Project Design Phase-I
Proposed Solution Template

Date	19 September 2022
Team ID	PNT2022TMID27711
Project Name	Project – Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution Template:

S.No.	Parameter	Description
1.	**Problem Statement (Problem to be solved)**	Internet has dominated the world by dragging half of the world's population exponentially into the cyber world. With the booming of internet transactions, cybercrimes rapidly increased and with anonymity presented by the internet, Hackers attempt to trap the end-users through various forms such as phishing, SQL injection, malware, man-in-the-middle, domain name system tunnelling, ransomware, web trojan, and so on. Among all these attacks, phishing reports to be the most deceiving attack. Our main aim of this paper is classification of a phishing website with the aid of various machine learning techniques to achieve maximum accuracy and concise model.
2.	**Idea / Solution description**	This presents a methodology for phishing website detection based on machine learning classifiers with a wrapper feature selection method. Internet has dominated the world by dragging half of the world's population exponentially into the cyber world. With the booming of internet transactions, cybercrimes rapidly increased and with anonymity presented by the internet, Hackers attempt to trap the end-users through various forms such as phishing, SQL injection, malware, man-in-the-middle, domain name system tunnelling, ransomware, web trojan, and so on. Among all these attacks, phishing reports to be the most deceiving attack. Our main aim of this paper is classification of a phishing website with the aid of various machine learning techniques to achieve maximum accuracy and concise model.

3.	**Novelty / Uniqueness**	This system is designed for resources are used as intend, prevents from valuable information from leaks out, produce better control mechanism and alerts the user to keep their information safe.
4.	**Social Impact / Customer Satisfaction**	To notify the user on blacklisted website through pop-up while they are trying to access and to notify the user on blacksited through email while they are trying to access.
5.	**Business Model (Revenue Model)**	The user can be notified if blacklisted website is being accessed. The admin can capture the blacklisted URLs to alert user. The system involves features like capturing blacklisted website, viewing blacklisted website, displaying pop-up notification and also displaying email notification.
6.	**Scalability of the Solution**	Accuracy of the model can be increased by training with large data. The model can be made to learn from the user input. Model is deployed in the web where the public from across the world can use to predict the likeliness of web phishing detection.