SCENARIO

Browsing, booking, attending, and rating a local city tour

Entice

How does someone

initially become aware of this process?

In this process the user can

detect the phishing

websites in which they

have entered their

confdential data or

sensitive data

The user can make online transactions in a secured way and can be sure of thier legitimate websites.

through phishing

websites.

The goal of the project is to secure confdential information.

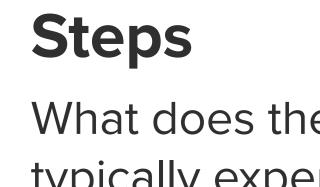
The user becomes alert if fnds it to be phishing

website and does not

provide any confdential data.

It becomes to detect if

the internet connectivity is slow or the browser version is older.



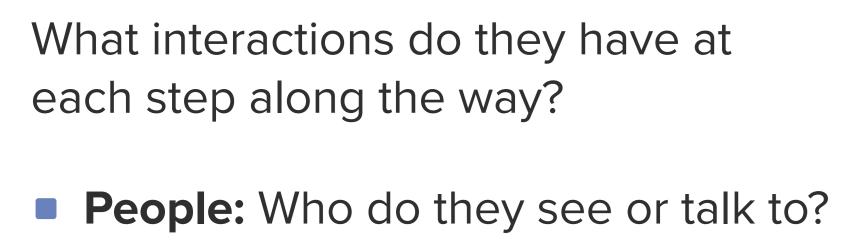
What does the person (or group) typically experience?

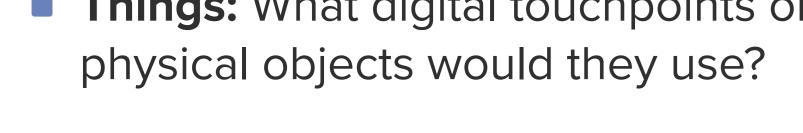


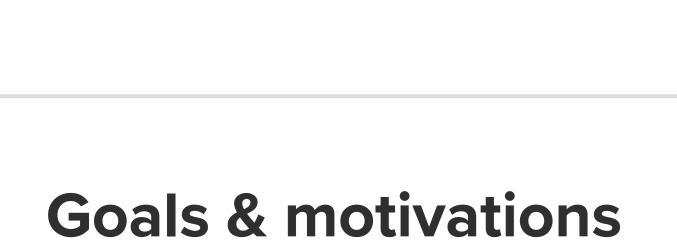
Interactions What interactions do they have at

each step along the way?

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

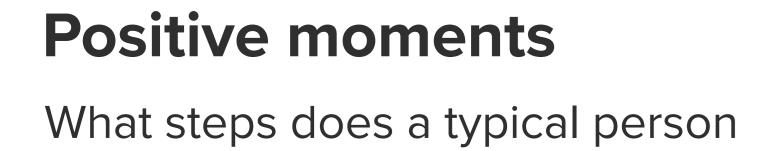




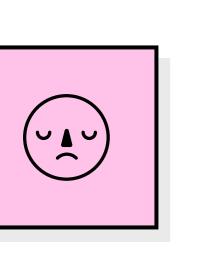


At each step, what is a person's primary goal or motivation?

("Help me..." or "Help me avoid...")



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



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



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

We need to develop a model to detect the phishing websites in order to achive data security and prevents from hackers Using this model the

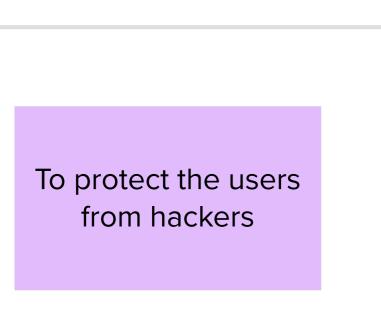
user can store in required fles/ drives

project. The user can browse and visit websites.

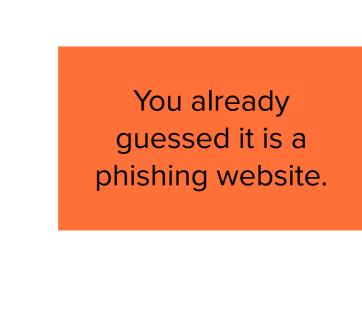
Internet facility, browser and URL of the visited website are required.

