Document an existing experience

Narrow your focus to a specific scenario or process within an existing product or service. In the **Steps** row, document the step-by-step process someone typically experiences, then add detail to each of the other rows.

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?

- Enter URL that user wishes to check
- Detection of malicious URLs using ML algorithm
- User can make online payment securely
- With the help of this system user can also purchase products online without any hesitation
- Provide URL to be checked
- Entering the website
- Enter the URL in search engine that to be detected
- Report the website if detected phishing.
- The entered URL is spilled and checked for previously reported URLs.
- Engage with Webpage
- At the end,the result is shown to the user
- The entered URL is detected using certain algorithms.
- Users have awareness of web phishing sites
- When the user gets the result of the site , the process gets completed as the site is not a phishing website.
- At the end, if the site is detected as the phishing website, the site is reported.
- Can use site again to check for web phishing sites

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?

- Person:Users can protect their information and make transactions with no worries
- Safe Browsing by using this detection technique.
- Only browser, a URL and internet facility are required
- Person Can be used by individual customers as well as a company
- They can see a search engine, precaution techniques, report option.
- Used by working employees , Businessmen, common people.
- URL of webpage
- Detects web phishing sites
- If this is a website, so it can be easily accessible.
- When the process completes, result is displayed.
- Relief that they are making a secure transaction
- Blacklist and Whitelist approaches are the traditional methods to identify the phishing sites
- User can share experience

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

- Primary goal is to detect web phishing URLs
- To avoid forfeiting of information
- To avoid losing of money
- To enter URL
- To reduce the loss of privacy data
- To know the website is legitimate or not
- Getting clarified 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?

- Accurate prediction of web phishing sites
- 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
- Users can make secure transactions
- Detects the malicious websites by simply using the URLs
- Satisfied 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?

- When the accuracy of prediction is inaccurate
- 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 diverted 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?

- Using this algorithm to train users to be able to detect Url's themselves by sending them emails to test themselves
- detecting all the sites using this product
- identifying the phishing sites
- Ability to report the detected malicious website
- Applying ML techniques in the proposed approach in order to analyze threat from URLs and produce effective results
- Next level of intelligence on top of signature-based prevention techniques and blacklists