Project Title: Web Phishing Detection | **Project Design Phase-I - Solution Fit Template** | **Team ID:** PNT2022TMID36037

Define CS, fit into CC

1. CUSTOMER SEGMENT(S) — CS

Who is your customer?
i.e. working parents of 0-5 y.o. kids

Here our customer is anyone who uses internet through which he shares personal / sensitive information.

Eg: Person who is making online transaction.

6. CUSTOMER CONSTRAINTS — CC

What constraints prevent your customers from taking action or limit their choices of solutions? i.e. spending power, budget, no cash, network connection, available devices.

* Not having enough knowledge about phishing activities and getting trapped in it.
* Not knowing how to protect them and identify malicious websites.
* Lacking information about anti-phishing and anti-spam software

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? i.e. pen and paper is an alternative to digital notetaking

Anti-phishing protection and anti-spam software are available to protect us from malicious activities, websites, links and mail.

Explore AS, differentiate

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

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.

* Maintaining the privacy of the end user is the main goal. i.e. their personal information should not be shared with others making it vulnerable to attacks.

* Users should be made aware of the phishing websites and thus should be made aware of it.

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?
i.e. customers have to do it because of the change in regulations.

* Fake / Phishing websites collect sensitive information and exploit them for their own use and indulge in malpractices.
* Sensitive information stolen (bank related details) can be used to make money out of it.

7. BEHAVIOUR — BE

What does your customer do to address the problem and get the job done?
i.e. directly related: find the right solar panel installer, calculate usage and benefits; indirectly associated: customers spend free time on volunteering work (i.e. Greenpeace)

Majority of the customer still doesn't know about the potential risk that web phishing poses and unaware of the pitfalls.

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

Identify strong TR & EM

3. TRIGGERS — TR

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

With social awareness and the concern to maintain the privacy of the data users should be made aware of information stealing and such malicious activities.

4. EMOTIONS: BEFORE / AFTER — EM

How do customers feel when they face a problem or a job and afterwards?
i.e. lost, insecure > confident, in control - use it in your communication strategy & design.

Before: insecure and terrified because their information is subjected to vulnerable activities.
After: Feels secured and privacy of data is maintained.

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.

The main objective of detecting malicious websites will be developed and along with-it user will be notified about it via SMS / WhatsApp. This can be implemented either using machine learning / deep learning techniques.

8. CHANNELS of BEHAVIOUR — CH

8.1 ONLINE
What kind of actions do customers take online? Extract online channels from #7

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

ONLINE: web application can be developed by which legitimate and phishing websites can be differentiated.

OFFLINE: Social awareness can be created and people can be educated the importance of securing the personal information.

Identify strong TR & EM