information. • **No social engineering tactics** – The email lacks urgency, authority pressure, or manipulation attempts. • **Casual and natural content** – The message follows a normal conversation pattern without unusual phrasing or generic terms. • **Conclusion:** This email exhibits multiple phishing red flags and should be considered malicious.

Email 2:

Is this email Safe or Malicious?	My Analysis
Malicious	• **Suspicious sender domain** – The email originates from a Russian domain (.ru), which is inconsistent with Microsoft or its subsidiaries. • **Inconsistent branding** – Mentions of 'OneDrive', 'Office365', and 'Microsoft' are used without clarity, reducing credibility. • **Hidden malicious link** – The email contains a hyperlink embedded in text, a common tactic used in phishing attempts. • **Unprofessional formatting & language** – Poor grammar, awkward phrasing, and unnecessary capitalization ('ADOBE PDF') indicate low legitimacy. • **Social engineering tactics** – Uses the word 'SECURITY' to falsely create urgency and importance. • **Unclear request for action** – The email urges the recipient to take action without providing clear context. • **Unprofessional email signature** – Signs off as 'Office365, Thank You, Customer Support', which is generic and lacks authenticity. • **Conclusion:** Multiple phishing indicators suggest that this email is malicious and should be treated with caution.

Email 3:

Is this email Safe or Malicious?	My Analysis
Malicious	• **Deceptive sender appearance** – The email mimics a friendly message, creating a false sense of trust. • **Embedded suspicious link** – The email asks the recipient to check a Facebook link, but the actual domain is not part of Facebook's official domains.

	• **Visual deception in domain name** – The letter 'b' in "Facebook" is replaced with a visually similar Greek beta (β), making the URL appear legitimate at a glance. • **Suspicious domain structure** – The URL ends in ".com.opt", which is not a known Facebook domain or subdomain. • **Potential credential harvesting** – This setup is a common phishing tactic used to trick users into entering their login credentials on a fake login page. • **Conclusion:** The email exhibits clear phishing characteristics by disguising a malicious link within a seemingly normal conversation. It should be flagged as malicious and reported.

Email 4:

Is this email Safe or Malicious?	My Analysis
Safe	• **Forwarded promotional email** – The email appears to be an advertisement rather than a phishing attempt. • **Sender consistency** – The email ID (aman.zoom@gmail.com) and display name (Adam Markus) have nothing unusual, indicating authenticity. • **Legitimate domain** – The promotional site's domain (.massdrop.com) is a well-known, legitimate domain, reducing suspicion. • **Professional formatting** – The email body appears professional, with no noticeable grammar errors or suspicious content. • **No urgency or authority tactics** – The email does not use pressure tactics or claim authority to manipulate the recipient. • **Conclusion:** The email does not exhibit malicious characteristics. It is a genuine promotional message forwarded by a known sender and can be considered safe.

Email 5:

Is this email Safe or Malicious?	My Analysis
Malicious	• **Suspicious sender identity** – The email claims to be from an FBI undercover agent but provides no surname, reducing credibility. • **Poor grammar and unprofessional wording** – Multiple grammatical mistakes and awkward sentence structure suggest a lack of professionalism, which is uncommon in official communications. • **Highly unrealistic context** – The story about burnt email accounts, blocked international communication, and a dictator preventing emails to first-world countries is extremely unlikely.

	• **Urgency and social engineering** – The sender is trying to create urgency by claiming they need to use the recipient's account to send an "extremely urgent email." • **Attempting to establish authority** – The email signature includes "Superintendent Vincent", attempting to sound authoritative to pressure the recipient. • **Suspicious email subject** – The title, "You are needed," is vague but designed to grab attention and create urgency. • **Conclusion:** The email is highly suspicious and malicious. It appears to be a social engineering attempt to gain unauthorized access to the recipient's email account by leveraging urgency, fake authority, and an improbable scenario. It should be reported and ignored.

Email 6:

Is this email Safe or Malicious?	My Analysis
Safe	• **Legitimate sender and recipient** – The email domains are @anz.com, which is a verified corporate domain. • **Clear and professional communication** – The grammar and wording are polished, making it look like a genuine office conversation. • **No suspicious elements** – The email contains no links or attachments, reducing the risk of phishing or malware. • **No urgency or social engineering** – The email does not pressure the recipient into taking any rushed or unsafe action. • **Email thread visibility** – The original email is included in the response, maintaining context and transparency. • **Conclusion:** The email appears safe. It is a legitimate office communication between colleagues with no phishing indicators or malicious intent.

Email 7:

Is this email Safe or Malicious?	My Analysis
Malicious	• **Suspicious sender name** – The name "Val.kill.ma" is unprofessional and not associated with a corporate entity like Geico. • **Inconsistent sender details** – The email signs off as "Mike Ferris", which does not match the sender name in the email header. • **Lack of context** – The email contains no message or explanation, just a single embedded link. • **Suspicious link** – The URL "hxxp://iwhrhwicy.urlif.y/receipt.php" is not a recognizable or legitimate Geico domain and is likely malicious.

	• **Misleading subject line** – The title suggests a promotional offer, but the email content does not match, making it appear as a phishing attempt. • **Conclusion:** This email is highly suspicious and malicious. The questionable sender name, mismatched details, lack of context, and unsafe URL indicate a phishing attempt, likely designed to redirect the recipient to a malicious site.