

Define CS, fit into CC	<b>1. CUSTOMER SEGMENT(S)</b> <b>CS</b> <ul style="list-style-type: none"><li>Millions of internet users use websites daily.</li><li>Websites such as e-commerce, banking, social media requires login credentials to access it</li></ul>	<b>6. CUSTOMER CONSTRAINTS</b> <b>CC</b> <ul style="list-style-type: none"><li>Lack of awareness in cybersecurity</li><li>Unaware of phishing attacks</li><li>Difficult in identifying phishing websites</li></ul>	<b>5. AVAILABLE SOLUTIONS</b> <b>AS</b> <ul style="list-style-type: none"><li>Seeking help with cybersecurity professionals</li><li>Cross checking the link with phishing database manually</li><li>Seeking solutions via social media</li></ul>	Explore AS, differentiate
	<b>2. JOBS-TO-BE-DONE / PROBLEMS</b> <b>J&amp;P</b> <ul style="list-style-type: none"><li>Analyze the URL links, phishing attacks and collection of datasets</li><li>Pre-processing and building an machine learning model to classify whether it is a phishing website or not</li><li>Building a website</li></ul>	<b>9. PROBLEM ROOT CAUSE</b> <b>RC</b> <ul style="list-style-type: none"><li>Growth in technology and growth in many number of users leads to do hackers/hacker groups to involve in malicious activities</li><li>Greed for money</li></ul>	<b>7. BEHAVIOUR</b> <b>BE</b> <ul style="list-style-type: none"><li>Using a website/extension to know about the entered URL is legitimate or not</li><li>Avoids theft of user credentials/information</li></ul>	

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

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

Identify strong TR & EM	<p>3. TRIGGERS <span>TR</span></p> <ul style="list-style-type: none"> <li>Scams which are increasing day-to-day</li> <li>Social Media</li> </ul>		<p>10. YOUR SOLUTION <span>SL</span></p> <ul style="list-style-type: none"> <li>A method which analyzes phishing website or not by using machine learning algorithms and also building a model with the machine learning algorithm.</li> <li>Integrating the built model with flask to create a website</li> <li>Hosting the application in IBM cloud</li> </ul>	<p>8. CHANNELS of BEHAVIOUR <span>CH</span></p> <p>8.1 Online:</p> <ul style="list-style-type: none"> <li>Using website to identify phishing website or not by entering the link and getting the result.</li> <li>Reporting the phishing site</li> </ul> <p>8.2 Offline:</p> <ul style="list-style-type: none"> <li>Creating awareness among the public</li> <li>File an complain to cybersecurity team</li> </ul>	Identify strong TR & EM
	<p>4. EMOTIONS: BEFORE / AFTER <span>EM</span></p> <ul style="list-style-type: none"> <li><b>Before:</b> Fear of insecurity, vulnerable to various cyber threats or attacks</li> <li><b>After:</b> No fear in theft of privacy, secure browsing in internet</li> </ul>				