

Define CS, fit into CC	<div>1.CUSTOMER SEGMENT(S)<div>CS</div></div> <div>The people or organization who required safe browsing.</div>	<div>6. CUSTOMER CONSTRAINTS<div>CC</div></div> <div>Phishers have also started to develop a psychology behind their emails that plays off urgency, greed or trust. Combined with the legitimate look and feel of the spoofed websites, even more cautious and aware users can fall vic-tim to their attacks”</div>	<div>5. AVAILABLE SOLUTIONS<div>AS</div></div> <div>Use anti-phishing protection and anti-spam software to protect yourself when malicious messages slip through to your computer. Anti-malware is included to prevent other types of threats. Similar to anti-spam software, anti-malware software is programmed by security researchers to spot even the stealthiest malware</div>	Explore AS, differentiate
	<div>2. JOBS-TO-BE-DONE / PROBLEMS<div>J&P</div></div> <div><div>a. Classify phishing and non phishing website.</div><div>b. Identifying phishing website</div><div>c. Which algorithm should be use to identify the phishing website more accurately.</div><div>d. how to protect our website.</div></div>	<div>9. PROBLEM ROOT CAUSE<div></div></div> <div>The largest door being opened for cyber criminals is, without a doubt, the one labelled with "security awareness". More specifically, a lack of employee training focusing on issues such as phishing and ransomware is the main reason for these attacks being so successful.</div>	<div>7. BEHAVIOUR<div></div></div> <div>Phisher creates informational websites that provide valuable information to the user. These websites also provide links to connect to Facebook, Gmail, and Twitter. These links redirect the user to phished websites instead of the authentic websites. To maintain the user’s confidence in deceptive links, phishers generally use link manipulation techniques</div>	
Identify strong TR & EM	<div>3. TRIGGERS<div>TR</div></div> <div>Hacking of confidential Data from an organization. Hack the bank informations which may leads to loss of money.</div>	<div>10. YOUR SOLUTION<div>SL</div></div> <div>To detect and predict e-banking phishing website be purpose intelligence, flexible and effective system that is based on classification Algorithms.</div>	<div>8.CHANNELS of BEHAVIOUR<div>CH</div></div> <div>Online; Using classification algorithm to predict the phishing website and alert a customer.. Offline ; No thread will be during offline...</div>	Identify strong TR & EM
	<div>4. EMOTIONS: BEFORE / AFTER<div>EM</div></div> <div>Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.</div>			

