|  |
| --- |
|  |

**We have provided two versions of the model answer for this task:**

**(1) A version using the task template; and**

**(2) An annotated version**

**Email 1:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * It’s clearly not spam as the reply indicates a previous relationship and that the email was expected and welcome. The date and time could indicate that the conversation was anticipated, as there is next to no delay in a reply. * This email is non malicious. It’s a typical conversation between friends and contains no potentially dangerous artefacts. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The email claims to be from one drive but the email sender is from a Russian domain which is well known for malicious emails. * The email tries to get the user to download a file, without providing information about the file’s content, or the sender. * The email’s format is unprofessional and contains poor grammar & spelling. Y * ou would not expect an email from an official Microsoft service to be formatted and presented like this. |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The email is presented as a question from a friend who cannot access Facebook, and asks the recipient to follow a link to see if Facebook is working for them. But the link provided is actually a phishing link make to look like facebook.com at first glance. * The senders account could be compromised, so a malicious email like this could still come from a trusted friends account. |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * This email is an example of generic marketing, it could be regarded as Spam (unwanted or unrequested marketing content). It’s been forwarded twice, but the original sender is a mass mail service. * If googled, the site can be seen as a sales site that contains no malicious content. * The email contains no links or requests for information, just pure advertising. |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The email is requesting the recipient’s credentials for unusual reasons. They’ve tried to make the issue seem urgent, which is a well-known persuasive technique often used for phishing. * The email lacks professionalism which gives more reason to believe it’s a fake. * Legitimate users/services would not ask for account details. This is almost always a sign of malicious activity. |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * This email is non malicious. It is a typical workplace email. There are no files, links or suspicious requests within the emails, and for the most part internal work emails can be trusted to be safe. * The senders email address matches the name on the signature, and appears to be well formatted and professional. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The email claims to be from Geico Insurance but the sender doesn’t have an official Geico email address, and the URL provided is not linked to Geico in any way. * The email sender claims to be someone called "Mike Ferris", but the display name of the sender is Val.kill.ma. * Legitimate companies would use HTTPS for any financial transactions. The link provided is just http, which is another indicator that this is a fake. HTTPS is secured and encrypted where as HTTP is not. |