**SCENARIO** Browsing, booking, local city tour Steps typically experience? Interactions each step along the way? **Goals & motivations** 

# attending, and rating a What does the person (or group)

## **Entice**

Home Page

The user can see the

details about the

application in home

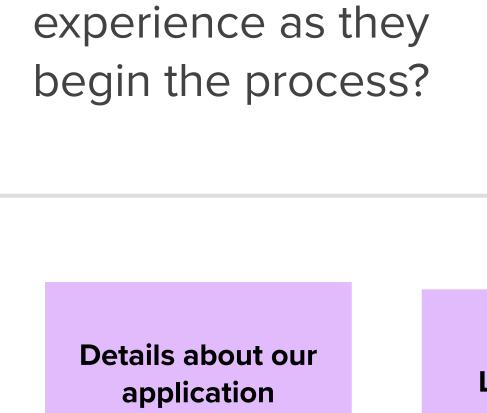
page

This website will be accessed through any devices with responsiveness.

How does someone initially become aware of this process?

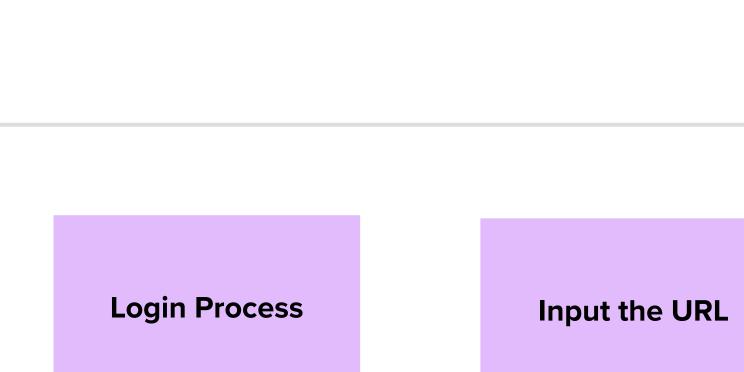
#### **Enter**

What do people



The user can explore the features and services of

our application in home

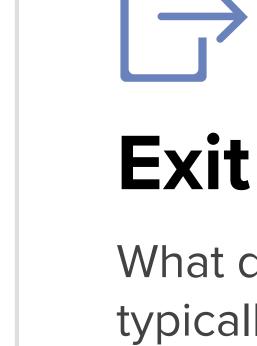


If the user is new to

our service, they can

register by entering the credentials

**URL Checking** The entered URL will be checked by passing into the The data will be The model will be deployed to the front end. model



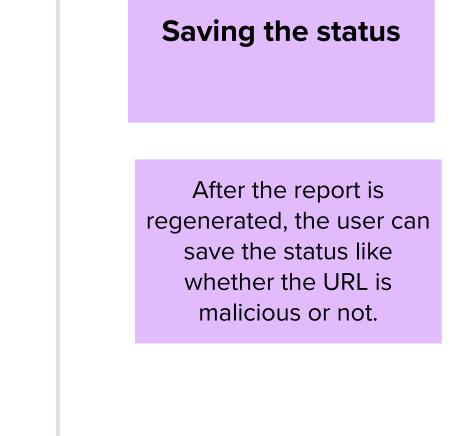
What do people typically experience as the process finishes?

logout

After the user finishes their process, they can logout from the application

The result will be displayed in the user interface if the process

gets complete.



Blacklist and whitelist approaches are the

traditional techniques to identify the phishing

**Extend** 

What happens after the

experience is over?

#### What interactions do they have at

People: Who do they see or talk to?

- Places: Where are they?
- Things: What digital touchpoints or



#### At each step, what is a person's

primary goal or motivation? ("Help me..." or "Help me avoid...")

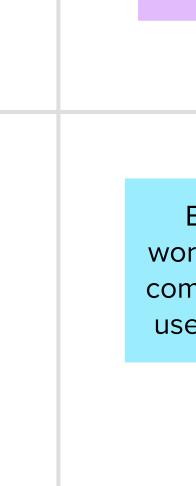
#### **Positive moments** What steps does a typical person

find enjoyable, productive, fun, motivating, delightful, or exciting?

### **Negative moments**

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

If the internet is disconnected, this application won't work



If the user is new to

our service, they

should have to

register.

The user can see the

o avoid the losing of

private data.

precaution technique and report option

The user should

login by entering the credentials in order to detect the URL.

After login, they can input the URL to detect whether the URL is

malicious or not

The user is already knows the phishing website and they guessed it.

It is the manual process. So, the user cannot verify for all the websites.

To know that the

This website is responsive in any kind of devices

Engage

happens?

In the core moments

in the process, what

This website is easily accessible

or not.

The user can detect the malicious website by just feeding the input URL to the application

Getting clarified about the phishing websites

Detect and prevent
against unknown
phishing attacks, as new
patterns are created by
hackers

Enhance the security

of the websites at

the time of developing

A new phishing website may prove to be detrimental because it

The user is already provided information even before if the website is detected as phishing site.

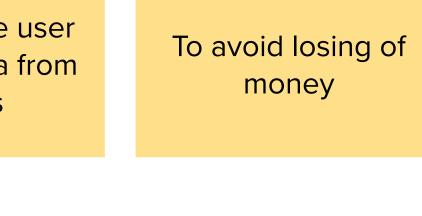
has not been added to the blacklist yet

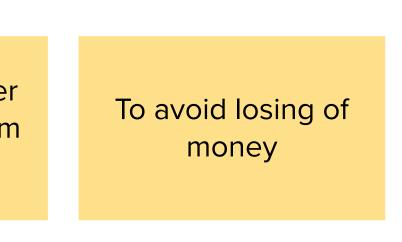


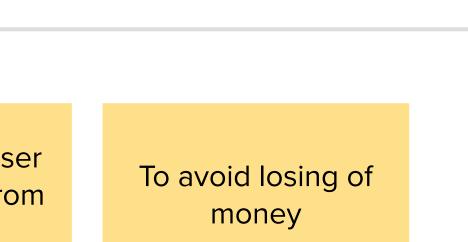
To secure the user sensitive data from hackers

When the site is

detected as phishing, the user should not give the data further.







Only the browser, URL is required to process the service.