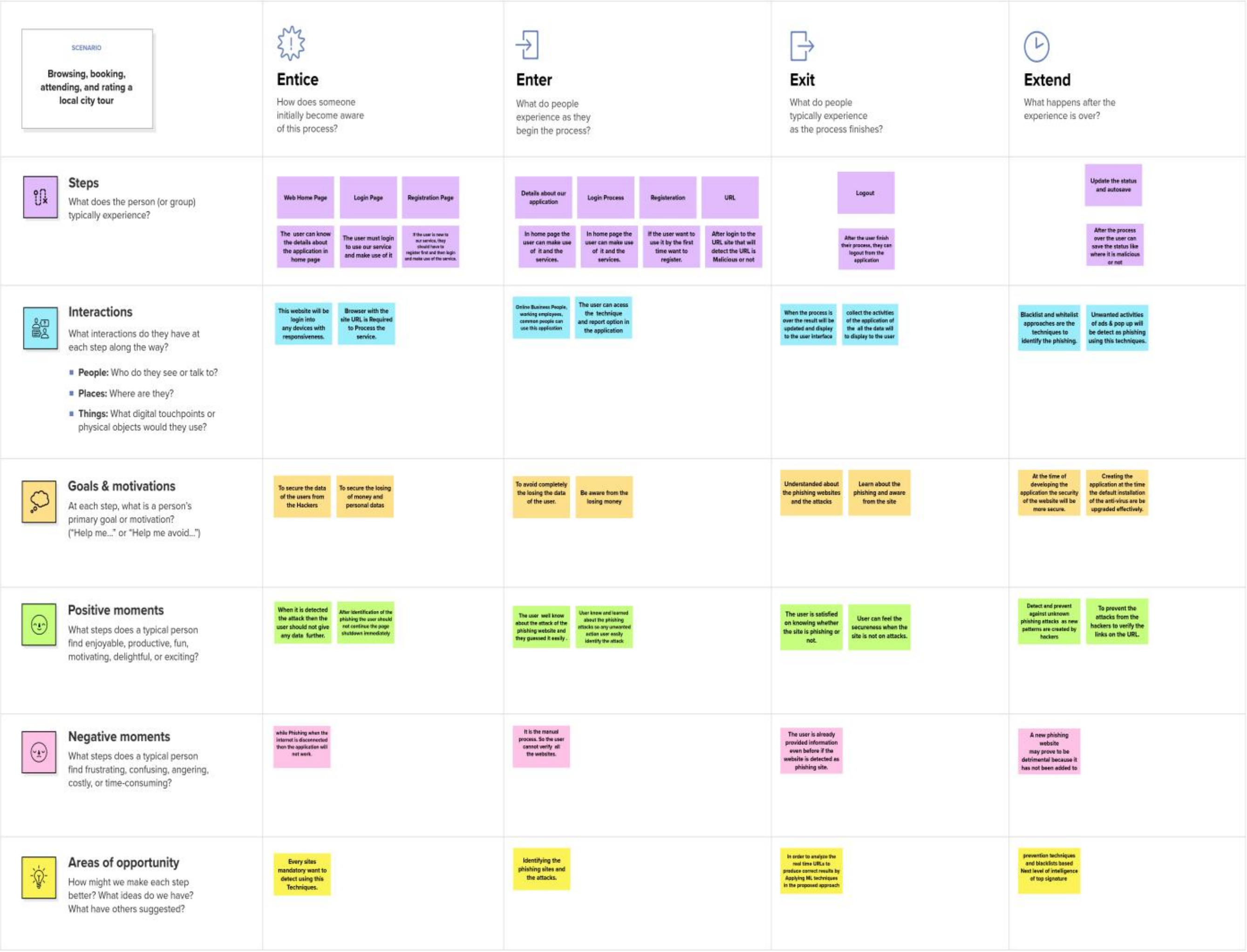
Project Design Phase-II

CUSTOMER JOURNEY

Date	06 October 2022
Team ID	PNT2022TMID29648
Project Name	WEB PHISHING DETECTION
Maximum Marks	4 Marks



SCENARIO Browsing, booking, attending, and rating a local city tour	**Entice** How does someone initially become aware of this process?	**Enter** What do people experience as they begin the process?	**Exit** What do people typically experience as the process finishes?	**Extend** What happens after the experience is over?
Steps What does the person (or group) typically experience?	Web Home Page Login Page Registration Page The user can know the details about the application in home page The user must login to use our service and make use of it If the user is new to our service, they should have to register first and then login and make use of the service.	Details about our application Login Process Registeration URL In home page the user can make use of it and the services. In home page the user can make use of it and the services. If the user want to use it by the first time want to register. After login to the URL site that will detect the URL is Malicious or not	Logout After the user finish their process, they can logout from the application	Update the status and autosave After the process over the user can save the status like where it is malicious or not
Interactions What interactions do they have at each step along the way? **People:** Who do they see or talk to? **Places:** Where are they? **Things:** What digital touchpoints or physical objects would they use?	This website will be login into any devices with responsiveness. Browser with the site URL is Required to Process the service.	Online Business People, working employees, common people can use this application The user can acess the technique and report option in the application	When the process is over the result will be updated and display to the user interface collect the activities of the application of the all the data will to display to the user	Blacklist and whitelist approaches are the techniques to identify the phishing. Unwanted activities of ads & pop up will be detect as phishing using this techniques.
Goals & motivations At each step, what is a person's primary goal or motivation? ("Help me..." or "Help me avoid...")	To secure the data of the users from the Hackers To secure the losing of money and personal datas	To avoid completely the losing the data of the user. Be aware from the losing money	Understanded about the phishing websites and the attacks Learn about the phishing and aware from the site	At the time of developing the application the security of the website will be more secure. Creating the application at the time the default installation of the anti-virus are be upgraded effectively.
Positive moments What steps does a typical person find enjoyable, productive, fun, motivating, delightful, or exciting?	When it is detected the attack then the user should not give any data further. After identification of the phishing the user should not continue the page shutdown immediately	The user well know about the attack of the phishing website and they guessed it easily . User know and learned about the phishing attacks so any unwanted action user easily identify the attack	The user is satisfied on knowing whether the site is phishing or not. User can feel the secureness when the site is not on attacks.	Detect and prevent against unknown phishing attacks as new patterns are created by hackers To prevent the attacks from the hackers to verify the links on the URL.
Negative moments What steps does a typical person find frustrating, confusing, angering, costly, or time-consuming?	while Phishing when the internet is disconnected then the application will not work.	It is the manual process. So the user cannot verify all the websites.	The user is already provided information even before if the website is detected as phishing site.	A new phishing website may prove to be detrimental because it has not been added to
Areas of opportunity How might we make each step better? What ideas do we have? What have others suggested?	Every sites mandatory want to detect using this Techniques.	Identifying the phishing sites and the attacks.	In order to analyze the real time URLs to produce correct results by Applying ML techniques in the proposed approach	prevention techniques and blacklists based Next level of intelligence of top signature