

Project Design Phase-II
Customer Journey Map

Date	03 October 2022
Team ID	PNT2022TMID23911
Project Name	Project – Web Phishing Detection
Maximum Marks	4 Marks

Template

Customer experience journey map

Use this framework to better understand customer needs, motivations, and obstacles by illustrating a key scenario or process from start to finish. When possible, use this map to document and summarize interviews and observations with real people rather than relying on your hunches or assumptions.

Created in partnership with

Product School

[Share template feedback](#)

Need some inspiration?

See a finished version of this template to kickstart your work.

[Open example](#) →

1

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 "True or False" to the left or right depending on the scenario you are documenting.

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?	<div>Users look at content that would lead to our service and then they proceed to book the tour.</div> <div>The user will be made aware of Phishing and ignore with it.</div> <div>User can make online payment securely.</div> <div>With the help of the user our site partner products come within any business.</div>	<div>Entering the website</div> <div>Enter the URL in search engine that it be detected.</div> <div>Report the website if it detects phishing.</div>	<div>The entered URL is updated 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 goes to the next step and a primary website.</div>	<div>When end, if the site is detected in the phishing website, the site is reported.</div>
Interactions What interactions do they have at each step along the way? <ul style="list-style-type: none">People: Who do they see or talk to?Places: Where are they?Things: What digital touchpoints or physical objects would they use?	<div>Just phishing Detection tool.</div> <div>The internet with sufficient data set is required.</div> <div>Updated Browser and Ad Blockers are required.</div>	<div>They can alter the settings for reports, exception techniques.</div> <div>User as Business Administrators, Employees as well as people.</div>	<div>This is a web application, so it is reliable.</div>	<div>When the process completed, result is displayed.</div>	<div>Report and Website appears on the website and report to identify the phishing site.</div>
Goals & motivations At each step, what is a person's primary goal or motivation? ("Help me..." or "Help me avoid...")	<div>To avoid sharing 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 alerted about the detected websites.</div>	<div>Enhance the security of the website at the time of Documenting.</div>
Positive moments What steps does a typical person find enjoyable, productive, fun, motivating, delightful, or exciting?	<div>The website is detected and reported to the user.</div>	<div>We can acquire knowledge about phishing website.</div>	<div>Detects the malicious websites by simply using the URLs.</div>	<div>Follows on tracking that the user phishing website or not.</div>	<div>Send an email report about phishing website to the user.</div>
Negative moments What steps does a typical person find frustrating, confusing, angering, costly, or time-consuming?	<div>Phishing connection with the system isn't work.</div>	<div>Using a manual process and it's very slow only for the website that is not work.</div>	<div>Searching of detected websites.</div>	<div>When the detected site is phishing website but the user doesn't provide information.</div>	<div>A real phishing website and report to the user and report to the website.</div>
Areas of opportunity How might we make each step better? What ideas do we have? What have others suggested?	<div>Detecting every site where the user visit.</div> <div>Reporting the detected website to the Cybersecurity Authority.</div>	<div>Identifying Phishing Sites.</div>	<div>Facility to report the detected malicious website.</div>	<div>Improving the website to make it more secure and the user can report the phishing website.</div>	<div>Report of phishing website to the user and report to the website.</div>