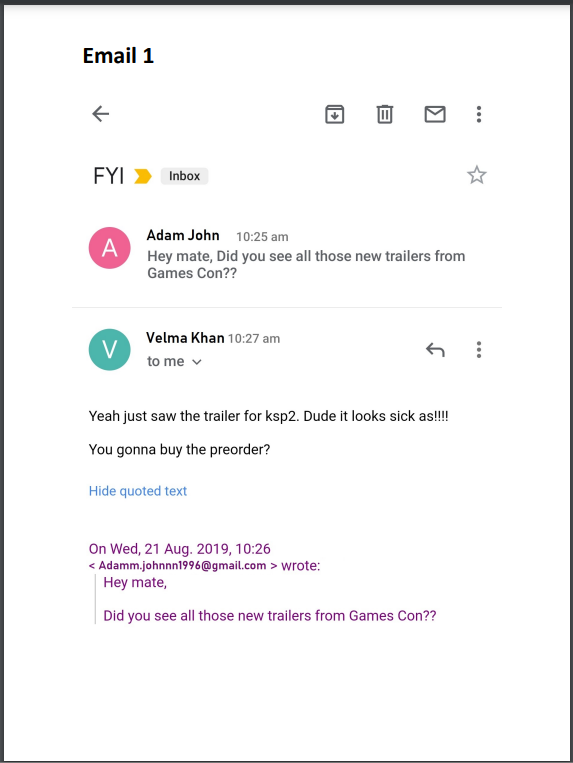
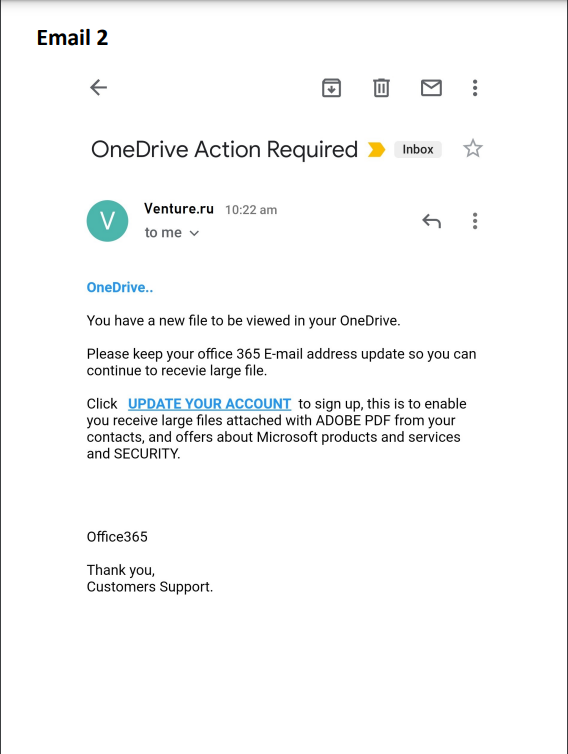
|  |
| --- |
|  |

**Email 1:**

****

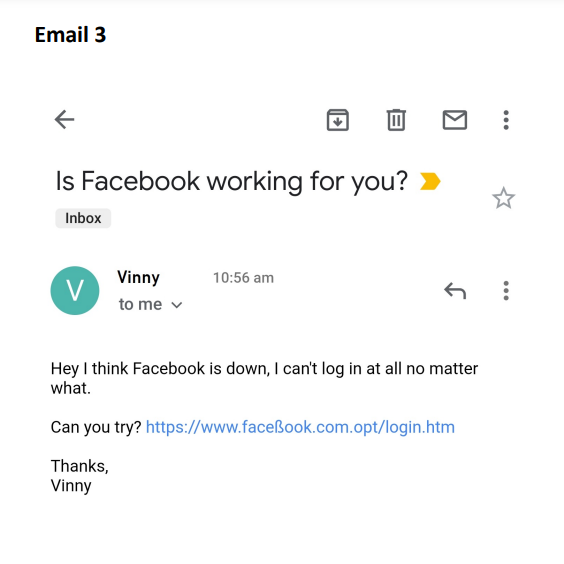
|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * The sender is a known acquaintance to the reciever. * This email is not malicious or spam email. * It depicts a typical conversation between two individuals who happen to be friends. * It contains no dangerous artifacts or potential risk factor. * Given the time and date, it is possible that the conversation was expected given how quickly the response is given. * It's obvious that it's not spam because the reply mentions a previous relationship and implies that the email was appreciated and expected. |

**Email 2:**

****

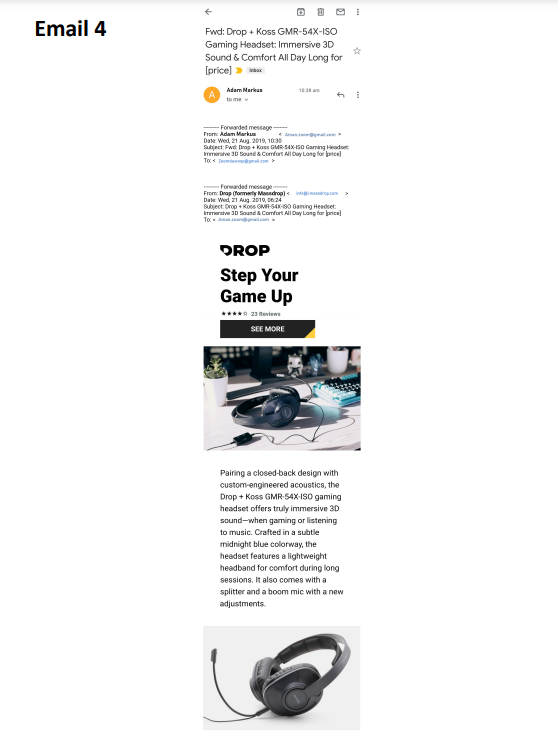
|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The email is sent using a russian domain. * The email sender is requesting the receiver to update its OneDrive account. * The email sender falsely claim to be sent by OneDrive while domain header tells it is sent by Venture.ru. * The email contains grammatical errors. * The email format is unprofessional. * The sender demands the user to download files without any context of file’s content * The undersigned is unprofessionally quoted as Office365. * This is enough indicators for us to assume that the link is probably safe and should be treated as such*.* |

