Project Title: WEB PHISHING DETECTION **Project design Phase - 1** **Team ID: PNT2022TMID44414**

Define CS, fit into CC

1. CUSTOMER SEGMENT(S)

CS

1.The main customer focus is on people who use the internet for e-transactions and banking organizations where safeguarding customers data is important and vital.

CC

6.CUSTOMER CONSTRAINTS

1.Lacking basic knowledge verifying the correct URL of the webpages
2. Malwares have become more complex then what a lav man can understand

5. AVAILABLE SOLUTIONS

AS

1.Using a good antivirus software or an anti-phishing toolbar which are available as extension in browsers. Verifying the websites privacy policy and ensuring the websites are SSL certified
2.Double checking the domain name
3.Anti-Spam Softwear and Blacklisting

Explore AS, differentiate

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

2. JOBS-TO-BE-DONE / PROBLEMS

J&P

1.The phishing websites must be detected prior and should be blacklisted.
2.Building a phishing URL detection website where the user can copy paste the URL and find if the URL is legitimate.
3. Companies tryst is broken if private data of customers are leaked.

9. PROBLEM ROOT CAUSE

RC

1.Lack of basic awareness among the common folk and leniency in the adaption of new security measures
2.Low-cost phishing and ransom ware tools are easy to get hold of

7. BEHAVIOUR

BE

1.Customer should take a “trust no one” approach when opening an email and should always verify the “From” address of the email.
2.Be wary of generic salutations in an email. Legitimate companies, especially those with which you have accounts or have done business typically will address you by name versus by a generic greeting.

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

3. TRIGGERS

TR

1.To prevent data including login credentials and credit card numbers from getting stolen.

2.Seeing others lose money due to phishing and their reputation getting damaged. This increases the awareness of the person

10. YOUR SOLUTION

SL

1.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 webpages and gives a warning message.

2.Machine Learning based approaches rely on classification algorithms such SVM and DT to train a model that can later automatically classify the fraudulent websites at run-time without any human intervention

8.CHANNELS OF BEHAVIOR

CH

ONLINE

1.By using appropriate firewalls and not clicking random pop ups in browsers and in email links.

OFFLINE

1.Not sharing confidential information in spam phone calls or in random messages.

Identify strong TR & EM

4.EMOTIONS: BEFORE / AFTER EM **Before** 1 .They feel threatened and insecure using the internet. 2. Anxiety and stress are also other emotions. Experienced. **After:** 1.Stress free and a sense of security knowing that their personal data is protected.	3.The real-time prediction includes whitelist filtering, blacklist interception, and 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.	2.Raising awareness by conducting small camps in your locality among the elderly and people who have less computer knowledge.