**Email 1:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * Adam John sent his email during time: 10:25am, but Velma Khan’s email states 10:26 * Email: [Adamm.johnnn1996@gmail.com](mailto:Adamm.johnnn1996@gmail.com) -> personal, conversation is friendly * Could be social engineering but not enough evidence to make a definitive judgment * However, there is no link or request to download a file * The email conversation itself has no method to conduct a cyber attack, it is simply a conversation between two people |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * Venture.ru is not related with Microsoft Office365 * Link attached, possible phishing attack * “…enable you receive large files” possible malware attached * Language is not professional or grammatically correct * No email signature from Microsoft |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The ‘b’ in Facebook is **ß**, incorrect domain name system (DNS) * Therefore, domain name will not direct user to the actual Facebook IP address but misdirect them to a malicious server * Link could be a phishing attack * Email is too short and colloquially written |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * Date: Wed, 21 Aug. 2019 (consistent) * Time: Massdrop (6:24) -> Adam Markus (10:30) -> Zoomdawoop (10:38) * Email: [info@i.massdrop.com](mailto:info@i.massdrop.com) -> [Aman.zoom@gmail.com](mailto:Aman.zoom@gmail.com) -> [Zoomdawoop@gmail.com](mailto:Zoomdawoop@gmail.com) * Content: consistent with advertised product (Koss GMR-54X-ISO Gamin Headset) * Warning: link to “SEE MORE” could be misdirect to IP Address with malicious content -> DNS spoofing? |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * An FBI would use better formatting * An “undercover” FBI agent contacting a user via e-mail is counter-intuitive * Why would Vincent send an email if “local dictatorship blocks all emails contacting…”, should be trained to understand the email may be traced by local dictator * Story is hard to believe * No verification for user’s identity * Unprofessionally written |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * No links that may be malicious * Name + Email: Alan Bryce and Reuben Corrigan matches ANZ work email * The conversation in email has nothing malicious * Time: Alan Bryce (2:11) -> Reuben Corrigan (2:17) * Date: Wednesday, August 21, 2019 (consistent) * Email signature: information is detailed, consistently formatted, professional appearance, address is present and consistent |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * Poorly formatted * Unprofessionally worded and presented * Link could be malicious (phishing) * “Cheers” -> colloquial * Mike Ferris does not match with email Val.kill.ma * Email’s too short for an advertisement * No email signature from Geico |