**Email 3:**



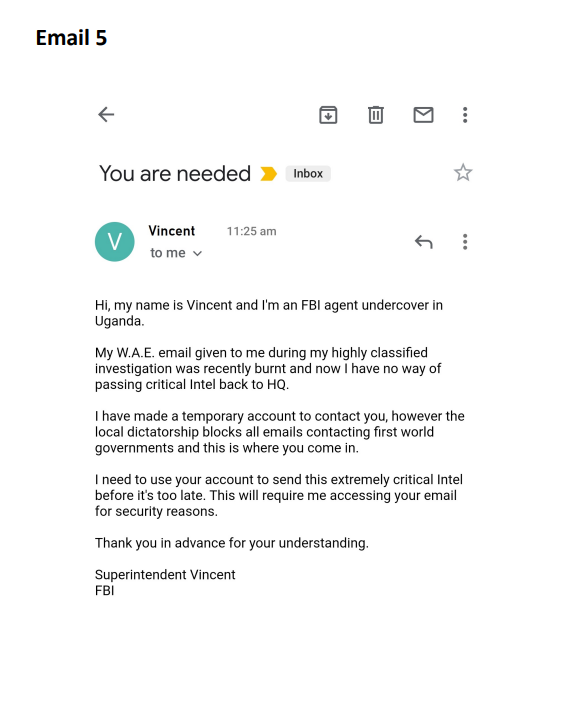
|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The striking feature of this email which makes it suspicious at first sight is the wrong spelling of facebook * This is a suspected phishing link to gather confidential credential of the reciever. * The email is masqueraded coming from a known acquaintance telling the receiver to verify if the facebook is working for them. * This is enough indicators for us to assume that the email is probably malicious and should be treated as such. |

**Email 4:**

****

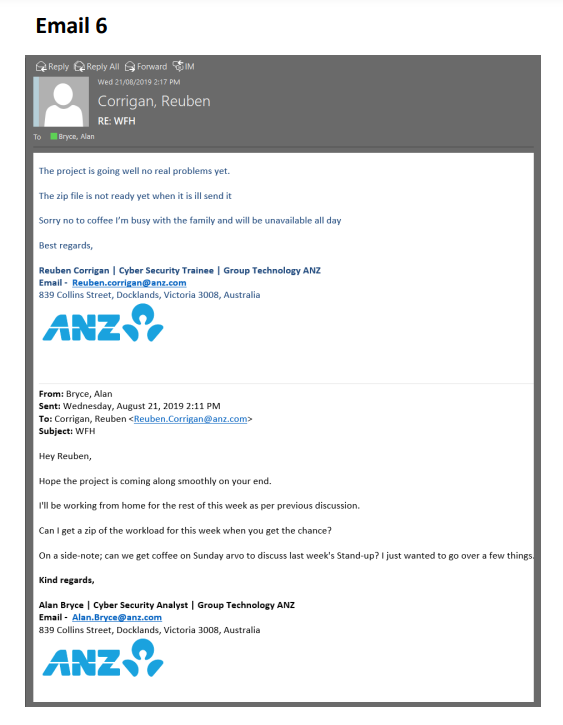
|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * This email is an example of generic marketing. * It can be categorised as a non-malicious spam email. * Although it was twice forwarded, the initial sender was a mass mailing service. * The email has no links or requests for information. * When googled, the site may be seen as a sales site without any dangerous material. * This is enough indicators for us to assume that the email is probably safe and should be treated as such. |

**Email 5:**



|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * Overall the email is unprofessionally written. * It demands the user to provide its sensitive information of the receiver such as its email credentials. * This is enough indicators for us to assume that the email is probably malicious and should be treated as such. * Finally the email tries to instill a sense of urgency and dread by stating that the sender requires the recievers credentials in order to provide the government with confidential intel. |

**Email 6:**

****

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * The email is safe and non-malicious. * It is a typical workplace email. * The email does not demand the reciever to download any files or enter any confidential credentials. * The email is an organizational email as it use anz.com domain. * Internal work emails can be trusted to be safe. * The email is written professionally. * This is enough indicators for us to assume that the email is probably malicious and should be treated as such. |

**Email 7:**

****

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * This email can be categorised as a phishing email. * It uses hxxp which is an indicator that it is a malicious link as any organisation would use HTTPS for carrying out trabsanctions. * It also contains a PHP file i.e. receipt.php which is another indicator that it is a fake reciept generated to carry out phishing attack. * The email sender (Val.kill.ma) and the undersigned (email signature: Mike Ferris) does not match. * The email sender falsely claim to be from Geico but it does not uses an official domain of Geico Insurance. |