Project Title: Web phishing Detection | **Project Design Phase-I - Solution Fit** | **Team ID:** PNT2022TMID47095

Define CS, fit into CC

CS

1. CUSTOMER SEGMENT(S)

Internet users who frequent millions of websites

especially those who utilise websites for e-banking and e-commerce.

6. CUSTOMER CONSTRAINTS

• Phishing attempts frequently result in the loss of a customer's credentials and valuable personal information.

5. AVAILABLE SOLUTIONS

• Manual self-analysis using address features as a basis for confirmation.

• Double checking the link with a phishing database.

Explore AS, differentiate

Focus on J&P, tap into BE, understand RC

2. JOBS-TO-BE-DONE / PROBLEMS

Obtaining the URLs of websites from customers, classifying them using various ML

RC

9. PROBLEM ROOT CAUSE

Developments in technology that encourage hacking and phishing.

Low effectiveness of algorithms.

Credential access that is unclear.

BE

7. BEHAVIOUR

• Making use of a unique extension that examines the current link

• The user can access the extension that offers results.

Focus on J&P, tap into BE, understand RC

Jobs to be done / Problem

3. TRIGGERS

TR

• As alerted with the urge or temptation to commit to a task.

4. EMOTIONS: BEFORE / AFTER

EM

• Before: Fear of Uncertainty, Vulnerability.

• After: Relief of maintaining privacy and confidence in website access.

10. YOUR SOLUTION

SL

Making a website in Python where a user may enter a URL and the system classifies it as a phishing website or not using machine learning algorithms and then provides the user with feedback

8. CHANNELS of BEHAVIOUR

CH

- **ONLINE**

Using the website link to examine the phishing website's behaviour and receiving feedback from the build with

Identify strong TR