|  |
| --- |
|  |

**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

***Example Answer*** *(Please note this is not part of the Task and is an example only. Please remove this section from your task submission):*

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * *The attached URL is from Russia.* * *The email sender is requesting the user download a file with fairly generic justification.* * *This is enough indicators for us to assume that the link is probably malicious and should be treated as such.* * *Overall the email is not very professional. It is far too generic using terms that could apply to almost anyone and anywhere such as “the report” and the job title of “anz employee”. Also ‘anz’ is not capitalized, and the email provided is not a business email.* * *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 job is on the line, and mentioning their bosses to provide some sort of authority to what they are saying. This is a common form of social engineering.* |

A screenshot of a chat

Description automatically generated

**Email 1:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * **Casual tone:** This email exchange has an informal tone, indicating it's likely between friends or colleagues discussing shared interests in gaming. * **Sender and recipients:** The conversation involves a back-and-forth between Adam and Velma, with a reference to the trailers and preorders for a game. * **Context:** The focus of the discussion revolves around new game trailers from Games Con, an annual gaming event, and Velma's interest in pre-ordering the game. * There don't appear to be any immediate indicators of malicious intent, based on the information shown. |

A screenshot of a email

Description automatically generated

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| malicious | * **Suspicious Sender Email (Venture.ru):** The email is from a domain ending in .ru, which is associated with Russia. Microsoft or OneDrive communications should come from official Microsoft domains like microsoft.com or office.com, not third-party or foreign domains. * **Poor Grammar and Spelling:** There are multiple grammatical errors, such as "recevie" instead of "receive" and "E-mail address update" instead of "updated." Professional emails from Microsoft are usually well-written and error-free. * **Unprofessional Formatting:** The email uses inconsistent capitalization, such as "Office365" and "Customers Support," which is unprofessional and uncharacteristic of legitimate companies. * **Urgent Call to Action (Social Engineering):** The email uses an urgent call to action with phrases like "Action Required" and asks the user to click a link to "UPDATE YOUR ACCOUNT." This is a classic phishing tactic to trick the user into clicking a malicious link. * **Unverified Link:** The "UPDATE YOUR ACCOUNT" link is likely malicious. Always hover over links in emails to verify the destination before clicking, especially when it involves sensitive accounts like OneDrive or Office 365. |

A screenshot of a computer

Description automatically generated

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * **Suspicious URL:** The URL provided in the email is "**https://www.faceßook.com.opt/login.htm**".Notice that "**faceßook**" uses a "**ß**" instead of a regular "**b**", which is a common trick used by attackers to make a fake URL look legitimate.The ".opt" subdomain is also suspicious, as legitimate Facebook URLs would use ".com" or ".fb.com". * **Casual Language and Urgency**: The sender, "Vinny", asks if Facebook is working for you and immediately provides a link. This could make the recipient feel inclined to click the link without verifying it first, exploiting urgency and trust. * **Phishing Setup:** The link is likely designed to lead to a fake login page to harvest your Facebook login credentials. Once entered, attackers could gain access to your Facebook account. |

A screenshot of a cell phone

Description automatically generated

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * This email appears to be a genuine product promotion or advertisement for a gaming headset. * This email doesn't ask for login credentials or direct the recipient to suspicious websites, which reduces the likelihood of phishing. |

A screenshot of a email

Description automatically generated

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * **Unrealistic Story:** The sender claims to be an undercover FBI agent in Uganda, which is highly unlikely. Government agencies like the FBI would never use random personal accounts to contact civilians for confidential matters. * **Urgent and Unusual Request:** The email asks the recipient to allow access to their email account to send "***critical Intel*.**" Legitimate government agencies would never ask individuals to hand over their email credentials, as this violates standard security protocols. * **Poor Grammar and Structure:** There are grammar mistakes and awkward phrasing, such as "***passing critical Intel back to HQ***" and "***my W.A.E. email was recently burnt***." Official communications from government agencies would be professionally written and free of such errors. * **Vague Terms:** Terms like "***local dictatorship***" and "***W.A.E. email***" are vague and meant to add urgency or intrigue, which is a common tactic in phishing scams. * **Request for Personal Information:** Asking for access to your email account is a major red flag. Scammers often try to gain access to personal accounts to steal sensitive information or commit further fraud. |

A screenshot of a chat

Description automatically generated

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * **Legitimate Correspondence:** The email contains what looks like a genuine conversation between Reuben Corrigan (Cyber Security Trainee) and Alan Bryce (Cyber Security Analyst), both seemingly working for ANZ Group Technology. The email content focuses on project updates, a zip file, and informal plans for a coffee meeting. * **Email Addresses**: Both email addresses use the @anz.com domain, which corresponds to ANZ (Australia and New Zealand Banking Group), a legitimate organization. This is a good indicator that the emails are internal communications. * **No Immediate Red Flags:** There's no sense of urgency, unexpected attachments, or suspicious links that typically accompany phishing or malicious emails. * Reuben mentions he will send the zip file once it is ready, which is a standard working practice. |

**A screenshot of a email

Description automatically generated**

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * **Suspicious Sender (Val.kill.ma):** The email address looks suspicious and doesn’t correspond to a legitimate business or entity. Random email addresses like this are often used by scammers to avoid detection. * **Untrustworthy Link**: The URL in the email, ***hxxp://iwhrhwicy.urlif.y/receipt.php***, is a clear attempt at hiding a malicious link by altering the typical "***http***" protocol to "***hxxp.***" This is a common trick to avoid automatic filters. * The domain urlif.y also looks strange and untrustworthy, which adds to the suspicion that this is a phishing link designed to steal personal information. * **Generic Message:** The message claims you can save on car insurance by switching to Geico, which is a common and well-known company, but the email is far too generic for it to be legitimate. Major companies don’t send unprofessional emails with unverified links like this. * **Unknown Sender (Mike Ferris):** The name Mike Ferris seems randomly included and does not provide any assurance or context. There’s no legitimate contact information or verification of identity. |