Project Design Phase-I
Proposed Solution

Date	8 October 2022
Team ID	PNT2022TMID27267
Project Name	Project - Web Phishing Detection
Maximum Marks	2 Marks

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Web Phishing Detection
2.	Idea / Solution description	Phishing attempts nefarious aims such as getting sensitive information by sending bulk emails pretending to be from an outstanding organization and reputable institution. Phishers use social engineering and spear-phishing techniques to deploy malware into a given network that steals all-important operation data of the organization . Generally, this phenomenon has shown four principal forms of acting: (i)**Email-to-email:** when a hacker sends an email asking for personal data from the victim in question (ii)**Email-to-website:** when a hacker sends an email embedded with a phishing web address to the victim (iii)**Website-to-website:** when an unfortunate victim taps on the phishing website through another website or an online advert (iv)**Browser-to-website:** when somebody incorrectly spells an authentic web address and after that gets alluded to a phishing site that has a semantic similarity to the real web address.
3.	Novelty / Uniqueness	Can detect hidden phishing technologies present in website
4.	Social Impact / Customer Satisfaction	Prevent scams and other malicious intents of using other's personal data
5.	Business Model (Revenue Model)	This model can be implemented alongside other apps and services as add-on for revenue. It can also be used as a plugin for users that surf the internet unprotected
6.	Scalability of the Solution	Can be implemented in all internet browsers as means of countering web phishing on a large scale.