Date- 27th May,2025
Purpose of task- Reviewing a phishing email and analysing it.

Introduction:
The purpose of this task is to analyse the workings and social engineering aspects of phishing attacks done by scammers and hackers. Phishing email may contain websites that look identical to the original website that the scammer is trying to imitate,that open up when clicked on the attached link. The attached link may also redirect to another website that automatically downloads a payload that may contain malware or ransomware. Thus,this task becomes really important for the security of the firm and the person itself.

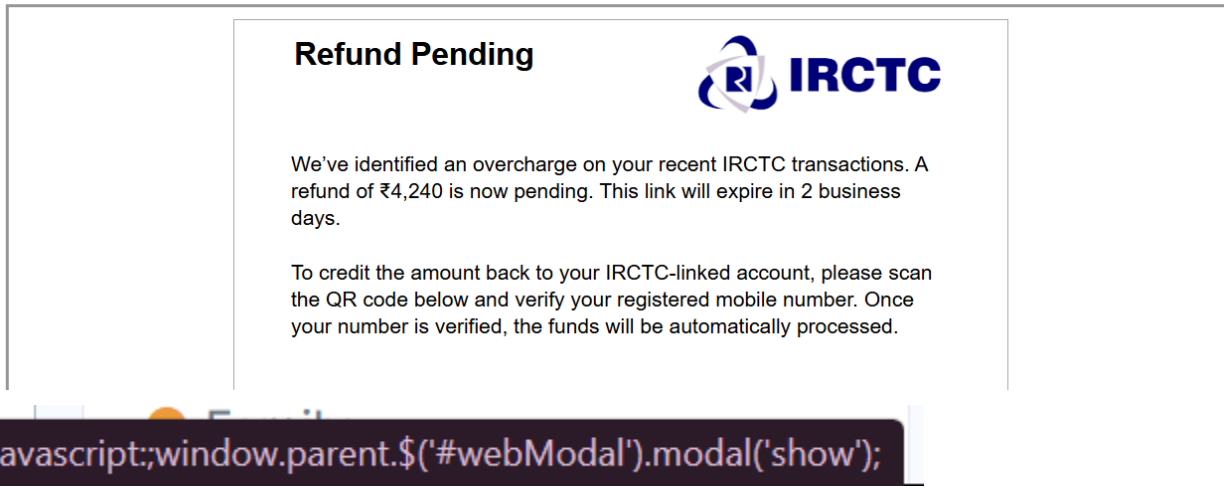
Methods used:
Analysing the header like sender's address,CC,subject,etc.
Analysing the body for grammatical errors,unprofessional language,etc.
Analysing the attachments like Link,QR code,PDF, etc.

Findings:
The sample email was used from an online website(CaInPhish.com) that provided the template for a phishing attack as a sample.
We found that the email of the sender didn't match that of the entity it tried to imitate.
We also found that the link was redirected to some other website when clicked,which was found when the mouse was hovering over the attached link.
Also it showed tax as 0,whereas govt generally charges GST in the IRCTC refunds.
It also created an urgency through it's language in the body and the subject too.

Conclusion:
These traits are common in phishing emails and must not be ignored.

Below attached are the screenshots of the phishing email that was analysed.

IRCTC Helpdesk (irctc-helpdesk@securesupportcloud[.]com)
to john[.]doe@mybusiness[.]com




```
javascript:;window.parent.$('#webModal').modal('show');
```

Pending Refund

Overcharge	₹4,240
Taxes	₹0