Project Design Phase-I
Problem – Solution Fit Template

Date	19 September 2022
Team ID	PNT2022TMID52622
Project Name	Project - Web Phishing Detection
Maximum Marks	2 Marks

Problem – Solution Fit Template:

The Problem-Solution Fit simply means that you have found a problem with your customer and that the solution you have realized for it actually solves the customer's problem. It helps entrepreneurs, marketers and corporate innovators identify behavioral patterns and recognize what would work and why

Purpose:

- ✈ Solve complex problems in a way that fits the state of your customers.
- ✈ Succeed faster and increase your solution adoption by tapping into existing mediums and channels of behavior.
- ✈ Sharpen your communication and marketing strategy with the right triggers and messaging.
- ✈ Increase touch-points with your company by finding the right problem-behavior fit and building trust by solving frequent annoyances, or urgent or costly problems.
- ✈ **Understand the existing situation in order to improve it for your target group.**

Template:

Problem-Solution fit canvas 2.0

Purpose / Vision To detect phishing sites.

Define CS, fit into CC

1. CUSTOMER SEGMENT(S) CS

Who is your customer?
i.e. working parents of 0-5 y.o. kids

Everyone who uses Internet will be our target. This can include:

- Individual
- Family
- Company
- Government

The customers can be of any age group and can belong to any nationality. This application will be used by anyone who surfs online.

6. CUSTOMER CONSTRAINTS CC

What constraints prevent your customers from taking action or limit their choices of solutions? i.e. spending power, budget, no cash, network connection, available devices.

Novel phishing approaches suffer low detection accuracy. The most common technique used is the blacklist-based method. It has become inefficient since registering a new domain has become easier. No comprehensive blacklist can ensure a perfect up-to-date database.

5. AVAILABLE SOLUTIONS AS

Which solutions are available to the customers when they face the problem or need to get the job done? What have they tried in the past? What pros & cons do these solutions have? i.e. pen and paper is an alternative to digital notetaking

The solutions that are available detect phishing sites:

- by using a blacklist and whitelist
- by using hyperlinks
- by inspecting the various URL components
- page content inspection

All of these techniques suffer low detection accuracy and high false alarm. Blacklist-based method is inefficient in responding to emanating phishing attacks since registering new domain has become easier, no comprehensive blacklist can ensure a perfect up-to-date database.

Explore AS, differentiate

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

2. JOBS-TO-BE-DONE / PROBLEMS J&P

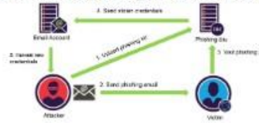
Which jobs-to-be-done (or problems) do you address for your customers?
There could be more than one; explore different sides.

- An efficient and intelligent system is designed 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.
- This system will intelligently provide all necessary details to the user to convince them if a site is genuine or not.

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?
i.e. customers have to do it because of the change in regulations.

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 users by creating a real website that looks like the 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 believes that she/he 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?
i.e. directly related: find the right solar panel installer, calculate usage and benefits; indirectly associated: customers spend free time on volunteering work (i.e. Greenpeace)

- Know what a phishing scam looks like
- Don't click on every link
- Get free anti-phishing add-ons
- Don't give your information to an unsecured site
- Rotate passwords regularly
- Don't ignore updates
- Install firewalls
- Don't be tempted by pop-ups
- Don't give out important information unless you must
- Have a Data Security Platform to spot signs of an attack

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

Identify strong TR & EM

3. TRIGGERS TR

What triggers customers to act? i.e. seeing their neighbour installing solar panels, reading about a more efficient solution in the news.

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 URLs.

4. EMOTIONS: BEFORE / AFTER EM

How do customers feel when they face a problem or a job and afterwards?
i.e. lost, insecure > confident, in control - use it in your communication strategy & design.

BEFORE: doubtful and anxious about their privacy
AFTER: sense of safety whenever he/she attempts to provide sensitive information to a site

10. YOUR SOLUTION SL

If you are working on an existing business, write down your current solution first, fill in the canvas, and check how much it fits reality.
If you are working on a new business proposition, then keep it blank until you fill in the canvas and come up with a solution that fits within customer limitations, solves a problem and matches customer behaviour.

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? Extract online channels from #7

All the phishing scams occur online. So, whatever a customer does is a trap if he/she is not cautious.

8.2 OFFLINE
What kind of actions do customers take offline? Extract offline channels from #7 and use them for customer development.

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

Extract online & offline CH of BE

References:

1. https://www.ideahackers.network/problem-solution-fit-canvas/
2. https://medium.com/@epicantus/problem-solution-fit-canvas-aa3dd59cb4fe