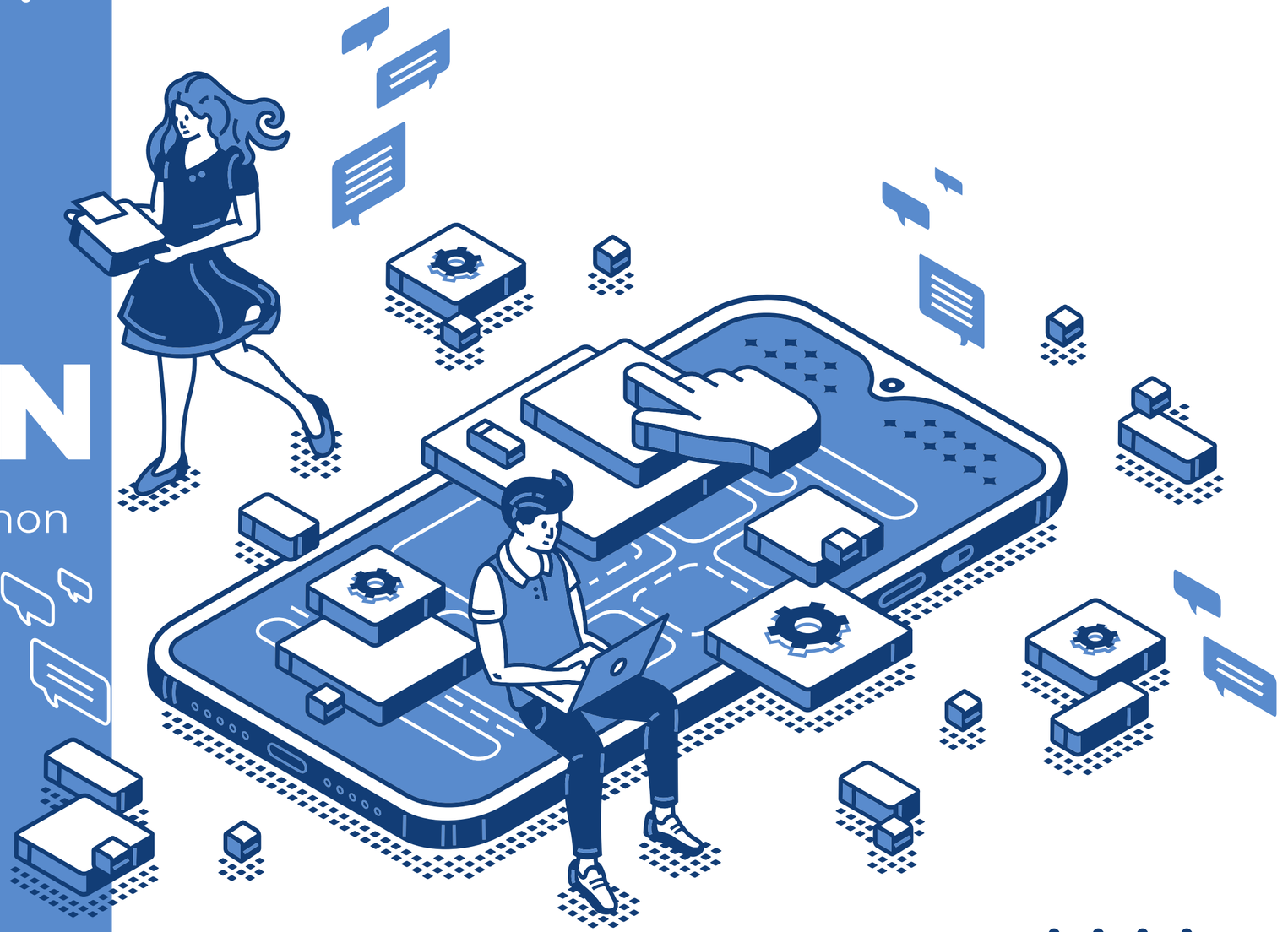
# PHISHING DETECTION

Machine Learning - Online Hackathon



# Problem Statement

As each coin has two sides, so does technology. On one hand, with the advancement in technology the lives are getting better, on the other hand, the ill use of technology is also increasing. The suspicious activities are increasing ranging from dos attacks, phishing, hacking etc. In this hackathon, we are concerned with the increasing phishing attacks.

# Proposed Solution

Our main aim is to detect the phishing attack at the different sites or organisation of various domain.

We have made a predictive model based on the given datasets which basically predicts that website is legitimate, suspicious, or phising.

# Approach

As the problem statement is very specific about the theme. So, firstly we describe the dataset with different parameters. We used StandardScaler for the data standarization. Then we used the method test,train,split to separate the datasets. Further we used Support Vector Machine(SVM) model for training the predictive model. We got 93.02% accuracy score on the training dataset and 92.57% accuracy on the test dataset. Eventually we saved the model of the predictive system.

# Advantages

- With the proposed model, we save a lot of money & phishing attacks on the organization.
- Our model gives high level of accuracy score on different inputs.
- We can deploy the proposed model on various platform.

# THANK YOU

We highly appreciate your valuable time.

**TEAM TORS**

Vikash Kumar