|  |
| --- |
|  |

**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** |
| This email is safe | According to me,   * It is safe as the user Velma Khan is replying to the question asked by the user Adam John regarding the new trailer of Gamescon. * Normal Conversation. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| This email is Malicious | According to me,   * First check the link at virustotal.com for its behaviour. * Then,First of all the email is received from a source named Venture.ru which belongs to russian origin. * And the name venture is not justified as it should be from customer support or office 365 rather than venture. * And the subject of Action Required will make the person see it in a haste and would feel a sense if urgency. * The whole content is irrelevant and seems very unprofessional from such a reputed company as it says UPDATE YOUR ACCOUNT to receive large files which is very suspicious. |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| This email is Malicious | According to me,   * First of all, if a person is not able to login he will not ask some other person to login on behalf of him to check if he is able to login or not which makes it very suspicious. * If you look closely, the link provided is very suspicious as the word name faceBook consist of a suspicious B which makes it malicious. |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| This email is Safe | According to me,   * The email is forwarded by user named Adam Markus. * It contains advertising of a product. |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| This email is Malicious | According to me,   * First of all,any undercover agent would not tell his identity for whatever reason to a unidentified person or a civillian. * The email looks generous and professional but suspicious too. * An agent is asking for your email access rather than contacting their team. * This kind of emails are made very specifically which is also known as spear phishing which are made to some selected candidates who have a patriotic background. |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| This email is Safe | According to me,   * This email looks very professional and relevant as no media and link is attached to the email. * It’s a normal conversation between a employee and a employer. * The email consists of a ANZ company logo which makes it more authentic email. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| This email is without a doubt Malicious | According to me,   * The email is very suspicious because of its subject and content as there is only one link to switch to geico but with no info about company with the link. * First of all, we will see the link in virus total for its authenticity but if we see it closely we can clearly see that the link starts with hxxp rather than http which makes it for sure malicious. * This email is a type of AD phishing type of mail. |