

Define CS, fit into CC	<b>1. CUSTOMER SEGMENT(S)</b> <ul style="list-style-type: none"> <li>In order to do e-banking and other type of payments online a webpage for an online platform is required</li> <li>Hackers/cyber thieves use this to their advantage and scams using web phishing sites</li> <li>These sites are hardly distinguishable from real sites in their appearance</li> </ul>	<b>6. CUSTOMER CONSTRAINTS</b> <ul style="list-style-type: none"> <li>It is hard for the users to e-banking and to do any kind of online transactions due to the possibility of entering a phishing site</li> <li>This led the user to lose money and confidential information to scams</li> <li>Thus, preventing them from using any kind of online transaction portals and banking</li> </ul>	<b>5. AVAILABLE SOLUTIONS</b> <ul style="list-style-type: none"> <li>To find these sites based on appearance is almost impossible hence we need a different method</li> <li>So, URL are used to find these sites using a blacklisting method they are stopped by the windows defender and helps the user from entering using warning</li> </ul>	Explore AS, differentiate
Focus on J&P, tap into BE, understand RC	<b>2. JOBS-TO-BE-DONE/PROBLEMS</b> <ul style="list-style-type: none"> <li>Blacklisting requires that the developer to update the newly added phishing site URL to the list every time a new one is discovered</li> <li>Thus, they cannot defend/protect the user from newly built of phishing web sites</li> <li>Which led to the issue again because when the hackers know that the sites are been discovered they change its URL to avoid detection</li> </ul>	<b>9. PROBLEM ROOT CAUSE</b> <ul style="list-style-type: none"> <li>Main problem in blacklisting is that it cannot stop fresh or zero-hour phishing attack</li> <li>And the list is need to be updated regularly to reduce the damage cause by web phishing</li> <li>So, this method can only reduce or stop the phishing after one or many users are attacked thus it is not an effective method</li> </ul>	<b>10. BEHAVIOUR</b> <ul style="list-style-type: none"> <li>The users need to report phishing sites to cyber security dept or respective offices</li> <li>So that it can be added to blacklist</li> <li>This not only inefficient some users even don't report it and they stop using the platforms altogether</li> </ul>	Focus on J&P, tap into BE, understand RC
Identify Strong TR & EM	<b>3. TRIGGERS</b> <ul style="list-style-type: none"> <li>User's financial losses are really huge due to web phishing.</li> <li>Not only individuals even big companies are affected.</li> <li>It also leads to confidential information loss</li> </ul> <b>4. EMOTIONS: BEFORE/AFTER</b> <ul style="list-style-type: none"> <li>BEFORE: Users were unsatisfied and highly anxious to use e-banking and online payment platforms.</li> <li>AFTER: They find it comfortable and secured to use e-banking and other transaction.</li> </ul>	<b>10. YOUR SOLUTION</b> <ul style="list-style-type: none"> <li>The solution proposed is to use a ML based system to detect the web phishing sites.</li> <li>Since the URLs can be treated as string, they can be split into different parts based on they attribute and features.</li> <li>Based on that we build a classification-algorithm based ML model to identify the web phishing site URLs.</li> <li>Its effectiveness can be automatically improved by training it at regular intervals.</li> </ul>	<b>8. CHANNELS of BEHAVIOUR</b> <b>8.1 ONLINE</b> <ul style="list-style-type: none"> <li>Users are avoiding to use e-banking sites form link provided through mails and message due to fear of phishing</li> </ul> <b>8.2 OFFLINE</b> <ul style="list-style-type: none"> <li>Users are visit banks even though they are busy and have even take leave from work</li> </ul>	Extract online & offline CH of BE