To ensure secured

transactions.



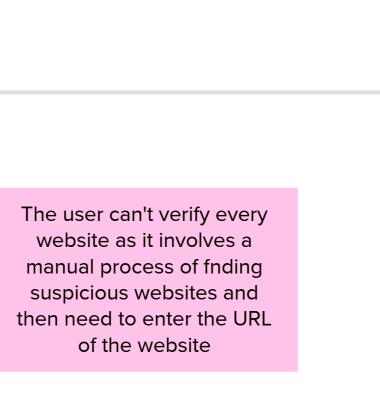


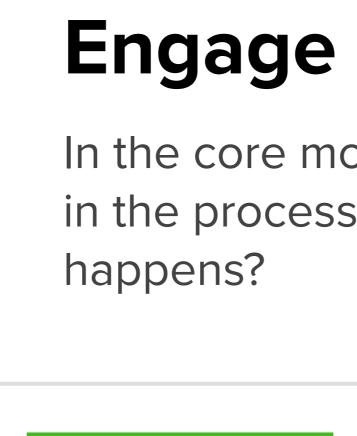


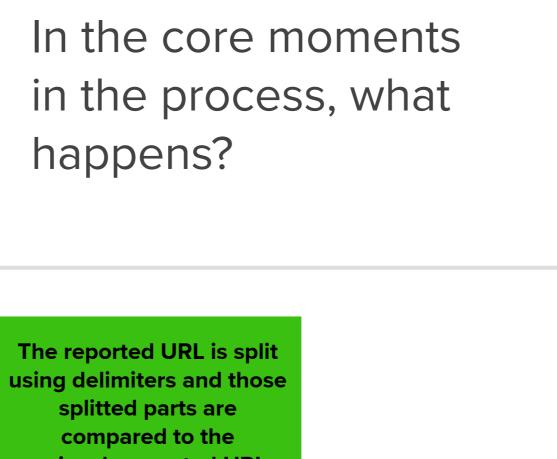
To minimize the

loss of confdential

data.







previously reported URLs At the end the user will be awrae

The developed model reliable

whether the website is to be

To detect if the site is legitimate or not.

The URL's submitted by the users helps the model to detect phishing websites and checks whether the URL is already in the list of already detected websites.

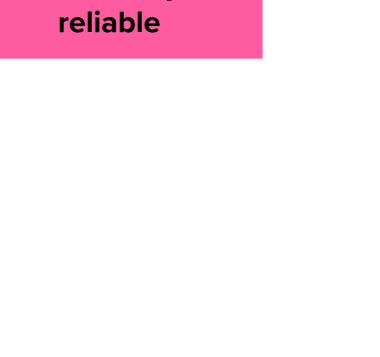
Searching the deleted websites.

Facility to repor the phishing

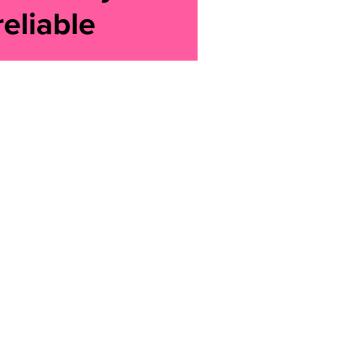
website.

