Problem – Solution Fit :

Essentially, the problem solution fit means that you have found a problem with a customer and that the solution you have realized solves it for them. By Identifying behavioural patterns, it helps enterpreneurs , marketers and corporate innovators identify what and why.

Purpose:

- ❑ Find a way to solve complex problems in a manner that is appropriate for the customer's situation.
- ❑ Utilize existing channels and media to gain more adoption of your solution.
- ❑ Use the right triggers and messaging to refine your communication and marketing strategy.
- ❑ Ensure we find the right fit between problem-behavior and your company's needs by resolving frequent annoyances, urgent problems and costly problems.
- ❑ Understand the existing situation in order to improve it for your target group.

Problem – Solution Fit:

| Define CS, fit into CC | **1.CUSTOMER SEGMENT(S)** `CS`

a.Users who buy products on-line and make payments via e-banking.

b. Sensitive data will be shared through these kind of websites. | **6. CUSTOMER CONSTRAINTS**

a. Not being able to see the main process of the transaction site, they will not be able to know the real nature of the site.
b. sense of insecurity when faced with constraints.
c. Not knowing how to protect them and identify malicious | **5. AVAILABLE SOLUTIONS** `AS`

a The above solutions check if the website is available in the legitimate websites list, but have property limitations such as exact name and adding items to the list frequently.
b.Other ML model solution predictions are based on the content of the URL instead of its properties | Explore AS, differentiate |
| Focus on J&P, tap into BE, understand | **2. JOBS-TO-BE-DONE / PROBLEMS**

a.Websites with link that contain malware.

b.Saying that they've noticed some suspicious activity or log-in attempts.

c.Claim there is a problem with your account or your payment information.

d.Want you to click on a link to make a payment, but the link has malware. | **9. PROBLEM ROOT CAUSE** `RC`

a.Attackers keep fooling people by spoofing original sites.

b.They use their knowledge on the domain for cheating and other bad intentions.

c.Common people will not have much knowledge on this domain. They find it harder just to use the web service. | **7. BEHAVIOUR** `BE`

a.Users need to be more aware about what information they provide to the sites.

b.They should not believe any site they visit even if they look the legitimate ones. | Focus on J&P, tap into BE, understand |

3. TRIGGERS `TR`

a. Loss of money
b. Loss of intellectual property.
c. Damage to reputation
d. Disruption of operational activities

4. EMOTIONS: BEFORE / AFTER `EM`

BEFORE:
- ✓ Stressed
- ✓ Fear
- ✓ Frustrated
- ✓ Confused

AFTER :
- ✓ Confident
- ✓ Safe
- ✓ Peace
- ✓ Happy

10. YOUR SOLUTION `SL`

A deep learning-based framework by implementing it as a browser plug-in capable of determining whether there is a phishing risk in real-time when the user visits a web page and gives a warning message. The real-time prediction includes whitelist filtering, blacklist interception, and machine learning (ML) prediction. To deal with phishing attacks and distinguishing the phishing webpages automatically, Blacklist based detection technique keeps a list of websites' URLs that are categorized as phishing sites. If a web-page requested by a user exists in the formed list, the connection to the queried website is blocked. Machine Learning (ML) based approaches rely on classification algorithms such as Support Vector Machines (SVM) and Decision Trees (DT) to train a model that can later automatically classify the fraudulent websites at run-time without any human

8. CHANNELS of BEHAVIOUR `CH`

8.1 ONLINE
Enter the URL and predicts the user

8.2 OFFLINE
a. Offline
b. Checks the site already available legitimate sites list.
c. Stores the phishing site to another list..