|  |
| --- |
|  |

**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 | * It appears to be safe because there are no suspicious links present in the email. * It appears to be a normal conversation between two people. * The email names are not suspicious. * There are enough indicators to tell it is safe. * Since it is a normal conversation between two people without demanding/convincing for money,it is safe.. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The email is not at all professional. * There is no logo of the onedrive or office365,which is enough to say it’s not safe/malicious. * The email sender is convincing to click on the link. * The name of the email isn’t consistent with the display name. * There is no customer support number too. * There are spelling mistakes in the email which makes it non-professional.. |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The URL is fake. * The email sender is convincing to click on the link. * That appears to be a phishing email. * This type of email is a common form of social engineering. |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| safe | * This appears to be a profeesional one. * The email consists of full details of the product. * There are enough indicators to tell it is safe. |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| malicious | * The email sender is convincing the receiver to share the critical intel which is unsafe for receiver. * There are enough indicators to state its unsafe/malicious. * The email is not professional. * FBI won’t share details through email. |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * It appears to be a complete professional email. * There’s a professional logo. * The email name appears to be professional and legal. * Address is also mentioned in the email. * Email writing is complete professional. * There are enough indicatiors to tell it is safe. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The URL is fake. * The email is not professional. * The email name is appears to be a fake name. * The url is appears to a malicious link. |