Project Design Phase-I
Proposed Solution Template

Date	24 September 2022
Team ID	PNT2022TMID40190
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)	i. Phishing is a fraudulent technique that is used over the internet to manipulate user to extract their personal information such as Username, Passwords, Credit Cards, Bank Account information etc. ii. Phishing use multiple methods, including E-mail, Uniform Resource Locators(URL's), Instant messages, Form posting, Telephone calls and Text messages to steal user information. iii. Many cypher infiltrations are accomplished through phishing attacks where user are tricked into interacting with web pages that appear to be legitimate. iv. This project aim tto develop these methods of defense utilizing various approaches to categorising Websites and narrow them down to the best Machine Learning algorithm by comparing the accuracy rate, false positive and false negative rate of each algorithm.
2.	Idea / Solution description	i. This project aim to develop these methods of defense utilizing various approaches to categorising Websites and narrow them down to the best Machine Learning algorithm by comparing the accuracy rate, false positive and false negative rate of each algorithm. ii. To find unknown malicious urls copared to the blacklist approach. iii. And Use anti-phishing protection and anti-spam software to protect yourself.
3.	Novelty / Uniqueness	i. Our model uses the power of Machine learning to detect phishing sites. ii. Python serves as a powerful tool to execute the application with Low false positives, High accuracy. iii. Uses the latest techniques that gives an efficient and great performance. iv. It can easily differentiate the fake and safe URL's. If it's fake means, a warning message will be intimate to the users.

4.	Social Impact / Customer Satisfaction	i. According to recent research by Google, these was a 4505 increase in phishing websites from January to March 2021. ii. Phishing has a list of negative effects on a business, including loss of money, loss of intellectual property, damage to reputation, and disruption of operational activities. iii. As an impact of this model, people can able to find fraudulent websites of fake ones. iv. So that, they can avoid sharing sensitive data with unrecognized websites.
5.	Business Model (Revenue Model)	➢ Our model can be used by all user's to secure their data from malicious websites. ➢ It's an openn source tool.
6.	Scalability of the Solution	A-part from E-Banking sector the idea proposed can be developed into platfrom independent model. Adapts to all sort of web application and ease of preventing users from scam.