







Define CS, fit into CC	<b>1. CUSTOMER SEGMENT(S)</b>  <ul style="list-style-type: none"><li>● Business Organization</li><li>● Online Banking Sector</li><li>● Those who use Websites and URL's for surfing through internet</li></ul>	<b>6. CUSTOMER CONSTRAINTS</b>  <p>Provides full access to scan the transaction process of the user and no breakdown of server connections</p>	<b>5. AVAILABLE SOLUTIONS</b>  <p>This is applied to three different machine learning classifier - support vector machine, logistic regression and Naive Bayes. After training and testing the algorithms, it is observed that Naive Bayes classifier recorded the highest accuracy</p>	Explore AS, differentiate
	<b>2. JOBS-TO-BE-DONE / PROBLEMS</b>  <p>To identify the phishing sites and to protect users Credentials from hackers</p>	<b>9. PROBLEM ROOT CAUSE</b>  <p>Having the data without any protection using anti phishing technologies, So that attacker creates fake website and steal the data.</p>	<b>7. BEHAVIOUR</b>  <p>Customer finds the web phishing detection websites or applications and also the customer should provide all the transaction details of whole process .</p>	
Focus on J&P, tap into BE, understand RC				Focus on J&P, tap into BE, understand RC

<div>3. TRIGGERS<div>TR</div></div> <div>Customer will get triggered because of data get stolen, theft of money and loss of privacy.</div>	<div>10. YOUR SOLUTION<div>SL</div></div> <div>The links that gets checked for identifying phishing ,and we will be using various algorithm for making accurate prediction. Especially we are using Ada Boost Algorithm to make high accuracy prediction.</div>	<div>8.CHANNELS of BEHAVIOR<div>CH</div></div> <div>8.1 ONLINE</div> <div>Pass the URL as input and identify whether it is a phishing site or not.</div> <div>8.2 OFFLINE</div> <div>Using the phishing detection application to predict the phishing sites in offline mode(offload the app).</div>
<div>4. EMOTIONS: BEFORE / AFTER<div>EM</div></div> <div><b>BEFORE :</b> Believing that the data is protected and secured in the Organization. <b>AFTER :</b> Feeling depressed as the data and money have been stolen.</div>		