Project Title: Web Phishing detection **Project Design Phase-I - Solution Fit Template** **Team ID:**PNT2022TMID44340

Define CS, fit into CC

1. CUSTOMER SEGMENT(S) CS

- Online payment service users
- Internet based financial services business
- Retail services

6. CUSTOMER CONSTRAINTS CC

- Not knowing how to protect them and identify malicious
- Human are prone to make errors
- Insufficient backup processes, lack of user testing by organization as they require more resources, money
- Organization don't flow BYOD – Bring your own device concept for individual employee
- Malware have become more complex than what a layman can understand
- Phishing tools are low-cost and widespread.

5. AVAILABLE SOLUTIONS AS

- Use VPN, incognito mode
- Check for spelling mistakes in URL
- Perform regular scans
- Verify the websites privacy policy
- Always type the websites URL
- Double check the domain name and age
- 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

- websites with link that contain malware
- Saying that they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you need to confirm some personal or financial information
- include an invoice you don't recognize
- want you to click on a link to make a payment — but the link has malware

9. PROBLEM ROOT CAUSE RC

- Individuals are the weakest link
- Lack of training and awareness about phishing and ransomware
- Organization are not performing sufficient due diligence
- Criminals are well funded to develop technical skills for more sophisticated attacks
- Scammers demand ransom from affected individuals or organizations

7. BEHAVIOUR BE

- Using Instant firewalls
- By not being tempted to click any pop ups
- To rotate password regularly
- By not clicking on the link from unknown mails or instant messages

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

3. TRIGGERS

TR

- Loss of money
- Loss of intellectual property
- damage to reputation,
- disruption of operational activities

4. EMOTIONS: BEFORE / AFTER

EM

Before: Fear about phisihing.
After: They loss all sensitive informations.

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 intervention.

8. CHANNELS of BEHAVIOUR

CH

8.1 ONLINE

Using firewalls
By not clicking random pop ups
using unsecure wifi for online transactions
using incognito and VPNs

8.2 OFFLINE

Nothing accessible during offline.