|  |
| --- |
|  |

**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 | * You initiated the conversation. * The sender is a friend replying to a question that you asked. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The name of the sender is not from Microsoft * The sender wants you to urgently update your account by using a link that they sent. * The email is not professional |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The sender could’ve contacted you by phone to ask if Facebook was not working to get a quicker response. * The url is suspicious. * You do not need a url from an email to login to Facebook. |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * The email was forwarded from a friend * The email is an advertisement for a product * The email is very professional |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The email is from an “undercover” FBI agent in Uganda * The agent is asking you to send a critical email when you are not a part of the FBI * The user is asking for your account’s login information * The email tries to instill a sense of urgency and dread |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * This email comes from a coworker at ANZ that you have spoken with previously. * You initiated the conversation. * The email is professional. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The email is not professional * The name “Mike Ferris” isn’t consistent with the display name * The email contains a link with no description of what it contains. |