Ideation Phase
Define the Problem Statements

Date	22 October 2022
Team ID	PNT2022TMID03377
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

Web Phishing Detection problem Statement:

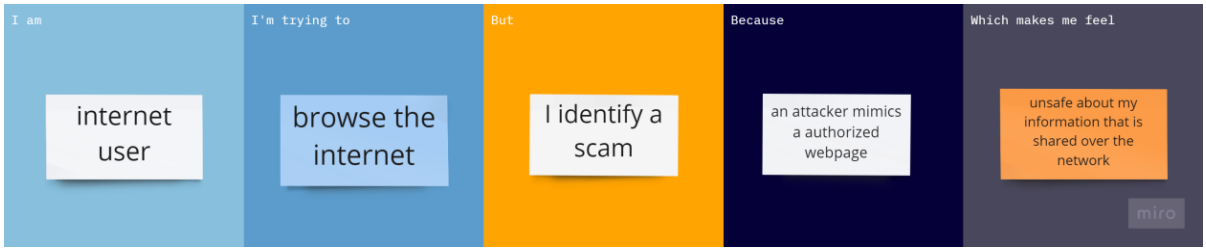
Phishing attacks are becoming more and more sophisticated, and our algorithms are suffering to keep up with this level of sophistication. They have low detection rate and high false alarm especially when novel phishing approaches are use. The blacklist-based method is unable to keep up with the current phishing attacks as registering new domains has become easier. Moreover, comprehensive blacklist can ensure a perfect up-to-date database. Various other techniques such as page content inspection algorithms have been used to combat the false negatives but as each algorithm uses a different approach, their accuracy varies. Therefore, a combination of the two can increase the accuracy while implementing different error detection methods.

Problem Statement 1:

Problem Statement 2:

Problem Statement 3:

Problem Statement 4:



Problem Statement (PS)	I am (Customer)	I'm trying to	But	Because	Which makes me feel
PS-1	Vendor	Use online transactions	I find illegal pages who indulge in bankruptcy	Of counterfeit websites who steal credentials	Unsafe about online transactions
PS-2	Account holder in Bank	Use credit and withdraw money from bank account	I find fraudulent webpages who steal account details	an attacker masquerades a reputable entity	doubtful about using those features
PS-3	enterprise user	open mails in the cloud server	I detect malicious mails	they are not cryptographically signed	Emails are not verified and third party intrusions
PS-4	internet user	browse the internet	I identify a scam	an attacker mimics a authorized webpage	unsafe about my information that is shared over the network