

**Email 1:****Is this email Safe or Malicious?**

**Safe**

**My Analysis:**

- The email is a casual conversation about games between friends, with no requests for personal information or sensitive data.
- The sender's email address matches the content of the conversation, and there are no suspicious links or attachments.
- The email aligns with the guidelines since it doesn't ask for any personal information or direct the user to any links for verification.

**Email 2:****Is this email Safe or Malicious?**

**Malicious**

**My Analysis:**

- This email is from an unusual domain (Venture.ru) and contains a request to click a link to update an Office 365 account.
- The email asks for updates to your email address and mentions security and large files, which is not typical for genuine communications from Microsoft.
- This email fits the phishing criteria since it involves requesting personal information through a link and uses a suspicious domain.

**Email 3:****Is this email Safe or Malicious?**

**Malicious**

**My Analysis:**

- The email contains a suspicious link to <https://www.faceRook.com.opt/login.htm>, which is a misspelled version of Facebook and likely intended to steal login credentials.
- It asks the recipient to check if Facebook is working and includes a link that could be a phishing attempt.
- This email is malicious because it directs the recipient to a potentially harmful website.

**Email 4:****Is this email Safe or Malicious?**

**Safe**

**My Analysis:**

- The email forwards a message about a gaming headset sale, with no suspicious links or requests for personal information.
- The email comes from a legitimate domain (i.massdrop.com) and the content appears to be a standard marketing communication.
- The email adheres to the guidelines as it does not ask for personal information or direct the user to any suspicious websites.

**Email 5:****Is this email Safe or Malicious?**

**Malicious**

**My Analysis:**

- This email claims to be from an FBI agent and requests the use of your email account to send critical information. It's a classic example of a scam or phishing attempt.
- It uses urgency and a fake identity to manipulate the recipient, and asks for access to personal email accounts.
- The email fits the criteria of phishing and scam attempts, since it solicits sensitive information under false pretenses.

**Email 6:****Is this email Safe or Malicious?**

**Safe**

**My Analysis:**

- The email exchange is between two ANZ employees and involves professional communication about a project.
- The email domain (@anz.com) and contact details are consistent with ANZ communication
- It adheres to the guidelines as it doesn't involve requests for personal information or suspicious links.

**Email 7:****Is this email Safe or Malicious?****Malicious****My Analysis:**

- The email contains a link to [hxxp://iwhrhwicy.urlif.y/receipt.php](http://hxxp://iwhrhwicy.urlif.y/receipt.php), which is suspicious and obfuscated.
- The message promotes a car insurance discount but uses a questionable URL that does not correspond to a legitimate insurance provider.
- This email is likely phishing due to the suspicious link and promotional content that may be used to gather personal information.