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

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?

- It protects our data from unauthorized users, Hence this proposed idea will give the Confidentiality on Data
- The user can gain the knowledge about phishing vs legitimate website
- User can make payments securely
- This system gives relief to the user in purchasing products, business tools from cyber attacks.
- Entering into the Website
- Type / Enter the URL in Search bar
- Report the website if it is a phishing website
- The entered URL is splitted and checked for previously reported URLs.
- The entered URL is detected using certain algorithms
- 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 or blocked.

Interactions

What interactions do they have at each step along the way?

- **People:** Who do they see or talk to?
- **Places:** Where are they?
- **Things:** What digital touchpoints or physical objects would they use?

- Anti phishing Extensions detection used
- The internet with sufficient data rate is required
- Updated Browsers and Ad Blockers are required
- They can alter the settings for reports, encryption techniques
- Used on Business Administrators, Employees as well as peoples.
- This is a web application , so it is reliable
- When the process completed, result is displayed
- Blacklist and Whitelist approaches are the traditional methods to identify the phishing sites

Goals & motivations

At each step, what is a person's primary goal or motivation? ("Help me..." or "Help me avoid...")

- To prevent data leakage from unauthorized persons
- To improve the level of security so that it can reduce cyber attacks
- To minimize the data loss and improve privacy
- To know whether the website is legitimate or not.
- Analyzing the Predicted websites.
- Enhance the security of the websites at the time of Developing

Positive moments

What steps does a typical person find enjoyable, productive, fun, motivating, delightful, or exciting?

- If the website is detected as phished one, then the user couldn't able to enter his/her details.
- We can acquire knowledge about phished website
- Detects the malicious websites by simply using the URLs.
- Fulfillment on knowing that the site is phishing website or not.
- Detect and prevent against unknown phishing attacks, as new patterns are developed by attackers

Negative moments

What steps does a typical person find frustrating, confusing, angering, costly, or time-consuming?

- If there is no network connectivity it may fail
- Being a manual process users couldn't able verify all website that he/she visits
- Searching of Hidden and Revoked Websites
- When the detected site is phishing website but the user already provided information
- Attackers can develop more until the website is blacklisted or blocked

Areas of opportunity

How might we make each step better? What ideas do we have? What have others suggested?

- Detecting every sites where the user visits
- Reporting the infected website to the Cybersecurity Authority
- Identifying Phishing Sites
- Facility to report the detected malicious website
- Implementing ML/DL 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