1. To perform email investigation based on the emails provided by various departments of your organisations and generate a incidence response report for it.

Scenario:

Your company has forwarded you some e-mails. You have to investigate these e-mails. Mention that n your investigation of the emails, what signs did you find to indicate whether each email was malicious or safe?

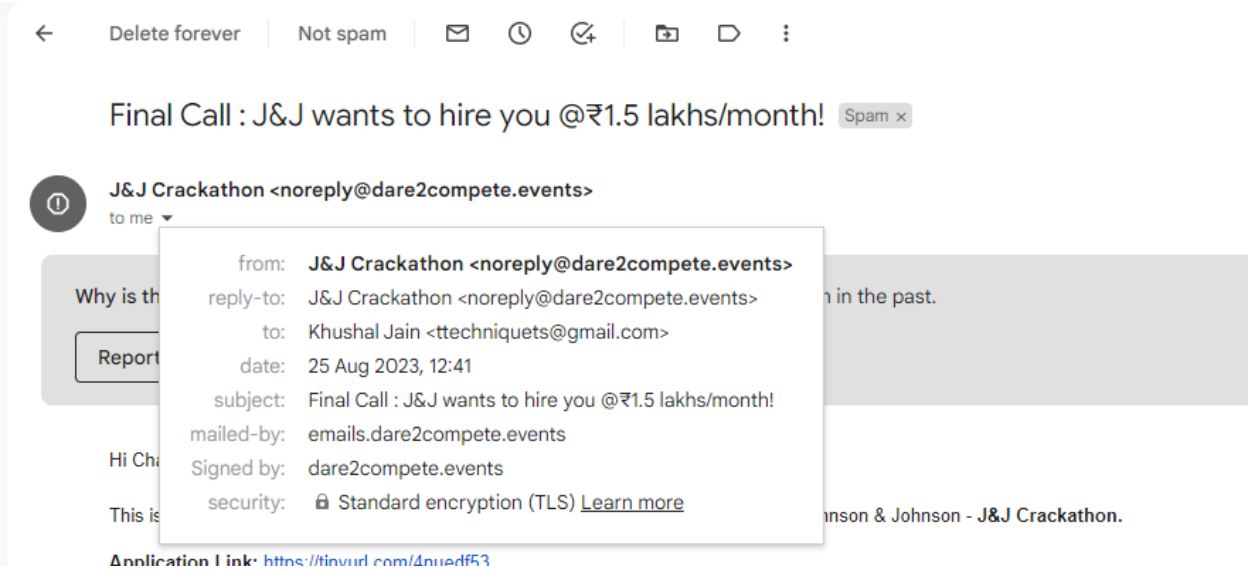

Fig : E-mail 1

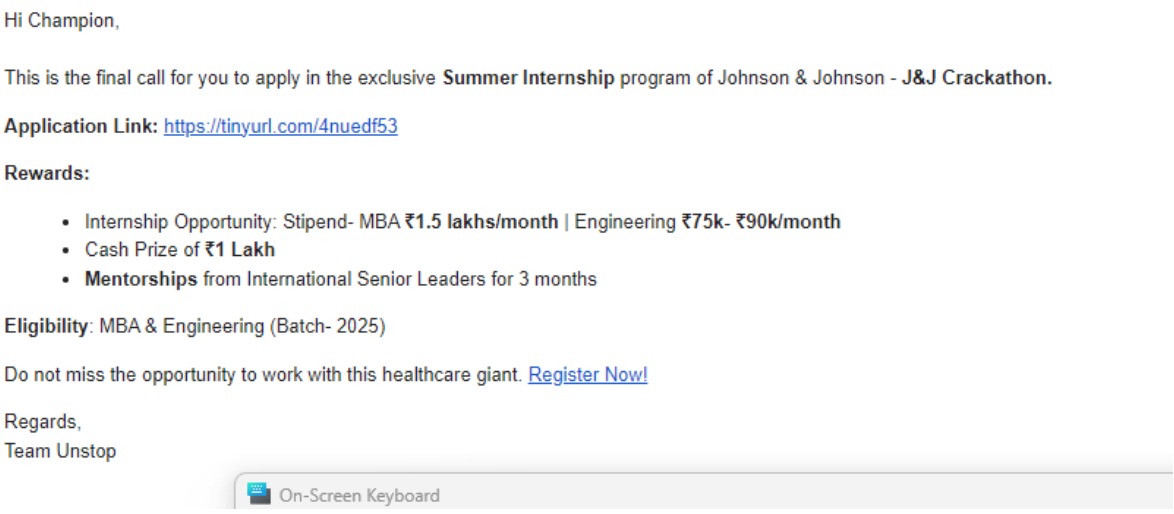

Fig : E-mail 2

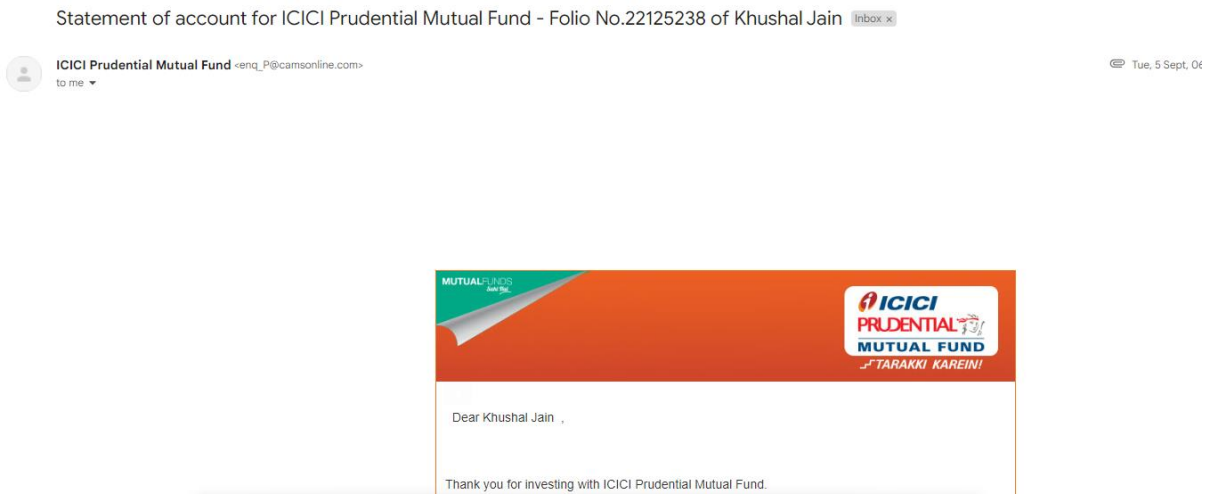

Fig: E-mail 3

Solution:

E-mail 1 Solution

Is this email Safe or Malicious?	**My Analysis**
Malicious	• *The e-mail is not very professional. It has mispelled receive as recevie. The e-mail doesn't seems to come from One Drive or Microsoft as the e-mail mentions the name as Venture.ru but if the e-mail would have came from Microsoft, it would display the name as Microsoft Support or One Drive Support Team. There are many other such grammatical errors.* • *The e-mail states that the user has one new file to be viewed in the OneDrive but the last paragraph states that the user has to sign up by clicking on Update Your Account. This clearly reveals that the e-mail is malicious.* • *The e-mail states that the user will receive files attached with ADOBE PDF and SECURITY is written in bold to lay emphasis which was clearly not required. This is suspicious.* • *The e-mail requires user to click on the link and perform some actions by providing login credentials. This e-mail is associated with phishing attack.*
Malicious	• *The e-mail is not very professional. It has spelling and gramatical mistakes.* • *The email in itself is spam as it is asking the receive to do a impersonation.* • *The sender is asking to contact him privately at his personal email address.*
Malicious	• *Springbanking.com is not a banking domain.* • *The username is suspicious.* • *The mail s coming from springbanking.com from the response is required at outllook.com email id.* • *The e-mail in itself is suspicious.*