






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, attending, and rating a local city tour		<div></div> <div>Entice</div> <div>How does someone initially become aware of this process?</div>	<div></div> <div>Enter</div> <div>What do people experience as they begin the process?</div>	<div></div> <div>Engage</div> <div>In the core moments in the process, what happens?</div>	<div></div> <div>Exit</div> <div>What do people typically experience as the process finishes?</div>	<div></div> <div>Extend</div> <div>What happens after the experience is over?</div>
<div>Steps</div> <div>What does the person (or group) typically experience?</div>	<div><div>need to build a system that would save the user and his data, therefore the user must be protected from hacking</div><div>The user will be made aware of Phishing and phishing can be avoided</div><div>User can make online payment securely</div><div>With the help of this product, users can purchase products online without any hesitation</div></div>	<div><div>Entering the website</div><div>Enter the URL in search engine that to be detected</div><div>Report the website if it detected phishing.</div></div>	<div><div>The entered URL is reported by reported URLs.</div><div>The entered URL is detected using certain algorithms.</div><div>At the end, the result is shown to the user.</div></div>	<div><div>When the user gets the result of the site, the process gets completed as the site is not a phishing website.</div><div>At the end, if the site is detected as the phishing website, the site is reported.</div></div>		
<div>Interactions</div> <div>What interactions do they have at each step along the way?</div> <div>People: Who do they see or talk to?</div> <div>Places: Where are they?</div> <div>Things: What digital touchpoints or physical objects would they use?</div>	<div><div>Safe Browsing by using this detection technique.</div><div>Only browser, a URL and internet facility are required</div></div>	<div><div>They can use a search engine to report</div><div>Used by visiting common people.</div></div>	<div><div>this is a website, so it can be easily accessible.</div></div>	<div><div>When the process completes, result is displayed.</div><div>Blacklist and Whitelist approaches are the traditional methods to identify the phishing sites</div></div>		
<div>Goals &amp; motivations</div> <div>At each step, what is a person's primary goal or motivation? (“Help me...” or “Help me avoid...”)</div>	<div><div>To avoid thefting of information</div><div>To avoid losing of money</div></div>	<div><div>To reduce the loss of privacy data</div></div>	<div><div>To know the website is legitimate or not</div></div>	<div><div>Getting clarified about the doubtful websites.</div><div>Enhance the security of the websites at the time of Developing</div></div>		
<div>Positive moments</div> <div>What steps does a typical person find enjoyable, productive, fun, motivating, delightful, or exciting?</div>	<div><div>when the detected site is a phishing website, and user doesn't give any information</div></div>	<div><div>You already know it is a phishing site and You guessed it</div></div>	<div><div>Detects the malicious websites by simply using the URLs.</div></div>	<div><div>Satisfied on knowing that the site is phishing website or not.</div><div>Detect and prevent against unknown phishing attacks, as new patterns are created by attackers.</div></div>		
<div>Negative moments</div> <div>What steps does a typical person find frustrating, confusing, angering, costly, or time-consuming?</div>	<div><div>If Internet connection fails, this system won't work.</div></div>	<div><div>being a manual process and the users cannot verify for all the websites that he visits</div></div>	<div><div>Searching of deleted websites.</div></div>	<div><div>when the detected site is phishing website but the user already provided information</div><div>a new phishing website may prove to be detrimental because it has not been added to the blacklist yet</div></div>		
<div>Areas of opportunity</div> <div>How might we make each step better? What ideas do we have? What have others suggested?</div>	<div><div>detecting all the sites using this product</div></div>	<div><div>Identifying the phishing sites</div></div>	<div><div>facility to report the detected malicious website</div></div>	<div><div>Applying ML techniques in the proposed approach in order to analyse the real time URLs and produce effective results</div><div>Next level of intelligence on top of signature-based prevention techniques and blacklists</div></div>		

