Project Title: Web Phishing Detection **Project Design Phase-I - Solution Fit Template** **Team ID:** PNT2022TMID51349

Define CS, fit into CC

1. CUSTOMER SEGMENT(S) CS

Who is your customer?

Our Customer can be of any aged group who use internet for their daily purpose

6. CUSTOMER CONSTRAINTS CC

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

User can protect their data from hacking by following some constraints such as using strong password, two-factor authentication, picture password based and don't login unwanted link

5. AVAILABLE SOLUTIONS AS

Which solutions are available to the customers when they face the problem

The currently available solutions for web phishing detection include the blacklist and whitelist, heuristic algorithm, visual similarity and machine learning.

Among which the heuristics and machine learning techniques are more widely used to prevent customers from these kinds of site from stealing data.

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?

This System detect whether the website is phishing website or not in a early stage if the website is a phishing website it gives an alert message to the user.

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?

Scammers try to gain access to victims' sensitive information by masquerading as a reputable organization or person. The phisher obtains basic information of the targeted user by creating a real website that looks like a genuine website, or by hacking a real website. This site can be a social media site or a lottery site or any promotional site. Thus, a phisher relies on building trust, so that the victim believe that he/she is in contact with a reputable entity. A phisher might use tricks, persuasion, visceral influence, and/or any other technique to gain a user's trust.

7. BEHAVIOUR BE

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

- Know what a phishing scam looks like.
- Don't click on every link.
- Get free anti-phishing add-ons
- Rotate passwords regularly
- Don't ignore updates
- Install firewalls
- Don't be tempted by pop-ups
- Don't give your information to an unsecured site

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

Identify

3. TRIGGERS

TR

What triggers customers to act?

The ever-evolving social engineering attacks, the difficulty to track down cybercriminals because of the anonymity nature of the internet and the suspicious characteristics of URL's.

4. EMOTIONS: BEFORE / AFTER

E

M

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

Before: The user felt insecure to use internet and doubtful about their privacy.

After: They feel very secure to provide their he/she sensitive information to a website.

10. YOUR SOLUTION

Our solution is to build an efficient and intelligent system to detect phishing sites by applying a machine learning algorithm which implements classification algorithms and techniques to extract the phishing datasets criteria to classify their legitimacy.

8. CHANNELS of BEHAVIOUR

CH

8.1 ONLINE

What kind of actions do customers take online?

All the phishing scams occurs online.so, the customer tends to lose their data to phishing site.

8.2 OFFLINE

What kind of actions do customers take offline?

Offline attacks are also possible. An attacker can eavesdrop or watch keystrokes pressed by the customer to get sensitive credentials to start the attack.