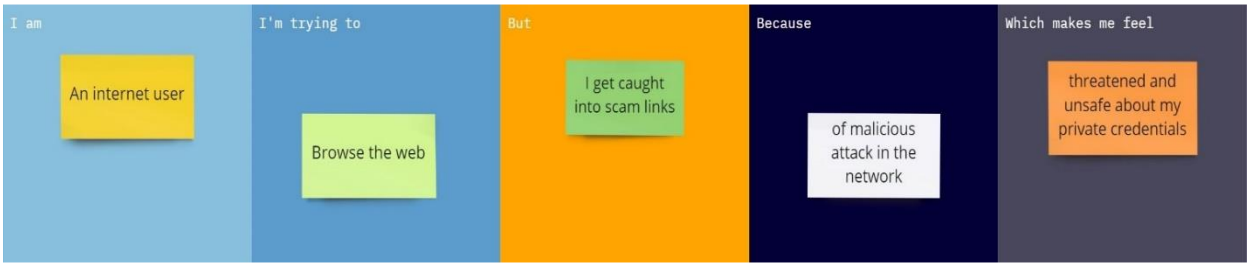
Ideation Phase
Define the Problem Statements

Date	19 September 2022
Team ID	PNT2022TMID00733
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

Problem Statement:

Phishing attacks succeed when human users fail to detect phishing sites. Generally speaking, past work in anti-phishing falls into four categories: studies to understand why people fall for phishing attacks, methods for training people not to fall for phishing attacks, user interfaces for helping people make better decisions about rusting email and websites, and automated tools to detect phishing. Our work describes an automated approach to detect phishing. Most of the end user normally takes decision only based on what he/she look and feel. When a user is accessing internet he/she only see the screen of a browser. He/she then work on the command of a web-page. The user doesn't concern about the back-end process and most phishing attempts get this type of unintentional opportunity given by the user and make them fool. Common users who look for information on the web are unsafe on the internet who need a method to ensure the links they click are secure because scams are common and no one should become a victim of web phishing.

Problem Statement Template:



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

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