

Define CS, fit into CC	<p>1. CUSTOMER SEGMENT(S) CS</p> <ul style="list-style-type: none"> Online payment service users Internet based financial services business Retail services 	<p>6. CUSTOMER CONSTRAINTS CC</p> <ul style="list-style-type: none"> Lack of awareness about web phishing Human are prone to make errors Insufficient backup processes, lack of user testing by organization as they require more resources, money Organization don't flow BYOD – Bring your own device concept for individual employee Malware have become more complex than what a layman can understand Phishing tools are low-cost and widespread. 	<p>5. AVAILABLE SOLUTIONS AS</p> <ul style="list-style-type: none"> Use VPN, incognito mode Check for spelling mistakes in URL Perform regular scans Verify the websites privacy policy Always type the websites URL Double check the domain name and age Check for site seals Check whether right click is enabled Run website through website checker Check your browser for google's transparency report 	Explore AS, differentiate
Focus on J&P, tap into BE, understand RC	<p>2. JOBS-TO-BE-DONE / PROBLEMS J&P</p> <ul style="list-style-type: none"> websites with link that contain malware Saying that they've noticed some suspicious activity or log-in attempts claim there's a problem with your account or your payment information say you need to confirm some personal or financial information include an invoice you don't recognize want you to click on a link to make a payment — but the link has malware 	<p>9. PROBLEM ROOT CAUSE RC</p> <ul style="list-style-type: none"> Individuals are the weakest link Lack of training and awareness about phishing and ransomware Organization are not performing sufficient due diligence Criminals are well funded to develop technical skills for more sophisticated attacks Scammers demand ransom from affected individuals or organizations 	<p>7. BEHAVIOUR BE</p> <ul style="list-style-type: none"> Using Instant firewalls By not being tempted to click any pop ups To rotate password regularly By not clicking on the link from unknown mails or instant messages 	Focus on J&P, tap into BE, understand RC

<div>3. TRIGGERS</div> <div>TR</div> <ul style="list-style-type: none"> • Loss of money • Loss of intellectual property • damage to reputation, • disruption of operational activities 	<div>10. YOUR SOLUTION</div> <div>SL</div> <p>A deep learning-based framework by implementing it as a browser plug-in capable of determining whether there is a phishing risk in real-time when the user visits a web page and gives a warning message. The real-time prediction includes whitelist filtering, blacklist interception, and machine learning (ML) prediction.</p> <p>To deal with phishing attacks and distinguishing the phishing webpages automatically, Blacklist based detection technique keeps a list of websites' URLs that are categorized as phishing sites. If a web-page requested by a user exists in the formed list, the connection to the queried website is blocked.</p> <p>Machine Learning (ML) based approaches rely on classification algorithms such as Support Vector Machines (SVM) and Decision Trees (DT) to train a model that can later automatically classify the fraudulent websites at run-time without any human intervention.</p>	<div>8. CHANNELS of BEHAVIOUR</div> <div>CH</div> <div>8.1 ONLINE</div> <p>Using firewalls</p> <p>By not clicking random pop ups</p> <p>using unsecure wifi for online transactions</p> <p>using incognito and VPNs</p>
<div>4. EMOTIONS: BEFORE / AFTER</div> <div>EM</div> <ul style="list-style-type: none"> • Insecure • Incautious • Hasty • Ill repute 		<div>8.2 OFFLINE</div> <p>By not giving confidential information in phone calls</p> <p>Or random messages</p> <p>By not sharing OTPs</p>