TASK

Email Analysis and Phishing Emails dentification

Analyst Name

Abdiaziz Ibrahim Kar

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	This email is non-malicious because it appears a normal conversation between friends or close individuals, there's the use of informal words such as dude, and mate. In addition, it doesn't contain any links.

Email 2:

Is this email Safe or Malicious?	My Analysis
Malicious	I classified this email as malicious. There's a sense of urgency, one of the techniques used in social engineering. The sender claims to be Microsoft, an organization with a high reputation but the email is poorly formatted, with punctuation errors. Moreover, the email contains a hyperlink that possibly directs recipients to malicious sites. Lastly, the sender has .ru as a top-level domain, an indication that the mail server is from Russia, a country associated with malicious sites.

Email 3:

Is this email Safe or Malicious?	My Analysis
Malicious	Without any hesitation, I classified this email malicious. The sender is either posing as someone known to the recipient or is using a compromised email account. The major red flag is the use of "HOMOGLYPH" – characters that appear similar but very different. Can you spot the Homoglyph in the link? Yes, you're right, we can't

	see the real B in Facebook word. Other examples of Homoglyph are LinkedIn, microsoft...

Email 4:

Is this email Safe or Malicious?	
Safe	After parsing the content, the email looks non-malicious, just a normal advertisement. There are no links and social engineering techniques detected.

Email 5:

Is this email Safe or Malicious?	My Analysis
Malicious	According to the email's content, I classified it as malicious. The sender tried to use Authority by posing as an FBI agent undercover in Uganda. Attackers often use this technique, knowing that individuals cannot defy such orders. The sender claims to need the employee's email credentials for "security reasons."

Email 6:

Is this email Safe or Malicious?	My Analysis
Safe	This email is not malicious. It's visible that both the recipient and the sender are from within the organization, and the signature names match.

Email 7:

Is this email Safe or Malicious?	My Analysis
Malicious	This email seems malicious because: (i) there's mismatch between the signature name (Mike Ferris) and the sender's name (Val.kill.ma) (ii) the sender impersonates Geico, car insurance company, but the link doesn't have the company's domain name.