**Team Members:**

| NAME: | REG NO: |
|---|---|
| Siva AN | 19BCE1582 |
| P Jayavignesh | 19BCE1589 |
| A AVINASH | 19BCE1618 |

## ISM – Review 1

## Live phishing websites detection using machine learning

Phishing websites:

A phishing website is a common social engineering method that mimics trustful uniform resource locators (URLs) and webpages.

A phishing website is a domain similar in name and appearance to an official website. They're made in order to fool someone into believing it is legitimate.

## Objective:

The objective of this project is to collect data & extract the selected features from the URLs and with the help of machine learning predict if the website is a phishing website or not.

## Features of the website taken into consideration:

- Length of URL
- DNS Record
- Website Traffic
- Age of Domain
- HTML and JavaScript based Features

## Dataset:

- The dataset taken is generated from PhishTank dataset which consists of legitimate and phishy url's.

- The features of those URL's are extracted using the definition functions mentioned above.

- Many features are taken , including the class label. The dataset is then preprocessed and used to train the machine learning model.

## Implementation of User Interface

- We can make it as a background application, which provides a warning or pop-up notification whenever the user visits any phishy websites.
- We can also try to come with an chrome extension, which does the same work.

## Machine learning Model

- As our aim is to classify the URL into one of the 2 categories , 3 classification algorithms are used.

- The same training set is used to train all the 3 models.

- Each model is then fitted over the data, when predicted they give us a result of all the classes of the training set.

- Once all 3 algorithm's give us the output , They are then passed into a majority voting mechanism , which provides us with the final predicted class labels.