

## Project Design Phase-I Problem – Solution Fit

Date	03 October 2022
Team ID	PNT2022TMID26922
Project Name	Project – WEB PHISHING DETECTION
Maximum Marks	2 Marks

### Problem – Solution Fit :

The Problem-Solution Fit simply means that you have found a problem with your customer and that the solution you have realized for it actually solves the customer's problem. It helps entrepreneurs, marketers and corporate innovators identify behavioral patterns and recognize what would work and why

### Purpose:

- ☐ Solve complex problems in a way that fits the state of your customers.
- ☐ Succeed faster and increase your solution adoption by tapping into existing mediums and channels of behavior.
- ☐ Sharpen your communication and marketing strategy with the right triggers and messaging.
- ☐ Increase touch-points with your company by finding the right problem-behavior fit and building trust by solving frequent annoyances, or urgent or costly problems.
- ☐ **Understand the existing situation in order to improve it for your target group.**

Identify strong TR & EM	<b>1. CUSTOMER SEGMENT(S)</b> <span style="float: right;">CS</span>  Web users, mainly persons who purchase products through online payment or make online transactions.	<b>6. CUSTOMER CONSTRAINTS</b> <span style="float: right;">CC</span>  No breakdown of server connections and full permission to scan the transaction process.	<b>5. AVAILABLE SOLUTIONS</b> <span style="float: right;">AS</span>  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 solution
	<b>2. JOBS TO BE DONE/PROBLEMS</b> <span style="float: right;">J&amp;P</span>  To keep the user's data and transactions protected from phishing sites and attackers.	<b>9. PROBLEM ROOT CAUSE</b> <span style="float: right;">RC</span>  Poor network authentication or use of traditional encryption technique. Fooling customers by spoofing original websites.	<b>7. BEHAVIOUR</b> <span style="float: right;">BF</span>  Directly related: finds the user friendly Web phishing detection application  Indirectly related: permission to access the whole transaction process and server connectivity
	<b>3. TRIGGERS</b> <span style="float: right;">TR</span> If web phishing detection is implemented successfully, it makes other users and shopping sites to prefer our application for payments and transactions.  <b>4. EMOTIONS: BEFORE / AFTER</b> <span style="float: right;">EM</span>  Before : getting cheated up by phishing website. After : data confidentiality and secure transactions.	<b>10. YOUR SOLUTION</b> <span style="float: right;">SL</span>  1. Create a web application or web page to get the active URL as input. 2. Extract URL contents and test the model using data mining algorithm and predict. If the website is a hacked one send alert message and store it in blacklisted URLs or else continue the transaction process. 3. Prediction is more accurate.	<b>8. CHANNELS of BEHAVIOUR</b> <span style="float: right;">CH</span>  Online : Inputs the active url and extract the details for prediction.  Offline : Stores the detected phishing sites to Blacklisted url.