Project Title: WEB PHISHING DETECTION

Project Design Phase-I - Solution Fit

Team ID: PNT2022TMID27012

Define CS, fit into CC

1. CUSTOMER SEGMENT(S)

CS

General user

ATM user

Design user

Gamer

Tester

6. CUSTOMER CONSTRAINTS

CC

a. Lack of security

b.Anxious for the personal details are robbed.

c.Doubtful

d.Hit or Pass for other website

e.Nervous of the outcome

5. AVAILABLE SOLUTIONS

AS

a. Protecting by using security software
Apps such as AVANAN, IRONSCALES, ABNORMAL..atc
Likewise Avanan offers cloud-based email and application protection against sophisticated phishing, malware, account compromise and data loss attacks. Designed to work with Office 365 and G Suite, you can deploy Avanan's solution in minutes as an Office 365 app or configure it manually with a fast and simple deployment process. Once deployed, it offers security for all connected cloud-based applications like OneDrive, Google Drive and Teams.

b.Using multi factor authentication

c.Backing up for data

Explore AS, differentiate

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

2. JOBS-TO-BE-DONE / PROBLEMS

J&P

a.Phishing has a list of negative effects on a business, including **loss of money, loss of intellectual property, damage to reputation, and disruption of operational activities**.

b.These effects work together to cause loss of company value, sometimes with irreparable repercussions.

9. PROBLEM ROOT CAUSE

RC

a. Lack of security awareness

b. Criminals on money

c. Not performing sufficient

d. Malware is sophisticated

e. Low cost phishing tools

7. BEHAVIOUR

BE

a. Reporting the problem

b. Deleting accounts

c. Contact the person involved in phishing

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

3. TRIGGERS

TR

a. Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim by opening an email, instant message.

b. Phishing tricks victims into giving over credentials for all sorts of sensitive accounts, such as email, corporate intranets and more. Even for cautious users, it's sometimes difficult to detect a phishing attack.

4. EMOTIONS: BEFORE / AFTER

EM

Despair, nervous, lack of confidence, loss

10. YOUR SOLUTION

SL

a.BEFORE PHISHING ATTACK HAPPENS:

Inspection on the new websites, emails and other social media invitations that require filling of personal details should be wisely checked through various software tools like VPN, firewall, security...etc.

a.AFTER PHISHING ATTACK HAPPENS:

Report the actions by giving a solid complaint.

By scanning, by getting the details of the criminal through using a phishing tool against them could also be another solution through valid authority and without breaking the code.

8.CHANNELS of BEHAVIOUR

CH

8.1 ONLINE

a. Reporting the problem
b. Deleting accounts
c. Contact the person involved in phishing

8.2 OFFLINE

a. Police complain

b. Report to the organization in person

Identify strong TR & EM