Project Design Phase-I
Problem – Solution Fit Template

Date	19 September 2022
Team ID	PNT2022TMID00733
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

Problem – Solution Fit Template:

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.**

Template:

1. CUSTOMER SEGMENT(S) `CS`

Who is your customer?

- ✓ The customer focus is on people who use the internet for e-transactions where safeguarding customers data important and vital.
- ✓ Government agencies and industries are another customer base where they require phishing detection systems to safeguard confidential information.

6. CUSTOMER CONSTRAINTS `CC`

What constraints prevent your customers from taking action or limit their choices of solutions?

- ✓ Lack of basic knowledge in verifying the correct URL of the webpage.
- ✓ Lack of user testing by organization as they require more resources and money. They are always in a rush which makes them prone to errors.
- ✓ Malwares have become more complex than what a layman can understand.

5. AVAILABLE SOLUTIONS `AS`

Which solutions are available to the customers when they face the problem or need to get the job done? What have they tried in the past? What pros & cons do these solutions have?

- ✓ Using a good Antivirus software or an Anti-Phishing toolbar which are available as extensions in browsers.
- ✓ Verifying the websites privacy policy and ensuring the websites are SSL certified.
- ✓ Double checking the domain name.
- ✓ Anti-Spam software and Blacklisting.

Define CS, fit into CC

Explore AS, differentiate

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

Which jobs-to-be-done (or problems) do you address for your customers? There could be more than one; explore different sides.

- ✓ The phishing websites must be detected prior and should be blacklisted.
- ✓ Building a phishing URL detecting website where the user can copy paste the URL and find if the URL is legitimate.
- ✓ Companies trust is broken if private data of customers are leaked.

9. PROBLEM ROOT CAUSE `RC`

What is the real reason that this problem exists? What is the back story behind the need to do this job?

- ✓ Lack of basic awareness among the common folk and leniency in the adaption of new security measures.
- ✓ Low-cost phishing and ransomware tools are easy to get hold of.
- ✓ The financial incentive is high which makes more people to launch phishing attacks despite of the consequences.

7. BEHAVIOUR `BE`

What does your customer do to address the problem and get the job done?

- ✓ Customers should take a "trust no one" approach when opening an email and should always verify the "From" address of the email.
- ✓ Avoid clicking links or attachments in emails from unfamiliar sources and change your passwords regularly.

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

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

3. TRIGGER `TR`

What triggers customers to act? i.e. seeing their neighbour installing solar panels, reading about a more efficient solution in the news.

- ✓ To prevent data including login credentials and credit card numbers from getting stolen.
- ✓ Seeing others lose Money due to phishing and their reputation getting damaged. This increases the awareness of the people.

4. EMOTIONS: BEFORE / AFTER `EM`

How do customers feel when they face a problem or a job and afterwards?

BEFORE:
1. They feel threatened and insecure using the internet.
2. Fear of insecurity, Subject to vulnerability.

AFTER:
1. Data confidentiality.
2. Secure Transactions.

10. YOUR SOLUTION `SL`

If you are working on an existing business, write down your current solution first, fill in the canvas, and check how much it fits reality.

If you are working on a new business proposition, then keep it blank until you fill in the canvas and come up with a solution that fits within customer limitations, solves a problem and matches customer behaviour.

This project trains a model that can automatically classify the phishing websites at run-time without any human interventions.

We would create an interactive webpage using HTML & Python where a user may enter an URL and the system classifies whether it is a phishing or a legitimate webpage using Machine learning (ML) algorithms and then provide the user with appropriate feedback. If it is a phished webpage, then it will be added to the blacklist. This provides better data confidentiality to the users.

8. CHANNELS OF BEHAVIOUR `CH`

8.1 ONLINE
What kind of actions do customers take online?

- ✓ By using appropriate firewalls and not clicking random pop ups in browsers and in email links.
- ✓ Using a secure Wi-Fi network for online transactions and always double checking the URL twice beforehand.

8.2 OFFLINE
What kind of actions do customers take offline? Extract offline channels from #7 and use them for customer development.

- ✓ Not sharing confidential information in spam phone calls or in random messages.
- ✓ Raising awareness by conducting small camps in your locality among the elderly and people who have less computer knowledge.

Identify strong TR & EM

Extract online & offline CH of BE