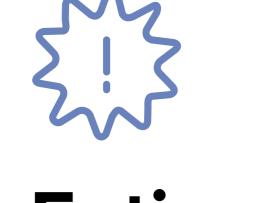
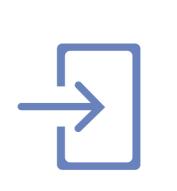
**SCENARIO Steps** 

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?

What does the person (or group) typically experience?

Awareness of phishing websites through past incidents

Alert mechanism from developed app or extension

Download Extension for background process

Report the website if phishing is detected.

Feature extraction from main web page The URL is split and checked for malicious activity

End result is displayed to user

The user gets the detection results

User gets a sense of safety

The site is reported if found malicious



#### 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?

Interaction between application and browser

The User sees a detailed report of the analysis

Interaction between application and browser

The User sees a detailed report of the analysis

**Establish connection** with user's browser

web scraping extract URL

When the process completes, result is displayed.

**Blacklist and Whitelist** approaches are the traditional methods to identify the phishing



### **Goals & motivations**

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

Safe and secure browsing experience Increasing Digital payments

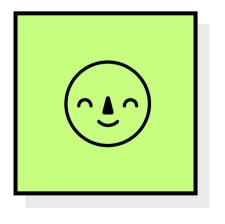
Safe and secure browsing experience Increasing Digital payments

Develop reliable ML algorithms for classification

Effecient Hyperparameter tuning

Getting clarifed about the doubtful websites

Enhance the security of the websites at the time of Developing



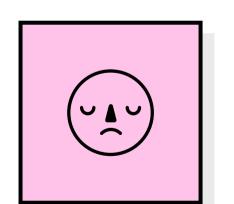
## **Positive moments**

What steps does a typical person find enjoyable, productive, fun, motivating, delightful, or exciting? Avoiding attack from phishing website

Safe and secure transactions

Applying ML algorithm to classify Satisfied on knowing whether the status of the website

Detect and prevention unknown phishing attacks, as new patterns are created by attackers.



## **Negative moments**

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

Algorithm detecting False Negative result

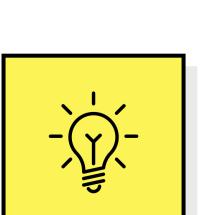
User entering critical and sensitive information

Searching of deleted websites

activity after user entered the information

detection of phishing

a new phishing website may prove to be detrimental because it has not been added to the blacklist yet



## Areas of opportunity

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

Develop an automated system Improve reliability of the algorithm

Improve reliability of the algorithm

Facility to report phishing websites

Applying ML 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