Project Design Phase-I
Proposed Solution Template

Date	5 October2022
Team ID	PNT2022TMID10582
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)	Web phishing tends to steal a lots of information from the user during the online activities like online transaction like user important documents that has been attached to that websites . There are Multiple Types of Attacks happens here every day, but there is no auto detection Process through Machine Learning is achieved.
2.	Idea / Solution description	To use anti-phishing protection and anti-spam software to protect yourself. for example to detect and predict e-banking phishing websites, we proposed an intelligent, flexible and effective system that is based on using classification algorithms. The e-banking phishing website can be detected based on some important characteristics like URL and domain identity and security and encryption criteria in the final phishing detection rate.With the various user awareness of regular update of passwords to online account which makes the intruders hard to predict the password and never ever share your personal details and financial details over the internet because internet is the major and simple way for getting the user information so be aware of this.
3.	Novelty / Uniqueness	Machine learning technology consists of many algorithms which requires past data to make a decision or prediction of future data. Using this technique, algorithm will analyze various blacklisted and legitimate URL's and their features to accurately detect the phishing websites including zero-hour phishing websites.

4.	Social Impact / Customer Satisfaction	Phishing website has a list of effects on a business, including loss of money, loss of intellectual property, damage of reputation, and disruption of operational activities. Example: Facebook and Google between 2013 and 2015 Facebook and google were tricked out of $100 million due to an extended phishing campaign. At present UBER had an social engineering based attack on one of their company employee's account where the attacker can able to access their internal cloud and etc. Customer Satisfaction: By using our web phishing detection website the user can check their websites by copy and paste the phishing URL. After knowing the result they can be completely safe from above mentioned impacts.
5.	Business Model (Revenue Model)	As long as phishing websites continue to operate, many more people and companies will suffer privacy leaks and data breaches or financial loses. However, the existing phishing detection method do not fully analyze the features of phishing and the performance and efficiency of the models only apply to certain limited datasets and further need to be improved to be applied to the real web environment.
6.	Scalability of the Solution	This project's performance rate will be high and it also provide many capabilities to the user without reducing its efficiency to detect the malicious websites. thus scalability of this project will be high .