|  |
| --- |
|  |

**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 | * This appears to be a trailer-related discussion over email. * There are no malicious links provided in the email. * The email of Adam is of the form [name@domain.com](mailto:name@domain.com), and the domain here is “gmail.com” which is correctly spelled.   These are person-to-person emails, and Gmail is known to mark such emails as “important” |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * If this was indeed a OneDrive action email, the email would have been received from Microsoft, and not Venture.ru * .ru indicates that this email is from Russia * The word “OneDrive..” appears to be a hyperlink, it appears at the start of the email with no context, which feels suspicious. * Spelling and grammar errors in the next few lines “Please keep your Office 365 E-mail address update so you can continue to recevie large file” * Yet another link to supposedly update the account to sign up and enable receiving large files from Adobe. The link is suspicious, and the context is confusing – Microsoft is ideally clear with the requirements and details about it. * Random words are written in caps. “ADOBE”, “SECURITY” * “Office365” precedes the thank you note. Unclear context. * Spelling error at the end “Customers Support.” * The email is written unprofessionally and has no company disclaimer. |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * Appears person-to-person email, marked important by Gmail. * The link has a special character. “Facebook” is spelled incorrectly * The link says [https://www.faceβook.com**.opt**](https://www.faceβook.com.opt). Here, “.opt” also indicates that this could be a malicious email. |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Potentially malicious | * The email is an ad, which contains a link disguised as “see more” * The sender Adam appears to have forwarded this email from [info@i.massdrop.com](mailto:info@i.massdrop.com) with no context. This could have been forwarded manually by Adam or could have been forwarded via an email worm. * The sender has the name “Adam Markus” but has the email [Aman.zoom@gmail.com](mailto:Aman.zoom@gmail.com), which does not correlate with the name. * The “See more” link could be malicious. |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The information provides sounds like a fictitious fairy tale story, which is untrustable. * The email asks to share account details – account ID and password. This can be used with malicious intent. * There are no malicious links in this email, so in itself the email is passive, but sending details can be dangerous. |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * This is an email conversation between two employees of the organization ANZ. * The details of the employees and the company logo are provided. There is a certain level of professional etiquette followed. * There is no zip file shared yet (which could contain potential malware), so in itself, these emails are safe. * There are no personal details requested during the discussion. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The title indicates that this could be an ad, but it's marked important by Google, this could be a person-to-person email. * The sender’s ID is Val.kill.ma : The email appears to be sent from Morocco. Additionally, this does not indicate a reputable company name. * The URL is potentially dangerous – hxxp : It appears to be an unrecognized protocol, the domain is iwhrhwicy.urlif.y – which is an unrecognizable company, and this is a PHP file. Php files are known to be used to perform injection attacks, Session Management attacks, XSS attacks, etc. * There is no context provided in the body, which makes the email more suspicious. |