



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.

<div>SCENARIO</div> <div>Browsing, booking, attending, and rating a local city tour</div>					
	<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></div> <div>Steps</div> <div>What does the person (or group) typically experience?</div>	<div>need to build a system that must meet the user entity also, meet this proposed flow and ensure the leader from leading</div> <div>The user will be made aware of phishing and legitimate mails by which he can have result</div> <div>User can make online payment securely</div> <div>With the help of this system user can also purchase products online without any hesitation</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>The entered URL is verified and checked for previously 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>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> <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>	<div>Safe Browsing by using this detection technique.</div> <div>Only browser, a URL and internet facility are required</div>	<div>They can see a search engine, precaution techniques, report option.</div> <div>Used by working employees, Businessmen, common people.</div>	<div>this is a website, so it can be easily accessible.</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> <div>Goals & motivations</div> <div>At each step, what is a person's primary goal or motivation? ("Help me..." or "Help me avoid...")</div>	<div>To avoid theft of information</div> <div>To avoid losing of money</div>	<div>To reduce the loss of privacy data</div>	<div>To know the website is legitimate or not</div>	<div>Getting clarified about the doubtful websites.</div>	<div>Enhance the security of the website at the time of Developing</div>
<div></div> <div>Positive moments</div> <div>What steps does a typical person find enjoyable, productive, fun, motivating, delightful, or exciting?</div>	<div>when the detected site is a phishing website and user doesn't give any information</div>	<div>You already know it is a phishing site and You guessed it</div>	<div>Detects the malicious websites by simply using the URLs.</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> <div>Negative moments</div> <div>What steps does a typical person find frustrating, confusing, angering, costly, or time-consuming?</div>	<div>If internet connection fails, this system won't work.</div>	<div>being a manual process and the users cannot verify for all the websites that he visits</div>	<div>Searching of detected websites.</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> <div>Areas of opportunity</div> <div>How might we make each step better? What ideas do we have? What have others suggested?</div>	<div>detecting all the sites using this product</div>	<div>Identifying the phishing sites</div>	<div>facility to report the detected malicious website</div>	<div>Applying ML techniques or the proposed approach in order to analyze the new URLs and produce effective results</div>	<div>Next level of intelligence on top of signature-based prevention techniques and blacklists</div>