

Define CS, fit into CC	<b>1. CUSTOMER SEGMENT(S)</b> <b>CS</b> This is mainly designed for the classification of user. Mainly for users who are prepaid users. The users are mainly classified based on the criteria of age, gender, subscription, regulations, etc...	<b>6. CUSTOMER CONSTRAINTS</b> <b>CC</b> Phishing attacks have become so realistic that even the most cyber-aware recipient can be fooled into providing sensitive information. Don't ignore any of the updates, don't give your information to any of the unsecured site.	<b>5. AVAILABLE SOLUTIONS</b> <b>AS</b> To prevent phishing of people data something like anti-spyware and firewall should be used so that we can safeguard our data. They prevent data by blocking them. People and programmers should update their programs and system so data can be prevented from hacked.	Explore AS, differential
	<b>2. JOBS-TO-BE-DONE</b> <b>J&amp;P</b> Measures to avoid phishing of data include keep informed about phishing techniques, think before you click, install an anti-phishing toolbar, verify a site's security, check your online accounts regularly, use firewalls, be wary of pop-ups, use antivirus software and keep your browser up to date.	<b>9. PROBLEM ROOT CAUSE</b> <b>RC</b> Lack of security awareness among people is one of the most main reason for phishing. Organization should be aware of how the benefits and purpose of security awareness training can secure their employees from falling victim to phishing attack.	<b>7. BEHAVIOUR</b> <b>BE</b> The thing or the behaviour of phishing site is that it looks extremely similar to a legitimate site and that it has at least one field to enable users to input their credentials.	

<b>3. TRIGGERS</b> <b>TR</b> There are many ways to trigger. Some of them are installing unsecured and unsafe applications, opening emails and messages sent by unknown. Some mail contain spelled error words that are the signs of malicious messages.	<b>10. YOUR SOLUTION</b> <b>SL</b> We should be aware of hackers and phishing, everyone should have a knowledge of internet and consequences. We should on click on any links sent by unknown and we should not open any fraudulent texts.	<b>8. CHANNELS of BEHAVIOUR</b> <b>CH</b> The user will have a more data and thing that are highly confidential and it should not be shared with anyone so some security should be added to it so that it could be prevented.
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	<div data-bbox="152 63 454 89"><b>4. EMOTIONS: BEFORE / AFTER</b></div> <div data-bbox="721 59 761 90"><b>EM</b></div> <div data-bbox="152 97 790 201"><p>BEFORE: Everything will be in normal condition.</p><p>AFTER: People feel insecure , they won't be able to concentrate on their regular duties and the data they lost can be flashed by the hacker.</p></div>			
--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--