## 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.

**TIP**

As you add steps to the experience, move each these "Five Es" the left or right depending on the scenario you are documenting.

SCENARIO

**Browsing, booking, Online transactions, visiting websites**

| | Entice<br>How does someone initially become aware of this process? | Enter<br>What do people experience as they begin the process? | Engage<br>In the core moments in the process, what happens? | Exit<br>What do people typically experience as the process finishes? | Extend<br>What happens after the experience is over? |
|---|---|---|---|---|---|
| **Steps**<br>What does the person (or group) typically experience? | need to build a system that would save the user and his data. Hence this proposed idea will restrict the hacker from hacking<br>The user will be made aware of Phishing and legitimate mails by which he can save himself<br>User can make online payment securely<br>With the help of this system user can also purchase products online without any hesitation | Entering the website<br>Enter the URL in search engine that to be detected<br>Report the website if it detected phishing. | The entered URL is splited and checked for previously reported URLs.<br>The entered URL is detected using certain algorithms.<br>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 not a phishing website. | At the end, if the site is detected as the phishing website, the site is reported. |
| **Interactions**<br>What interactions do they have at each step along the way?<br>■ **People:** Who do they see or talk to?<br>■ **Places:** Where are they?<br>■ **Things:** What digital touchpoints or physical objects would they use? | Safe Browsing by using this detection technique.<br>Only browser, a URL and internet facility are required | They can see a search engine, precausion techniques, report option.<br>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 sites |
| **Goals & motivations**<br>At each step, what is a person's primary goal or motivation? ("Help me..." or "Help me avoid...") | To avoid thefting of information<br>To avoid losing of money | 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**<br>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. | 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**<br>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**<br>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 signature-based prevention techniques and blacklists |