|  |
| --- |
|  |



**Email 1:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * The email seems to be from a personal aquaintance. * There’s no suspicious links attached. * The email is personal rather than professional. Since the 2nd user responded in a casual way, it seems like the 2nd person knew the 1st person already. * The email address is similar to the User name. * There is no sense of urgency or no sign of asking any sort of information or credentials from the user. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The subject line demonstrates some sense of urgency. * The email address is not verified. It is not of Microsoft origin or work related email address. Email address domain- Russian. * The first line of email is a hyper-link. The hyperlink does not seem to be legitimate. * The context of the email doesn’t seem to be professional. Furthermore, no such emails are usually sent from OneDrive. * The grammar of the content in the email is not proper (Unprofessional). * Before signing up, the email is asking to ‘Update Account’ and also unless the person is a Onedrive user, he’s not supposed to get such mails. * ‘ADOBE PDF’ & ‘SECURITY’ are written in block letters, which doesn’t look legitimate. * No proper designation of the sender and also, it is mentioning Customer’s’ Support. * Clearly an attempt of social engineering. |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * This email should be sent to a facebook customer support executive. * The subject line creates suspicion. * The sender does not necessarily nedd to have send the URL of facebook. * The link provided in the email is a pharming link. The letter ‘b’ of facebook semms to be written in cyrilic or similar script which look similar but has a different ASCII value. * The other user (Vinny) is trying his luck on Social engineering or email phishing precisely. |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * The email is from a verifid domain. * Does not ask any credentials * No sense of urgency noticed * Follow the SET best practises as a precaution. * The designation of sender is missing |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * Subject line itself gives a fake impression * FBI agents, especially undercover agents never send such mails. * Asking for credentials or account of the victim. * Creating a sense of urgency * No supporting document to prove his identity * Email does not hold up a professional structue. |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * This email is a revert back from the recepient * All proper designations have been mentioned. * Used company verified email domain and company logo with appropriate details (viz. address) * Although seems personal, the mail seems safe. * Does not ask for any personal information. * Might be a chance of impersonation, SET best practises advised. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * Mail seem to be a marketing gimmick * The username of the sender is suspicious. * No content in the mail to elaborate the subject line. * The URL mentioned does not have ‘https’. * Clearly high chance of Social Engineering. |

Email Social Engineering Analysis done by:

Amith P V

https://www.linkedin.com/in/amithpv1/