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.

Email 1:

Is this email Safe or Malicious?	My Analysis
Safe	• No attachments • The email seems to be just a casual conversation between friends • No indicator of a malicious email

Email 2:

Is this email Safe or Malicious?	My Analysis
Malicious	• No formal greeting including the name of the customer • There are inconsistencies in the email such as wrong spellings, additional spaces in the paragraph and incorrect grammar • Sender's email is not related to Office365 • The URL could potentially redirect to malicious websites or files

Email 3:

Is this email Safe or Malicious?	My Analysis
Malicious	• URL is redirecting to a fake Facebook login • B in facebook has been replaced by an ASCII character to confuse the receiver with the correct link • The URL is considered phishing because it mimics a legitimate Facebook login page but actually belongs to the com.opt domain, not Facebook. This is a deceptive tactic used to trick users into entering their credentials on a fake site controlled by attackers.

Email 4:

Is this email Safe or Malicious?	My Analysis
Safe	• Although email is not matching with the sender's name, the email does not contain harmful links or attachments. • The email Adam Markus forwarded is an advertisement of a product

Email 5:

Is this email Safe or Malicious?	My Analysis
Malicious	• The email is designed to create urgency and manipulate emotions • The sender asks the recipient to provide access to their personal email account which is not standard behavior for any legitimate agency. • Lack of official FBI badge number, email signature, official email domain, or contact method provided indicates email is not legitimate.

Email 6:

Is this email Safe or Malicious?	My Analysis
Safe	• There are no suspicious links, attachments, or requests for sensitive information. • The email reflects normal internal communication between two employees discussing work-from-home arrangements and a pending file. • Both sender and recipient use official ANZ email addresses, and the conversation aligns with expected business operations.

Email 7:

Is this email Safe or Malicious?	My Analysis
Malicious	• No formal greeting including the name of the customer • The email contains a suspicious shortened or obfuscated URL (hxxp://...receipt.php), commonly used to evade spam filters and deliver malware or phishing payloads. • The sender address Val.kill.ma and domain urlif.y are unusual and not associated with Geico • The content is unsolicited, attempts to lure the recipient with a fake promotional offer, and includes a PHP file, which may trigger a malicious script if clicked.