|  |
| --- |
|  |

**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** |
| Benign | * It seems normal conversation between two people * No suspicous links attached * Email address also seems fine for non-formal uses |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * First and formost if it’s from one drive name should be of something related to Microsoft * Venture.ru – Indicates russian origin * There are grammatical mistakes * Files attached with adobe pdf can execute in backgorund if Pdf files is executed * The concern for updating Email address is unnecessary |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * Link can be observerd - characters that look similar to English letters but have different Unicode standards, ex – cycrilic letters used to create visually similar text * Root domain is different – “.com.opt” |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Benign | * Researching for the same it’s valid info tha Drop fromerly known as Massdrop * It’s community – driven ecommerce website * Drop uses data and insights from community to develop and find products that feed their interests in audio products and mechanical keyboards |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * There should be definitely other secure and lawful procedure under any failure circumstances in government agencies like FBI * There no proof that request made is genuine * Also it’s saying to give access to email address account which can be used for illegal purposes |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Benign | * Email address are well aligned with name also ‘@anz.com’ shows it’s coming from genuine mail servers * Nowadays source are checked with help of SPF, DKIM and DMARC * ANZ logo seems original * No links were attached just normal conversation |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * Link provided is “http” which provides no certifcate proof, thus not a trustworthy source * Name not aligns with email * “.php links” can execute commands and download malicios executable files |