Project Title: WEB PHISHING DETECTION **Project Design Phase-I -Solution Fit** **Team ID: PNT2022TMID16684**

1. CUSTOMER SEGMENT(S) CS

Web users are mainly persons who purchase products through online payment or makeonline transactions.

6. CUSTOMER CONSTRAINTS CC

No breakdown of server connections and full permission to scan the transaction process.

5. AVAILABLE SOLUTIONS AS

Use multi-factor authentication to secure your accounts. Some accounts supply more security by needing two or more credentials to log in. Multi-factor authentication is one of the available solutions.

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

To keep the user's data and transactions protected from phishing sites and attackers.

9. PROBLEM ROOT CAUSE RC

Poor network authentication or use of traditional encryption techniques. Fooling customers by spoofing original websites.

7. BEHAVIOUR BE

Directly related: finds the user-friendly Web phishing detection application

Indirectly related: permission to access the whole transaction process and server connectivity

Identify strong TR & EM

3. TRIGGERS TR

If web phishing detection is implemented successfully, it makes other users and shopping sites prefer our application for payments and transactions.

4. EMOTIONS: BEFORE / AFTER EM

Before: getting cheated by phishing websites. After:

data confidentiality and secure transactions.

10. YOUR SOLUTION SL

1. Create a web application or web page to get the active URL as input.
2. Extract URL contents and test the model using a data mining algorithm and predict. If the website is hacked one sends an alert message and stores it in blacklisted URLs orelse continues the transaction process.

3.Prediction is more accurate.

8. CHANNELS of BEHAVIOUR CH

Online: Inputs the active URL and extract thedetails for prediction.

Offline: Stores the detected phishing sites toa Blacklisted URL.