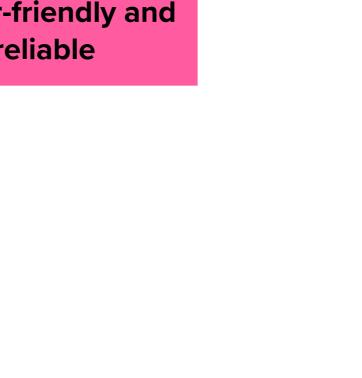


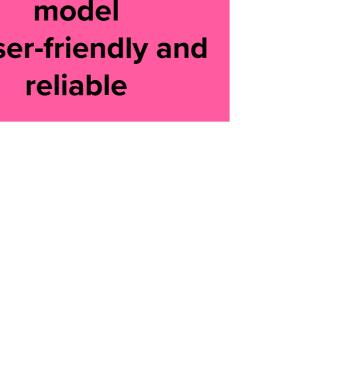








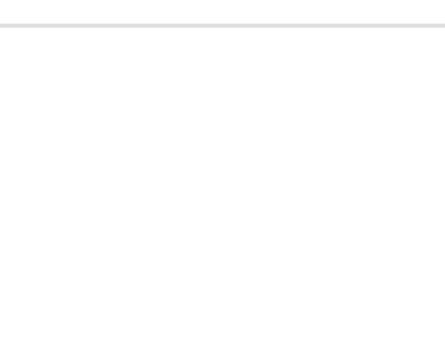


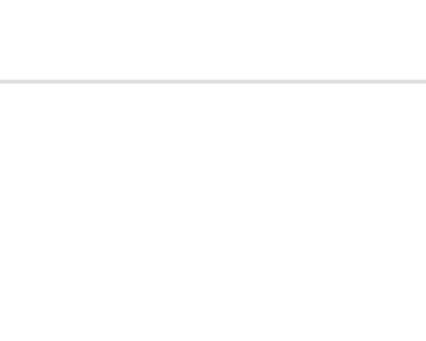




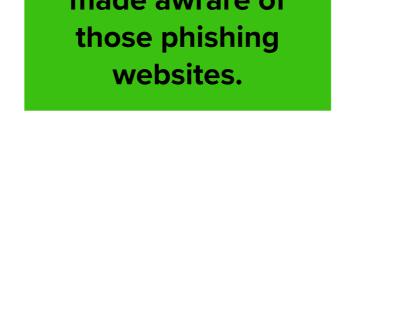


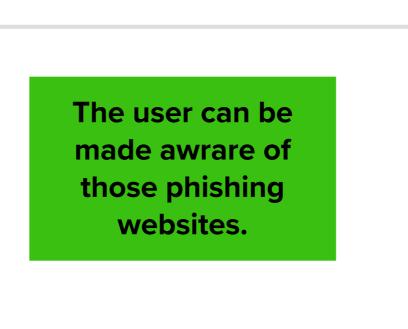


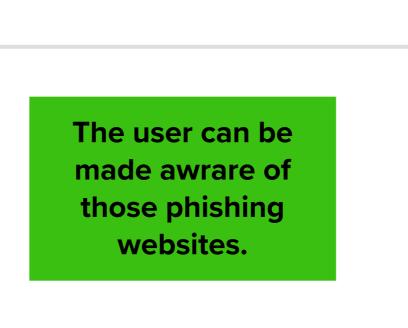


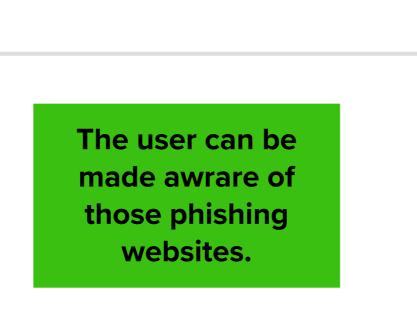












Exit

What do people typically experience as the process finishes?

The user can be

made aware of

phishing websites.

The result will be

displayed at the end

the process

Gets clarifed

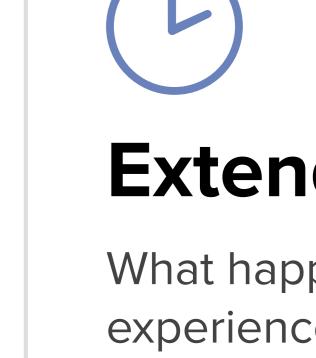
about the

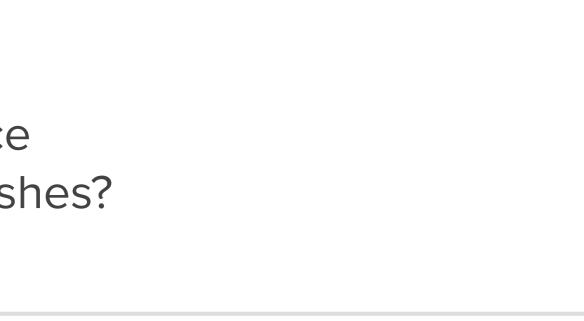
suspicious data.

