Ideation Phase
Define the Problem Statements

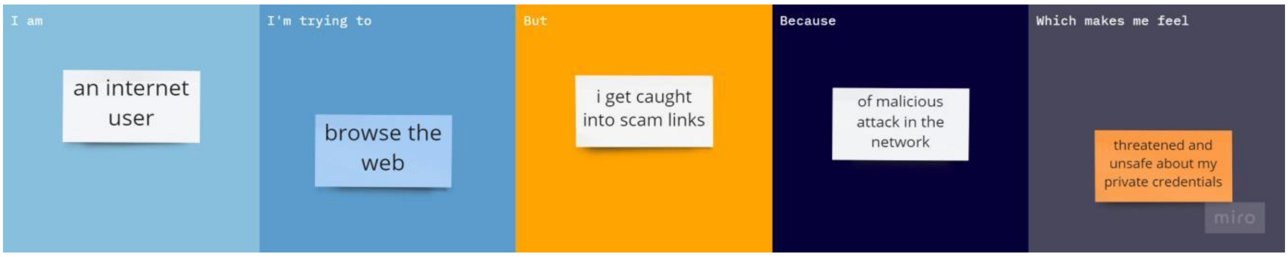
Date	14 November 2022
Team ID	PNT2022TMID49921
Project Name	Project – Web Phishing Detection
Maximum Marks	2 Marks

Problem Statement:

Phishing is a type of social engineering attack often used to steal user data. 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 used. The blacklist-based method is unable to keep up with the current phishing attacks as registering new domains has become easier. Moreover, a 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.

Since scams are widespread and nobody wants to fall for web phishing, regular users who search the internet for information need a way to make sure the links they click are safe.

Example:


I am
an internet user
I'm trying to
browse the web
But
i get caught into scam links
Because
of malicious attack in the network
Which makes me feel
threatened and unsafe about my private credentials
miro

Problem Statement (PS)	I am (Customer)	I'm trying to	But	Because	Which makes me feel
PS-1	Internet user	Browse the internet	I identify a scam	An attacker masquerades as a reputable entity	Unsafe about my information that is shared over the network
PS-2	Enterprise user	Open emails in the cloud server	I detect malicious protocols	They are not cryptographically signed	Emails are unverified and third-party intrusion