Project Design Phase-I
Proposed Solution Template

Date	19 September 2022
Team ID	PNT2022TMID40752
Project Name	Project – 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 user of the internet had to make an online purchase. He then used the internet to access the webpage. The process of displaying the goods takes time. He started to look at every item. He looks for the required products on an online page. Finally, he located the required products. He then entered all of his credit card information. password and username for making purchases via the internet. Then he got the notification "Your order" is entered successfully, and the transaction is finished. You will receive the merchandise they requested in two days. the following. He received a notification from the bank and his mobile device within 24 hours. The customer was astonished to find their account empty. Then only he realized that was a fake website and his bank account details was stolen by hacker .To avoid this scenario. We need to solve this problem by using the Web Phishing Detection
2.	Idea / Solution description	Every time we click on a website, an alert box stating whether it is secure or not must appear in order to combat the issue of phishing websites.The website can also be scanned to shield our computer or mobile device against phishing attacks. Although technology exists, it is still important for us as users to be aware of whether a website is secure or not. We should avoid visiting any unwelcome websites.
3.	Uniqueness	In the suggested method, the hyperlink-specific attributes were separated into 12 different categories and then used to train the machine learning algorithms. Using a dataset of phishing and non-phishing websites, we assessed how well our suggested phishing detection technique performed against several categorization algorithms.

4.	Customer Satisfaction	While utilising certain websites, an alert box will appear when we click on them, making the user aware of the website and increasing their pleasure with it. Additionally, we can scan the website to stop information from being hacked, which would increase consumer satisfaction even further.
5.	Scalability of the Solution	Thus, software-based phishing detection techniques are preferred for fighting against the phishing attack. Mostly available methods for detecting phishing attacks are blacklists/whitelists, natural language processing, visual similarity, rules, machine learning techniques