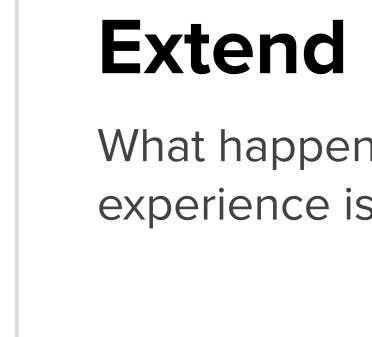
The model is productive by satisfying the user whether the site is legitimate or not.

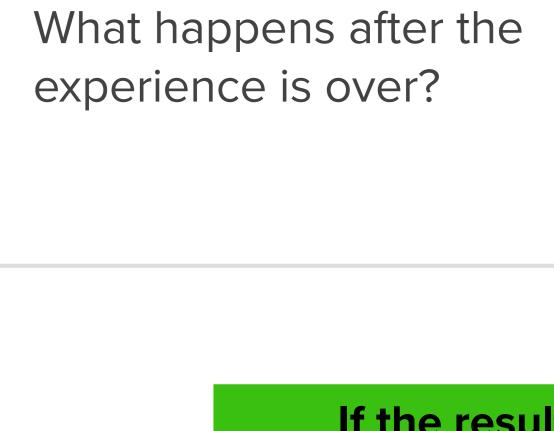
When the detected website is phishing website but appears to be legitimate to the outer world.

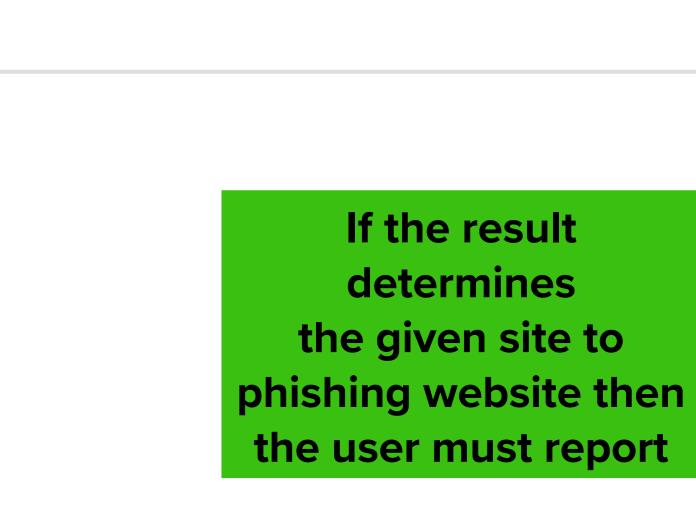
Using advanced ML algorithms to analyze the URL's and produce the desired outputs.

