|  |
| --- |
|  |

**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 | * From my analysis i can probably say that this email is safe to the it has been sended to. * This mail didn't have any suspicious link,file,etc. * This email also didn't have any ads, website link,downloadable file,etc. * This email looks like an conversation of two friends. * The sender of email (friend-1) is asking about if the friend-2 has seen the trailer of an game. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicius | * Probalby this is a malicious email. * This message suggest the person to kindly update the email address in microsoft office-365. * This mail does not looks like officialy mail from the microsoft company of from office * Although the sender is not the microsoft company. * It gives a link to another website to update the email address. |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * This mail also looks like an malicious email. * This email tells us that facebook server is down. * And gives us the link or we can say an malicious website link to check wheater the facebook server is down or not. * And in this link there is [https://www.faceBook.com](https://www.facebook.com/) * instead oh [https://www.facebook.com](https://www.facebook.com/) |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * This looks an suggestion of a friend to another friend. * This is an forwarded message from one friend to another. * In this there is an suggetion to buy gaming headset. * This email doesn't have any suspicious link. * Conversation email of friends. |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * This mail also looks like an malicious email. * The sender tells to reciever that he's an FBI undercover agent andh he's original email account has some problem. * He says that he urgently wants to send and urgent information to FBI some urgent information relaated to intel. * He says that he wants to access your email to sent this urgent information to FBI before it's too late. |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * From my analysis i can say that this email is safe. * It looks like an official email from an company employee. * This is also company email address. * It also have anz company's official logo. * This looks like an coversation between two company employees of same company who can use company's email address. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * This email is an malicious phising email. * This email tells the reciever that he has an opportunity to save up to 15% in buying an car insurance. * Further this phising email have an link to an malicious website. * You should'nt click any of the link like this. * The link have http protocol instead to https which is extremly insure. * The name of sender and a greeter is also different. * This type of email can steal your account credentials. |