Project Design Phase-I
Proposed Solution Template

Date	19 September 2022
Team ID	PNT2022TMID15077
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution Template:

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Phishing is a fraudulent technique that is used over the internet to manipulate users to extract their personal information such as username, passwords, credit cards, Bank Account Information etc. Web phishing tends to steal a lot of information from the user during online transactions like username, password and important documents that have been attached to that website. 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. In order to detect and predict e-banking phishing websites, we proposed an intelligent, flexible and effective system that is based on using classification algorithms. Through ML and data mining techniques like classification algorithms users are able to attain a warning signal to notify these phishing websites which helps the user to safeguard their identities and their login credentials etc. python is the language that helps to enable these techniques for the online users
3.	Novelty / Uniqueness	Machine learning technology consists of many algorithms which requires past data to make a decision or prediction of future data. This project not only able to identify the malicious websites it also has the ability to automatically block these kind of websites completely in the future when it has been identified and also blocks some various mails /ads from these malicious websites
4.	Social Impact / Customer Satisfaction	This web phishing detection project attains customer satisfaction by discarding various kinds of malicious websites to protect their privacy. This project is not only capable of being used by a single individual ,a large social community and an organisation can use this web phishing detection to protect their privacy. This project helps to block various malicious websites simultaneously.

		Example: Facebook and Google between 2013 and 2015 facebook and google were tricked out of $100 million due to an extended phishing campaign.
5.	Business Model (Revenue Model)	This developed model can be used as an enterprise applications by organisations which handles sensitive information and also can be sold to government agencies to prevent the loss of potential important dataHowever, 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 provides many capabilities to the user without reducing its efficiency to detect the malicious websites. Thus, the scalability of this project will be high .