|  |
| --- |
|  |

**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.**

**Here is an example to use as a reference point:**

A screenshot of a social media post

Description automatically generated

**Email 1:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * The email sender looks legitimate * There are no links * There are no attachements * The sender is not trying to make the user click on a link or download a file. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The email sender states its from onedrive but message sender email is venture.ru * The email is prompting the user to click on a link * There is a sort of important urgency to make the user update his account or else he will not receive big files |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * *The email sender is requesting the user to click on a link.* * *Overall the email is not very professional. It is far too generic using terms that could apply to almost anyone and anywhere such as “Hey” “No matter what” and the title of “Is Facebook Working for you”.* * *The name the email uses isn’t consistent with the display name.*   *Finally the email tries to instill a sense of urgency and dread by mentioning that the person’s account is not available to him and he is unable to log in. This is a common form of social engineering.* |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * Forwarded Multiple Times: The presence of multiple "Forwarded message" headers suggests the email has been passed through several accounts. While not inherently malicious, this can be a tactic used to obscure the original sender and make the email seem less suspicious. * Generic Subject Line with "[price]": The subject "Fwd: Drop + Koss GMR-54X-ISO Gaming Headset: Immersive 3D Sound & Comfort All Day Long for [price]" is oddly formatted with the bracketed "[price]". Legitimate marketing emails usually include the actual price. This placeholder suggests a template or a poorly constructed email, which can be a red flag. * Inconsistencies in Forwarded Headers: While not clearly visible, if you were to examine the "From," "Date," and "To" fields in each forwarded header, inconsistencies or unfamiliar email addresses could indicate tampering or that the email originated from a suspicious source. * "DROP Step Your Game Up" Advertisement: The inclusion of an advertisement for "DROP" within a forwarded email is unusual. Legitimate forwards typically don't embed promotional material like this. This suggests the email might have been injected with this content. * "SEE MORE" Button: Buttons like "SEE MORE" in unsolicited emails can lead to phishing websites designed to steal your credentials or install malware. Without knowing where this button leads, it's a potential risk. * \* Unsolicited Nature: You haven't indicated that you subscribed to marketing emails from "DROP" or were expecting this specific promotion. Unsolicited emails, especially those with unusual formatting or calls to action, should be treated with caution. |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | Implausible Scenario: An FBI agent, especially one undercover in a foreign country like Uganda, would never contact a random individual via email asking for access to their personal account to send "extremely critical Intel." This is not how law enforcement operates. Their communication methods for sensitive information are highly secure and would not involve using a civilian's email.  \* Generic Greeting: The email starts with a very generic "Hi, my name is Vincent..." This lacks any personalization and is typical of mass-distributed scam emails.  \* Suspicious Claim of Burned Email: The story about his "W.A.E. email" being "recently burnt" during a "highly classified investigation" and now needing to use your account is a fabricated and highly improbable scenario designed to create a sense of urgency and desperation.   * Claim of Local Dictatorship Blocking Emails: The excuse that the "local dictatorship blocks all emails contacting first Implausible Scenario: An FBI agent, especially one undercover in a foreign country like Uganda, would never contact a random individual via email asking for access to their personal account to send "extremely critical Intel." This is not how law enforcement operates. Their communication methods for sensitive information are highly secure and would not involve using a civilian's email.. * Generic Greeting: The email starts with a very generic "Hi, my name is Vincent..." This lacks any personalization and is typical of mass-distributed scam emails. * Suspicious Claim of Burned Email: The story about his "W.A.E. email" being "recently burnt" during a "highly classified investigation" and now needing to use your account is a fabricated and highly improbable scenario designed to create a sense of urgency and desperation. * Claim of Local Dictatorship Blocking Emails: The excuse that the "local dictatorship blocks all emails contacting first world governments" is a common trope used in these types of scams to explain why he can't use official channels. It's designed to sound dramatic but is highly unlikely. * Request for Account Access: The core request – needing to "use your account to send extremely critical Intel" and requiring "accessing your email for security reasons" – is a massive red flag. Granting anyone access to your email account would compromise your privacy and security and could lead to identity theft, financial fraud, and more. * Claimed Title and Affiliation: Identifying as "Superintendent Vincent, FBI" in a simple email is not a standard or secure way for an FBI agent to identify themselves, especially when making such an unusual request. Real FBI communication would follow strict protocols and use official channels. * \* Sense of Urgency: The phrase "before it's too late" is a common tactic used in scams to pressure recipients into acting quickly without thinking critically. * In short, this email hits almost every red flag for an online scam. It's trying to exploit your trust and curiosity with a far-fetched story to gain access to your email account, likely for malicious purposes. * What you should do immediately: * Do not reply to this email. * Do not click on any links or provide any information. * Mark this email as spam or junk. * Delete the email immediately. * Be wary of any future emails with similar stories or requests |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * Its just project based talk * The email sender looks legitimate * There are no links * There are no attachements * The sender is not trying to make the user click on a link or download a file. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * *The email sender is requesting the user to click on a link.* * The tone is not professional. * The sender is exploiting human greed. * Definetly a suspicious and should never be open using the link. |