Problem Statement

Phishing attacks are becoming more and more sophisticated, and our algorithms are suffering to keep up with this level of sophistication. They have low detection rate and high false alarm especially when novel phishing approaches are use. The blacklist-based method is unable to keep up with the current phishing attacks as registering new domains has become easier. Moreover, comprehensive blacklist can ensure a perfect up-to-date database. Various other techniques such as page content inspection algorithms have been used to combat the false negatives but as each algorithm uses a different approach, their accuracy varies. Therefore, a combination of the two can increase the accuracy while implementing different error detection methods.

Problem statements:

1.How to process dataset for phishing detection?

2.How to increase accuracy of [phishing websites](https://www.sciencedirect.com/topics/computer-science/phishing-website) algorithms?

3.How to reduce false negative rate in phishing websites algorithm?

4.What are the best combinations of [classifiers](https://www.sciencedirect.com/topics/computer-science/classification-machine-learning) that can efficiently detect phishing attacks?