Project Design Phase-I
Proposed Solution Template

Date	10 October 2022
Team ID	PNT2022TMID50791
Project Name	Project – WEB PHISHING DETECTION
Maximum Marks	2 Marks

Proposed Solution Template:

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	Attacker tries to steal your personal information and fools people to download malwares.Hackers build fake websites and send phishing emails that include links to those fake websites.They trick individuals for the theft of user data. Victims click on the link believing that it is legitimate and fill their personal information.The phisher steals the information and sells the stolen data or use it for other malicious information.
2.	Idea / Solution description	Database of URLs can be maintained as whitelist or blacklist. Use data mining algorithm to detect whether the website is phishing website or not. In ML , decision tree classifer help us to detect whether the URL is valid or not.Use two-factor authentication(2FA) on your important accounts.
3.	Novelty / Uniqueness	A novel approach to protect against phishing attacks at client side using auto-updated white-list. It combined the whitelist approach with heuristics and ML to propose the auto-updated whitelist. Blacklists and whitelists are used as a filtering module in many web phishing detection approaches to reduce the processing time wasted on pre-processing, feature extraction, and so on.

4.	Social Impact / Customer Satisfaction	This system can be used by many E-commerce or other websites in order to have good customer relationship. User can make online payment securely. Data mining algorithm used in this system provides better performance as compared to other traditional classifications algorithms. With the help of this system user can also purchase products online without any hesitation.
5.	Business Model (Revenue Model)	The 2020 Cyber Security Breaches Survey identified phishing attacks as the most disruptive form of cyberattack for UK businesses. For 67% of businesses, the single most disruptive attack in the last 12 months was a phishing attack. Phishing attacks can paralyse a business. Staff might be unable to continue their work. Data and assets might be stolen or damaged. Customers might be unable to access online services. Most businesses are able to restore operations within 24 hours. But in cases with a material outcome – including a loss of money or data – 41% of businesses take a day or more to recover.
6.	Scalability of the Solution	Whitelists can reduce false positives, improve performance, and reduce vulnerability to malware. However, whitelisting can be labor-intensive and time-consuming.Data mining is used in making better decisions, having a competitive advantage, and finding major problems. The Decision Tree algorithm is inadequate for applying regression and predicting continuous values.