Ideation Phase
Define the Problem Statements

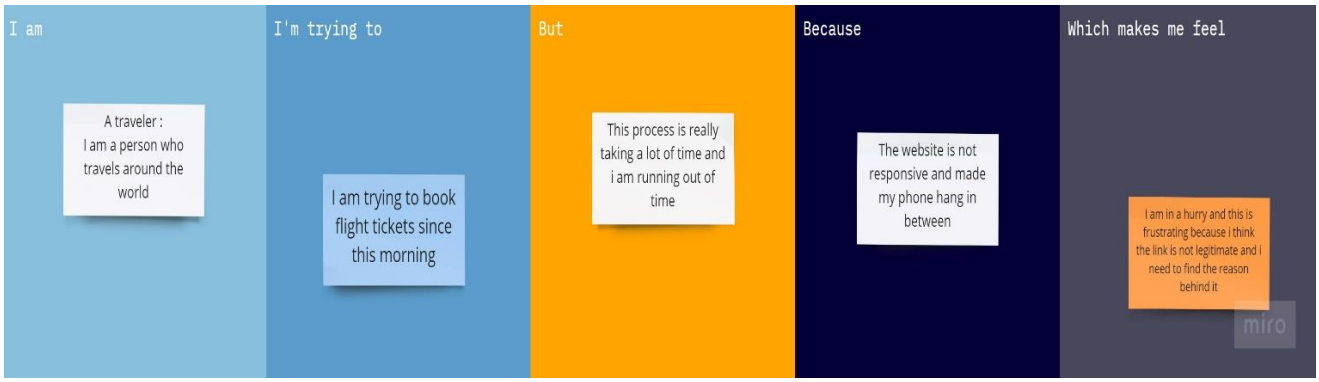
Date	19 September 2022
Team ID	PNT2022TMID15184
Project Name	WEB PHISHING DETECTION
Maximum Marks	2 Marks

Customer Problem Statement Template:

Internet has dominated the world by dragging half of the world's population exponentially into the cyber world. With the booming of internet transactions, cybercrimes rapidly increased and with anonymity presented by the internet, Hackers attempt to trap the end users through various forms like phishing.
Customers usually face problems with malicious links. These links will lead to a website that often steals login credentials or financial information like credit card numbers. Scanning a URL may have unexpected consequences, such as unsubscribing a user from a mailing list, so it is important that we limit these potential collateral damages.
Phishing may lead to financial loss, emotional loss, stress, and information scams of customers.

I am	Phishing can target any sector and user, from a business executive to a home social network user or online banking consumer. Participants between the ages of 18 and 25 are more susceptible to phishing than other age groups.
I'm trying to	• Never click any links or attachments in suspicious emails. • If the suspicious message appears to come from a person you know, contact that person via some other means such as text message or phone call to confirm it. • Report the message. • Delete it.
But	Phishing happens when a victim replies to a fraudulent email that demands urgent action. Examples of requested actions in a phishing email include: Clicking an attachment. Enabling macros in Word document. Different types of phishing are Spear Phishing, Whaling, Vishing, Email Phishing.
Because	Lack of security awareness among employees is also one of the major reasons for the success of phishing. Organizations should be aware of how the benefits and purpose of security awareness training can secure their employees from falling victim to phishing attacks.
Which makes me feel	software-based phishing detection techniques are preferred for fighting against the phishing attack. Mostly available methods for detecting phishing attacks are blacklists/whitelists, natural language processing, visual similarity, rules, machine learning techniques. We provide our best resources to the customers in a way that they can access all the resources that we provide.

Example:



Problem Statement (PS)	I am (Customer)	I'm trying to	But	Because	Which makes me feel
PS-1	Parineeti	I'm continuously getting Emails from unknown users	But these Emails are not showing any proper information	I think these Emails are from attackers	This problem is getting me on my nerves. I want a solution for this problem
PS-2	Shiv	Recently my social media account has been hacked I'm trying to figure out what's the problem	But I'm no longer able to access my account anymore	Because my account is being accessed by the hacker	This is making me feel unsafe about the information in my account. I want to solve this problem