

## 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

As you add steps to the experience, move each these typically experiences, then add detail to each of the other rows. "Five Es" the left or right depending on the scenario you are documenting. **Entice Exit** Engage **Extend** What do people What happens after the How does someone What do people In the core moments **SCENARIO** experience is over? initially become aware typically experience in the process, what experience as they as the process finishes? of this process? begin the process? happens? Browsing, booking, attending, and rating a local city tour At the end, if the site is detected as the phishing website, the site is reported or blocked. When the user gets the result of the site Steps It protects our data from unauthorized users,
Hence this proposed idea will give the
Confidentiality on Data Type / Enter the URL in Search bar Entering into the Website the knowledge The entered URL is splitted and checked the process gets The entered URL is What does the person (or group) completed as the site is not a phishing website. detected using certain algorithms for previously reported URLs. typically experience? This system gives relief to the user in purchasing Report the website if it is a phishing website products, business tools from cyber attacks. At the end, the result is shown to the user Used on Business Administrators, Employees as well as peoples. Interactions This is a web application , so it is reliable What interactions do they have at each step along the way? Updated Browsers and Ad Blockers are required People: Who do they see or talk to? Places: Where are they? Things: What digital touchpoints or physical objects would they use? Enhance the security of the websites at the time of Developing Analyzing the Predicted websites. To prevent data

leakage from

unauthorized

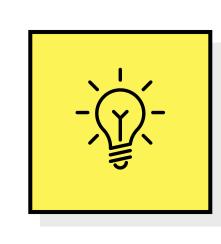
persons

To improve the level

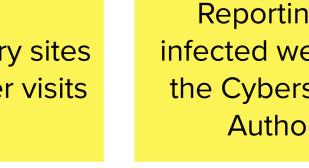
of security so that it

can reduce cyber

attacks **Goals & motivations** To minimize the data To know whether the loss and improve privacy or not. At each step, what is a person's primary goal or motivation? ("Help me..." or "Help me avoid...") Detect and prevent
against unknown
phishing attacks, as new
patterns are developed by
attackers **Positive moments** If the website is detected as phished one, then the user couldn't able to enter his/her details. What steps does a typical person find enjoyable, productive, fun, motivating, delightful, or exciting? When the detected site is phishing website but the user already provided information Searching of Hidden and Revoked Websites Attackers can develop more until the website is blacklisted or blocked If there is no network connectivity it may fail Being a manual process users couldn't **Negative moments** able verify all website that he/she visits What steps does a typical person find frustrating, confusing, angering, costly, or time-consuming? Areas of opportunity



What have others suggested?



order to analyze the real time URLs and produce effective results