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?

- **The user need to be aware of the phishing website by affected people**
- **The app indicates the user to be aware of being phishing accounts**
- when the person getting to know about phishing website then became more cautious.
- When the user getting the warning the user become alert
- **Entering the URL of the website**
- Report the website if it detected phishing.
- The entered URL is splited and checked for previously reported URLs.
- The entered URL is detected using certain algorithms.
- At the end, the result is shown to the user.
- When the user gets the result of the site , the process gets completed as the site is
- At the end, if the site is detected as the phishing website, the site is reported.

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?

- Safe Browsing by using this detection technique.
- Only browser, a URL and internet facility are required
- They can see a search engine, precausion techniques, report option.
- Used by working employees, Businessmen, common people.
- this is a website, so it can be easily accesible
- When the process completes, result is displayed.
- Blacklist and Whitelist approaches are the traditional methods to identify the phishing

Goals & motivations

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

- To avoid thefting of information
- To avoid losing of money
- To reduce the loss of privacy data
- To know the website is legitimate or not
- Getting clarifed about the doubtful websites
- Enhance the security of the websites at the time of Developing

Positive moments

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

- when the detected site is a phishing website, and user doesn't give any information
- You already know it is a phishing site and You guessed it
- Detects the malicious websites by simply using the URLs.
- Satisfed on knowing that the site is phishing website or not.
- Detect and prevent against unknown phishing attacks, as new patterns are created by attackers.

Negative moments

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

- If Internet connection fails, this system won't work
- being a manual process and the users cannot verify for all the websites that he visits
- Searching of deleted websites
- when the detected site is phishing website but the user already provided information
- a new phishing website may prove to be detrimental because it has not been added to the blacklist yet

Areas of opportunity

How might we make each step better? What ideas do we have? What have others suggested?

- 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 effective results
- Next level of intelligence on top of signaturebased prevention techniques and blacklists