Email 1:

Is this email Safe or Malicious?	My Analysis
Safe	• The email does not appear to be malicious. It presents a casual conversation between two individuals regarding game trailers from Games Con. • The email address is consistent with the provided name. Furthermore, the email provider being gmail suggests that Adam John used a personal email to contact Velma Khan. • Due to a personal email address being used and without more context, this could potentially be part of a more sophisticated phishing attempt whereby the sender is attempting to build rapport and build trust. However, this is extremely unlikely. • There are no suspicious indicators, i.e., the message contains no URLs, attachments, or suspicious requests.

Email 2:

Is this email Safe or Malicious?	My Analysis
Malicious	• The sender address contains the .ru (Russia) country code top-level domain (ccTLD). Whilst there are legitimate instances of this country code, they are often malicious and in this case, OneDrive will never send you an email originating from Russia. • The email subject also attempts to instill a sense of urgency by stating that an action is required. • The email provides a generalised greeting, this is often observed in phishing attempts. In this instance, the supposed OneDrive email does not reference the user by name. • The email body contains several gramatical errors, which suggests that this email was composed by a non-native english speaker, or was fed through a language translate tool. • All these indicators are more than enough to label the email as malicious, even without access to the URL or other indicators.

Email 3:

Is this email Safe or Malicious?	My Analysis

Malicious	• The primary indicator of this email being malicious can be observed within the provided URL. There appears to be a special character that replaces the b in facebook.com. This is known as a homograph attack whereby a threat actor uses special character sets or alphabets to impersonate a legitimate domain. • The sender composed the email to appear casual, likely to try and catch the reciever off guard. Furthermore, making a request for someone to visit a URL is often malicious. • The URI pointing to /login.htm immediately suggests that this is a credential harvesting attempt. In this case, the threat actor is clearly attempting to steal the recipients facebook credentials. • All the indicators lead me to the conclusion that this is a credential harvesting phishing email.

Email 4:

Is this email Safe or Malicious?	My Analysis
Safe	• The email appears to be a forwarded marketing email from Drop. The address info@i.massdrop,com is consistent with Drop's marketing infrastructure. It returns no malicious results on threat intelligence sources like Cisco Talos. • The only call to action within this email is the "SEE MORE" button. Without access to the raw email, I cannot determine where this button links to, and if the URL is legitimate. • There are no grammatical errors or any other indicators that suggest this email as being malicious, therefore, it is likely safe.

Email 5:

Is this email Safe or Malicious?	My Analysis
Malicious	• This email is a blatant social engineering attempt, similar to that of a Nigerian-style 419 scam, posing as an FBI agent to exploit trust and gather the users email credentials. • The FBI would never contact a user making such a request. This is a clear attempt at exploiting authority to try and coerce the user into helping, all under the guise of national security.

Email 6:

Is this email Safe or Malicious?	My Analysis
Safe	• This email thread appears legitimate and reflects normal internal communication between a cyber security trainee and a cyber security analyst at ANZ.

	• All email addresses used are from the legitimate ANZ domain, although without the raw email file I can't determine if the email was spoofed. • There are no URLs or attachments contained within this thread, only mention of a ZIP file. Whilst password protected ZIP files are often used as a means of delivering malware, this thread shows no such intent.

Email 7:

Is this email Safe or Malicious?	My Analysis
Malicious	• This email contains an extremely suspicous defanged URL. This is likely to avoid link detection by the email gateway. • urlif.y is a non-standard domain, and has no association with Geico. • The URI pointing to /receipt.php is not consistent with the email body. The email is disguised as a promotional message for 15% off car insurance, therefore it makes no sense to provide a link that points to receipt.php. • The email ID Val.kill.ma does not appear to be a legitimate Geico email. • All these indicators suggest that this is a phishing attempt, although the intent (i.e., credential harvesting, etc) is unknown.