|  |
| --- |
|  |

**Email 1:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | 1. The recipient knows the sender, which reduces the likelihood of the email being malicious. If the sender is trusted and known to the recipient, it's less likely that the email contains harmful content. 2. The conversation appears normal, and there are no suspicious links or spelling mistakes. Normal conversation patterns and absence of errors further support the email's safety. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | 1. The presence of a sense of urgency is a common tactic used by malicious actors to pressure recipients into taking immediate action without thoroughly considering the consequences. This urgency can indicate an attempt to manipulate the recipient into clicking on links or providing sensitive information hastily. 2. The account name mentioned in the email is irrelevant to the request or context of the email, it raises suspicion 3. Promising security or safety in exchange for clicking on links is a common tactic used in phishing emails. |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | 1. Spelling mistakes or unusual characters within a link can indicate an attempt to disguise a malicious URL |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | 1. If googled, the site can be seen as a sales site that contains no malicious content. 2. The email contains no links or requests for information, just pure advertising. |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Maliciois | 1. Emails that create a sense of urgency often aim to pressure the recipient into taking immediate action without thinking carefully. This urgency is a common tactic used by malicious actors to manipulate recipients into clicking on links or providing sensitive information hastily, before they have a chance to scrutinize the email properly. 2. Requests for access to accounts, especially without proper authentication or verification processes, are highly suspicious. |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | 1. The email pertains to a work-related conversation, indicating that it's likely part of normal business communication. 2. The absence of urgency in the email suggests that there's no pressure on the recipient to take immediate action. 3. The inclusion of employee tags and images further supports the legitimacy of the email. It indicates that the email is likely sent from within the organization and contains familiar elements that employees would recognize. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | 1. The presence of a random username, especially when combined with a link, strongly indicates a phishing attempt. 2. The use of a random username that is not associated with the legitimate sender, such as Geico in this case, is a common tactic used by phishing scammers. 3. The use of "hxxp" instead of "http" in the link is another indicator of a phishing attempt. Phishing scammers often manipulate URLs in this way to bypass email filters or to make the link appear less suspicious to recipients. |