Project Title: WEB PHISHING DETECTION **Project Design Phase-I - Solution Fit Template** **Team**

ID: PNT2022TMID15184

Define CS, fit into CC

1. CUSTOMER SEGMENT(S)

The Participants are mostly between the ages of 18 to 25 all young people. Participants may also vary from different age groups.

6. CUSTOMER CONSTRAINTS

Tips to Prevent Phishing Attacks

1.Know what a phishing scam looks like
2.Don't click on that link.
3.Get free anti-phishing add-ons.
4.Don't give your information an unsecured site.
5.Rotate passwords regularly.
6.Don't ignore those updates.
7.Install firewalls.
8.Don't be tempted by those pop-ups

5. AVAILABLE SOLUTIONS

We can find solution for phishing attacks by phishing detection websites Use anti-phishing protection and anti-spam software to protect yourself when malicious messages slip through to your computer. Anti-malware is included to prevent other types of threats. Similar to anti-spam software, anti-malware software is programmed by security researchers to spot even the stealthiest malware.

Explore AS, differentiat

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

2. JOBS-TO-BE-DONE / PROBLEMS

Malicious links will lead to a website that often steals login credentials or financial information like credit card numbers. Attachments from phishing emails can contain malware that once opened can leave the door open to the attacker to perform malicious behavior from the user's computer.

9. PROBLEM ROOT CAUSE

A phishing campaign tries to get the victim to do one of two things: Hand over sensitive information. These messages aim to trick the user into revealing important data often a username and password that the attacker can use to breach a system or account.

7. BEHAVIOUR

Phishing is described as a fraudulent activity that is done to steal confidential user information such as credit card numbers, login credentials, and passwords. It is usually done by using email or other forms of electronic communication by pretending to be from a reliable business entity.

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

3. TRIGGERS

Customers get triggers when phishing attacks are the practice of fraud communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine.

4. EMOTIONS: BEFORE / AFTER

From every phishing incident that has ever taken place in history, one constant effect is financial loss. First is the direct loss from transferred funds by employees who were fooled by the hackers. Second is the fines for non-compliance imposed by regulatory bodies like HIPAA, PCI, and PIPEDA, among others.

10. YOUR SOLUTION

Web phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by masquerading as a trustworthy website on the Internet. Researchers present some solutions to detect web phishing as follows. So we tend to provide a phishing detection website which can help customers to check the malicious websites and be aware of the phishing attackers. These days phishing attacks can be done in various ways like Email, social media, bank accounts, and URLs.

8. CHANNELS of BEHAVIOUR

ONLINE:

Report it. Forward phishing emails to **reportphishing@apwg.org** (an address used by the Anti-Phishing Working Group, which includes ISPs, security vendors, person financial institutions, and law enforcement agencies). Let the company or that was impersonated know about the phishing scheme.

OFFLINE:

To overcome phishing attack we can go to near by public service centers and report a file on the attack

Identify