|  |
| --- |
|  |

**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.**

**Email 1:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * The topic of conversation is quite niche and is directed to someone who seemingly already has a rapport with the sender. * The lack of attachments or links to click on, aswell as the friendly/casual conversation seem to indicate that this is merely a conversation between friends at this point. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The email is from a russian email address. * The subject of the email is about OneDrive, and the sender seems to be trying to impersonate OneDrive, however, the senders name is ‘Venture.ru’ which is a domain that does not seem to be under OneDrive’s purview * There are spelling errors in the email. Generally an email of this nature would be auto generated, which means it would have had to have been vetted first to ensure there were no spelling errors like this. * The email is not personalised. Generally in emails of this nature, the way for the reciever to ensure that the email is for them would be through the email directy addressing them, for example starting the email with a “Dear (username)” |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The link to facebook is not an official one. You can tell this by the stylized ‘B’ in Facebook, aswell as the .opt domain, which is not a domain associated with facebook. |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * The original email from “massdrop” seems to be from an official email address. I ascertained this from the email domain being “massdrop.com” * The syntax of the email seems to be well put together, including photographs and a write up of the item that is being sold. * While these points may make this email seem authentic, it is always better to treat every email with a certain layer of safety. If the attached product is something that was of interest to the reciever, I would recommend they use a search engine to access the massdrop site, and from there they will be able to ascertain whether massdrop is a vendor who the reciever would trust to do business with. |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * Superintendent Vincent fails to verify his credentials. * It is unlikely a scenario like this would happen in the real world. * The reciever must first wonder “why me?” as there are many official CIA emails, why would this sender need the details of your personal email account? |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * Both the sender and reciever are using official ANZ email addresses. * This snapshot seems to be a small part of a larger email chain with an ongoing conversation. This suggests that both parties in this conversation know each other, and are colleagues. * The work discussion also contains a side note on a different matter, which means that the email is personalised and we know for sure that the email from the reciever is intended for the sender as it is a conversation directly relevant to the relationship of this two people. * With this email chain containing only 2 people, we can ensure that nobody outside of the inteded purview will be able to access the zip file that will be eventually sent. This ensures that the file can only be accessed by the intended audience of this file. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The Subject of the email refers to Geico as the insurance provider, however the link provided is suspicious as there is no discernable names in the link, if the attached line that looks like a web address is even a web address at all. * The lack of personalization is another thing to look out for. Why is the Sender named “Val.kill.ma?” Notice the lack of body in the message. A large insurance provider like Geico would have a better designed advertisment that would contain more information than a faulty web address and a signature from a ‘Mike Ferris” |