# Problem-Solution Fit canvas

Purpose / Vision

Version:

Define CS, fit into CL

## 1. CUSTOMER SEGMENT(S) CS

The customer segmentation model was specifically designed for pre-paid subscriber-base. The segmentation model built on these features could now split the subscriber-base according to combinations of average revenue per user(ARPU) , dormancy,gender, package and usage which allowed handling each segment a per its subscribers' usage pattern.

## 6. CUSTOMER LIMITATIONS EG. BUDGET, DEVICES CL

What limits your customers to act when problem occurs?
Spending power, budget, no cash, network connection, Available devices?

Know what a phishing scam looks like.Don't click on that link. Get free anti-phishing add-ons.Don't give your information to an unsecured site. Rotate passwords regularly.Don't ignore those updates. Install firewalls.Don't be tempted by those pop-us.

## 5. AVAILABLE SOLUTIONS PLUSES & MINUSES AS

We focus on safely handling emails do manage to breach the security softwarelayer .Access the impacts of cyber security awareness training segment phishing simulation.

Explore AS, differentiate

Focus on PR, tap into BE, understand RC

## 2. PROBLEMS / PAINS + ITS FREQUENCY PR

Damage to reputation, disruptional operational activities.loss of money loss of intellectual property.loss of company value ,with irrepairable repercussions.

## 9. PROBLEM ROOT / CAUSE RC

Phishing detection techniques do suffer low detection accuracy and high false alarm especially when novel phishing approaches are introduced. Besides, the most common technique used, blacklist-based method is inefficient in responding emanating phishing attacks since registering new domain has become easier, no comprehensive blacklist can ensure a perfect up-to-date database. Furthermore, page content inspection has been used by some strategies to overcome the false negative problems and complement the vulnerabilities of the stale lists. Moreover, page content inspection algorithms each have different approach to phishing website detection with varying degrees of accuracy.

## 7. BEHAVIOR + ITS INTENSITY BE

Anti-spyware and firewall settings should be used to prevent phishing attacks and users should update the programs regularly.Firewall protection prevents access to malicious files by blocking the attacks.Antivirus software scans every file which comes through the internet to your computer.

Focus on PR, tap into BE, understand RC

## 3. TRIGGERS TO ACT TR

Assume every email is a phishing attempt.Check and verify email address.Read and emails carefully.Check grammar and spelling.Look for your name.Watch out for emails containing unusual requests.Be wary of links and attachments.

## 10. YOUR SOLUTION SL

Increase your alertness to phishing risks Install a cyber security culture and create cyber security heroes.Identify fraudulent emails but also provide specific guidance on how to handle suspect communications.

## 8. CHANNELS of BEHAVIOR CH

Since a user profile contains confidential user information, it is important that it does not add new security risks. We use a one-way secure hash function to hash the confidential data before it is stored. When the system needs to determine the equivalence between the data, the system just needs to compare the hash values.