Project Title:Web Phishing Detection **Project Design Phase-I - Solution Fit** **Team ID: PNT2022TMID31293**

Define CS, fit into CC

1. CUSTOMER SEGMENT(S) CS

- Users who purchase products online and make payaments through c-banking
- Online payment servies
- Web Broswers and Hand-Held applications
- Internet users who frequent millions of websites
- especially those who utilise websites for e- banking and e-commerce.

6. CUSTOMER CONSTRAINTS CC

- They won't be able to understand the true nature of the side because the can't observe the transaction site's primary procedure
- Customers are unable to distinguish between legitimate and fraudulent websites.
- They are unable to determine
- Whether they should believe the information provided in the websites
- Phishing attempts frequently result inthe loss of a customer's credentials and valuable personal information.

5. AVAILABLE SOLUTIONS AS

- Manual self-analysis using address features as a basis for confirmation.
- Double checking the link with a phishing database.
- To identify phishing ,there are numerous websites that oofer phishing detection services

Explore AS, differentiate

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

2. JOBS-TO-BE-DONE / PROBLEMS J&P

- To Ensure user safety by preventing user data from being stolen
- Eductaion the user on suspicious activity on the surface of the website
- Help the user identify authentic websites from fake phishing ones
- Obtaining the URLs ofwebsites from customers.

9. PROBLEM ROOT CAUSE RC

- The issue is that phoney websites can steal client information because of this vulnerability
- Developing in technology that encourage hacking and phishing
- Low effectiveness of algorithms
- Credential access

7. BEHAVIOUR BE

- Customers utilize phishig detection websites to avoid accessing fraudulent websites and safeguard their personal information on those websites
- Even if a website appears to be legitimate users should not believe it
- Making use of a unique extension that examines thecurrent link
- The user can access the extension that offers results.

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

Identify strong TR & EM

3. TRIGGERS TR

- Attractive Advertisements/Sales Coupon
- Pop-ups of various kinds
- Links pretending to be legitimate that prompt the user to center his/her personal details
- As alerted with the urge or temptation to commit to a task.

4. EMOTIONS: BEFORE / AFTER EM

- Before: Fear of Uncertainty,Vulnerability,Fear,Confused,Threatened,Voilated
- After: Relief of maintaining privacy and confidence in website access.Safe,Aware,Confident and Happy

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
- Using phishing detection websites to stop their information from being leaked is the greatest way to stop clients from visiting fraudulent websites

8. CHANNELS of BEHAVIOUR CH

8.1 ONLINE

Customers utilize phishing websites to provide the leakage of the information they otherwise supply to the website

Using the website link to examinethe phishing website's behaviour and receiving feedback from the build site

8.2 OFFLINE

There