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?

Engage

In the core moments in the process, what happens?

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?

Entice	Enter	Engage	Exit	Extend
Home Page The user can see the details about the application in home page	**Details about our application** The user can explore the features and services of our application in home page	**URL Checking** The entered URL will be checked by passing into the model	**logout** After the user finishes their process, they can logout from the application	**Saving the status** After the report is regenerated, the user can save the status like whether the URL is malicious or not.
Login Page The user must login to use our service	**Login Process** The user should login by entering the credentials in order to detect the URL.	**Using of algorithm** The model will be trained by using suitable algorithm		
Registration Page If the user is new to our service, they should have to register.	**Login Process** If the user is new to our service, they can register by entering the credentials	**Saving the data** The data will be deployed to the front end.		
	Input the URL After login, they can input the URL to detect whether the URL 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?

Entice	Enter	Engage	Exit	Extend
This website will be accessed through any devices with responsiveness.	Business man, working employees, common people can use this application	This website is responsive in any kind of devices	The result will be displayed in the user interface if the process gets complete.	Blacklist and whitelist approaches are the traditional techniques to identify the phishing.
Only the browser, URL is required to process the service.	The user can see the precaution technique and report option	This website is easily accessible		

Goals & motivations

At each step, what is a person's primary goal or motivation? ("Help me..." or "Help me avoid...")

Entice	Enter	Engage	Exit	Extend
To secure the user sensitive data from hackers	To avoid the losing of private data.	To know that the website is malicious or not.	Getting clarified about the phishing websites	Enhance the security of the websites at the time of developing
To avoid losing of money				

Positive moments

What steps does a typical person find enjoyable, productive, fun, motivating, delightful, or exciting?

Entice	Enter	Engage	Exit	Extend
When the site is detected as phishing, the user should not give the data further.	The user is already knows the phishing website and they guessed it.	The user can detect the malicious website by just feeding the input URL to the application	The user is satisfied on knowing whether the site is phishing or not.	Detect and prevent against unknown phishing attacks, as new patterns are created by hackers

Negative moments

What steps does a typical person find frustrating, confusing, angering, costly, or time-consuming?

Entice	Enter	Engage	Exit	Extend
If the internet is disconnected, this application won't work	It is the manual process, So, the user cannot verify for all the websites.	Searching of deleted 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 the blacklist yet

Areas of opportunity

Entice	Enter	Engage	Exit	Extend
Detecting all the sites using this product	Identifying the phishing sites	Facility to report the detected malicious website	Applying ML techniques in the proposed approach in order to analyze the real time URLs and produce correct results.	Next level of intelligence on top of signature based prevention techniques and blacklists