|  |
| --- |
|  |

**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 just a simple conversation between two people about Games Con. The email account is just a gmail account. The context of the conversation is about trailers for new games coming out. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | First indicator to me is that it comes from a TLD of ru which is Russian in origin.  It’s telling the user that they have a new file to be viewed in OneDrive.  It is asking the user to click a link and update the account so that they could receive large files from their contacts through Adobe PDF.  It is signed as Customer support from Office365 but the sender is Venture.ru |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | This is a typical phishing email.  It is asking the user if facebook is working, asking the user to login and see.  They provide the Url for the login page.  The url is not the typical login url for facebook. It has a special “B” character and is using a capital “B” in the url. |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | It appears to be a promotional email that is forwarded from users with gmail accounts  It may contain affiliate links, but no harm. |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | The email says that they are an FBI Agent undercover.  They are asking to access the users account to send higly classified information back to Headquarters  But at the end of the email, it is signed by the same person now refering to themselves as the superintendent of the FBI |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | It appears to be a work conversation between a Security Analyst and a Trainee  Typical conversation, there is asking for coffee, and for a zip file. The Trainee responds back that no to coffee and the zip file is not ready yet.  There is nothing supicious about the emails, they look like typical coporate emails.  There is also no links to click, nothing to download, and no typos |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | It is advertised as Geico. But it’s sender is from Val.kill.ma  The url looks really suspicous. I would not click it.  The email only contains a url, they might have already been a victim because it is a receipt. |