|  |
| --- |
|  |

**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* | 1. *This mail seems to be safe as this is reply to his mail.* 2. *There is no external URL or unsafe link attached to mail.* 3. *This is unofficial chat between two people.* |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | *1 . The sender of mail is Venture.ru not Microsoft and is from Russia.*   1. *The email sender is requesting the user update account by clicking on unknown link.* 2. *This is enough indicators for us to assume that the link is probably malicious and should be treated as such.* 3. *Overall the email is not very professional. It is far too generic using terms that could apply to almost anyone and anywhere such as “recevie” and and OneDrive.. . Also use of ADOBE any open sources product as support.* 4. *The name the email uses isn’t consistent with the display name i.e venture vs office365.* 5. *Insisting to update email otherwise will have to suffer from loss of large files seems to create urgency to update email address. This is a common form of social engineering.* |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| *Malicious* | 1. *Not looks like a formal or official mailer.* 2. *Phishing attack through a URL with b replaced with beta symbol and similar looking Facebook login page .So user easily believe and enter his/her credentials.* 3. *Seems to be a unprofessional mail.* 4. *Making user to give a try on link.* |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| *Malicious* | 1. *First of all it’s a forwarded message.* 2. *It’s giving temptation to click on external link to see more about product .* 3. *Price is not mentioned in mail so user gives a try to see more and may land into trouble.* |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| *Malicious* | 1. *It seems to be malicious because why will a FBI agent send critical Intel from outsiders mail.* 2. *Why would he /she disclose his/her identity to anyone.* 3. *The same way he/she can mail to Headquarters i.e from newly created account.* |

***Email 6:***

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| *Safe* | 1. *This mail seems to be normal work mail between two team members of a project and their seems no suspicious thing in mail.* |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| **Malicious** | 1. *Sender name is highly unprofessional and doesn’t seems to be a insurance company.* 2. *URL attached with mail is suspicious.* 3. *Hxxp is not an official protocol.* 4. *Nothing except URL to unknown site.* |