|  |
| --- |
|  |

**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:**

A screenshot of a social media post

Description automatically generated

***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 | Based on my analysis it appears that the email content resembles a conversation between friends discussing a gaming event. There is no indication of any request for information or any inclusion of attachments or links. The tone is relaxed. There is no sense of urgency or fear which're often present, in phishing attempts. Additionally the email addresses used seem to be personal and not imitating any business or organization. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | The email seems to come from a domain called venture.ru which is not usually linked to Microsoft or OneDrive services. The sender uses language to encourage the recipient to click on a link, for account updates which's a common trick used in phishing attempts. Moreover the email lacks personalization. Includes a mistake both of which raise suspicions. The email lacks a tone. Fails to provide specific information typically found in genuine communication, from service providers. |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | This email includes a URL that resembles a legitimate Facebook link. However, upon closer inspection, it is a clever imitation designed to deceive the recipient. The actual domain in the link is misspelled, which is a common trick used by phishers to lure individuals into clicking on a malicious link. The email attempts to create a sense of curiosity or urgency by suggesting that Facebook is down and seeking confirmation. This can lead to impulsive clicking without proper scrutiny. |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | The email appears to be a standard forwarded promotional message regarding a gaming headset. This is a typical marketing communication. It contains no direct requests for personal information and does not prompt the recipient to take any suspicious actions. The forwarding chain includes a known promotional product company, which adds legitimacy to the email content. |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | The narrative presented in the email is highly NOT possible because the sender is claiming to be an FBI agent in an undercover operation. The request to use the recipient’s email for sending critical intelligence is a big red flag. This is a typical scam tactic where the scammer pretends to be in a position of authority or in a desperate situation to gain access to personal accounts or information. |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | The email is a conversation between colleagues with a focus on work-related matters. The email addresses and content are consistent with the ANZ organization, and there are no suspicious requests or links. The language is professional, and the details mentioned are specific to their professional activities, which is what one would expect from legitimate internal communication. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | The email uses a recognizable advertising slogan in a context that is unrelated to the service being promoted. This is a common phishing technique. The inclusion of a non-secure link (indicated by "hxxp") is intended to bypass security measures and suggests malicious intent. There is also a lack of personalization and specific details which makes the email seem generic and untrustworthy. |