Project Design Phase-I
Proposed Solution Template

Date	19 September 2022
Team ID	PNT2022TMID28334
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)	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 Accout Information etc. There are a number of users who purchase products online and make payments through e-banking. There are e-banking websites that ask users to provide sensitive data such as username, password & credit card details etc. This type of e-banking website is known as a phising website. Web phising is one of many security threats to web services on the internet.
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. 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. Regularly change the passwords to online account which prevents many attacks.Finally never share your personal details and financial details over the internet.
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 backlisted 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 campain.

		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 phising 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 tool gives high performance and optimization. All sorts of web application and ease of preventing users from scam.