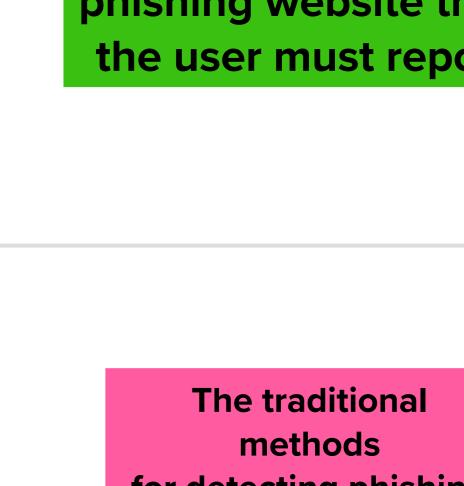


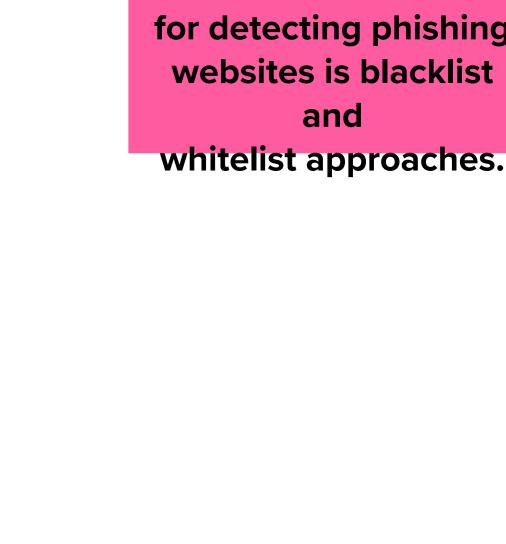




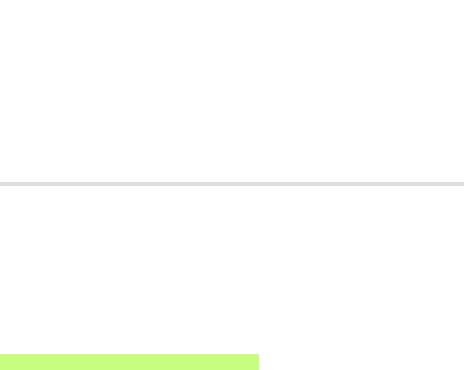


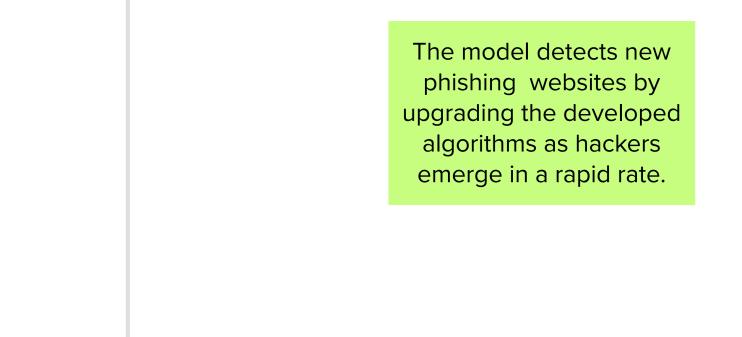


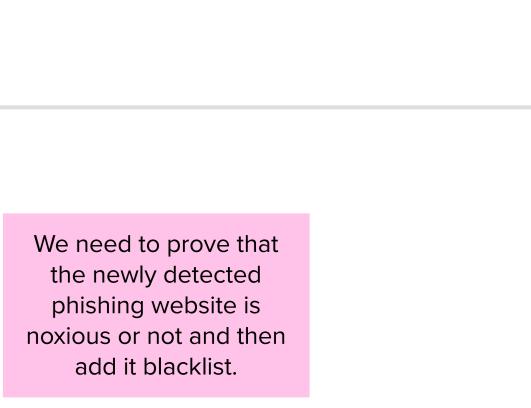










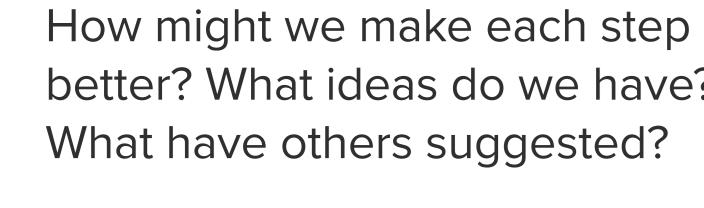


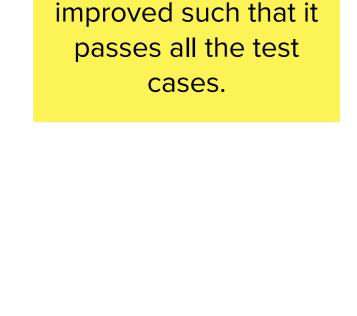
The future work is to

detect phishing webiste in an automated way instead of manual process











In efcient manner

the phishing websites is

identifed.

Enter

What do people

experience as they

begin the process?

The user can report

if something is

suspicious

The user is provided with search engines, detecting algorithms and reporting options

