**Email 1:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * First of all, this is a personal email template * The recipient and sender, both are speaking to each other informally * Adam John is the sender and the owner of this gmail inbox. He’s written a personal message to his friend Velma. * The reply to the mail sent is highly informal in nature, but on careful examination, the message is clearly to the point of the sender’s question and does not contain any mailicious external links. * Athough, it is important to notice that the time that sender ‘Adam John’ sent a mail originally isn’t the same as in the quoted text. * This might mean that the sender’s email thread has been compromised possibly and the recipient Velma Khan must be warned of further malicious emails. |

**Email 2:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * Clearly a social engineering attack to steal personal info. * Firstly, let’s go through all indicators that might easily slip by anyone who is not attentive or is in a hurry: * The email subject it so accurate in describing the task specified in the email. * The email is marked as important * UPDATE YOUR ACCOUNT is highlighted in such a way that it might redirect to an authentic link * The signature at the end is spot on to make it look like the email is genuinely from Microsoft. * Now, let’s go through all the malicious indicators: * The email is from Venture.ru (Russian link), not from Microsoft support. (signature at the end) * ‘Onedrive..’ the link at the top looks genuine and might be the authentic OneDrive link to prove to the viewer that the email is genuine. (Which shows the intelligence in the planning by the hacker) * The Grammar of the 2nd paragraph is wrong. * ‘office 365’ instead of ‘Office365’, ‘Recevie’ instead of ‘receive’, ‘Update’ insead of ‘updated’, ‘file’ instead of ‘files’. * SECURITY is in huge letters to scare the receipient into believing that there may be a compromise. * No customer support email asks for signing up, so the link might be http:// link or a proxy server. * The ‘customers support’ at the end clearly indicates that it is not written by a person who knows English or who’s using an auto signature generator by Microsoft’s emailer service. |

**Email 3:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The attached URL is clearly a proxy server. * ‘facebook’ is spelt wrongly, the url ends with ‘.com.opt’ linking to another domain entirely, ‘.htm’ is not the same as ‘.html’ showing malicious code injection. * The email is clearly informal from the subject line, showing that it is probably from a trusted friend of the recipient who’s identity has been compromised(identity theft) or another email address with that friend’s name is being used. * The description in the start shows a concerned friend trying to convince the recipient to click the malicious link. * Since, it is signed as ‘Vinny’ in the end, the url clearly indicates a social engineering attack designed to steal the identity and credentials of facebook belonging to the recipient. |

**Email 4:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe/Malicious | * This situation could be linked to either a malicious or a non-malicious thread. * Let me elaborate a bit, if the sender ‘Adam Markus’ is a trusted person to the recipient ‘me’, then it is a safe email. * This is because it clearly is a double forwarded promotional message from ‘i.massdrop.com’ regarding a product that is released by the massdrop company. * Further, it cearly is a trusted website by the person who sent it, however, it is important that sensitive info shouldn’t be entered through the link anyways. * Considering that the mail is malicious, there are 2 indicators: * ‘i.massdrop.com’ sounds like a proxy website with a fake address to steal personal info. * There’s a chance that the recipient doesn’t know Adam Markus, clearly meaning that he might be an attacker trying to steal sensitive info through phishing. |

**Email 5:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The subject line is informal even the content of the mail is set in a formal tone. * The name of the agent disclosed to a random person along with the details of the investigation is something that is out of the ordinary. * Further, the mail is clearly sent from the personal email of Vincent and not from an encrypted server which is expected of all secret emails. * Lastly, the email directly asks for the credentials of the email of the recipient which clearly shows the motive of the attacker- Social engineering to steal credentials. * Additionally, the personal style of the email with an informal signature without the details of the organization at the bottom for a high level operation is suspicious. |

**Email 6:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Safe | * This is an informal professional conversation between 2 colleagues at ANZ’s office through the official mailer thread. * The subject is crisp to indicate the contents of the mail and is professional in tone. To keep the personal things out of the context, Alan Bryce has clearly put it in as a side note. * The signature is also indicative of a professional tone. * The reply to the mail has been done on the same thread and is through an ‘Anz.com’ mail, so, it is safe. * Further the contents of the reply email is straight and to the point without any deviations or external links. |

**Email 7:**

|  |  |
| --- | --- |
| **Is this email Safe or Malicious?** | **My Analysis** |
| Malicious | * The URL is clearly flawed and leads to a malicious website. * First, the protocol itself is ‘hxxp’, clearly wrong, there’s a bunch of random words forming up the main address with the domain of a non-recognized server that could mean a potential hack * Finally, the ‘receipt’ php page clearly is trying to steal the car insurance details of the recipient, cause php is easy to use for monitoring traffic to steal credentials. * The subject of the email, is on its own indicative of a non-professional/promotional email. * The sender is some random person with a very questionable address ‘Val.kill.ma’. * Further, the email has no content specified by the sender clearly intending the recipient to fall bait to the subject line to save a few bucks on their car insurance. * The signature is in no way matching the sender’s address, clearly meaning it was sent from a custom smtp server to steal sensitive info. * This is clearly part of a phishing attack. |