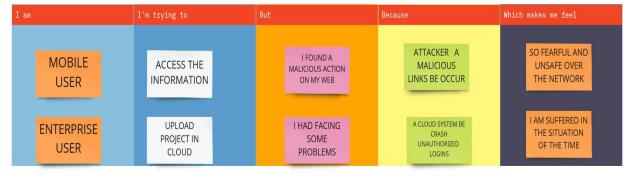# Ideation Phase

Problem Statement

Team ID	PNT2022TMID52463
Project Name	Project – web phishing detection

Customer Problem Statement

Phishing is a fraudulent technique that uses social and technological tricks to steal customer identification and financial credentials. Social media systems use spoofed e-mails from legitimate companies and agencies to enable users to use fake websites to divulge financial details like usernames and passwords. Hackers install malicious software on computers to steal credentials, often using systems to intercept username and passwords of consumers' online accounts. Phisher use multiple methods, including email, Uniform Resource Locators (URL), instant messages, forum postings, telephone calls, and text messages to steal user information. The structure of phishing content is similar to the original content and trick users to access the content in order to obtain their sensitive data. The primary objective of phishing is to gain certain personal information for financial gain or use of identity theft. Phishing attacks are causing severe economic damage around the world. Moreover, Most phishing attacks target financial/payment institutions and webmail, according to the Anti-Phishing. Working Group (APWG) latest Phishing pattern studies.

Problem Statement (PS)	Iam (Customer)	I'm trying to	But	Because	Which makes me feel
PS-1	Internet user	Access the information	I found a suspicious actions	Malicious link be occur on screen	Fearful and unsafe over the network
PS-2	Industrial user	Detect some file in cloud	I had facing some issue on cloud	A cloud system crashed due to unauthorized logins	I am suffered in the situation on this time and frustated