Project Design Phase-I
Proposed Solution Template

Date	30 October 2022
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution Template:

Project team shall fill the following information in proposed solution template.

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	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. Today, phishing schemes have gotten more varied, and are potentially more dangerous than before.
2.	Idea / Solution description	We conducted a literature review to identify the features of infected websites by phishing. As a result, a combination of the Naive Bayes and Decision tree algorithms has been constructed using the typical cycle of Machine Learning (ML) modelling. The main tools used have been Jupiter framework and Python. The proof of concept has been performed in a controlled environment. The infected websites has been obtained using Phish Tank. Finally, to yield the higher level of accuracy of phishing detection, the validation of results was accomplished using the most accepted algorithms in the scientific field such as ML Random Forest, Logistic Regression and Fictitious Classifier, according to our literature review.
3.	Novelty / Uniqueness	We have evaluated the performance of our proposed phishing detection approach on various classification algorithms using the phishing and non-phishing websites dataset.

4.	Social Impact / Customer Satisfaction	The first and foremost benefit of phishing simulation is the decreased security risks to your organization due to social engineering attacks involving human manipulation and deception. Second, many regulations and standards now require organizations to conduct regular training sessions for employees and monitor the effectiveness of such training sessions. Third, as employees become aware of possible use cases, they will act as a primary shield against such emails as they already know that those emails are not genuine and must be avoided. Simulated phishing attacks with appropriate reporting procedures are an excellent example of a strong security culture within an organization. Accordingly, the chances of fraudulent activity also decrease.
5.	Business Model (Revenue Model)	Phishing attacks can increase the business. Staff will not lose their jobs. Data and assets will be safe.
6.	Scalability of the Solution	This paper presents a proposal for scalable detection and isolation of phishing. The main ideas are to move the protection from end users towards the network provider and to employ the novel bad neighbourhood concept, in order to detect and isolate both phishing e-mail senders and phishing web servers. In addition, we propose to develop a self-management architecture that enables ISPs to protect their users against phishing attacks, and explain how this architecture could be evaluated.