Project Design Phase-I
Proposed Solution

Date	27 September 2022
Team ID	PNT2022TMID11612
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	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., often for malicious reasons. This type of e-banking website is known as a phishing website. Web service is one of the key communications software services for the Internet. Web phishing is one of many security threats to web services on the Internet. Common threats of web phishing: • Web phishing aims to steal private information, such as usernames, passwords, and credit card details, by way of impersonating a legitimate entity. • It will lead to information disclosure and property damage. • Large organizations may get trapped in different kinds of scams.

2.	Idea / Solution description	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. We implemented classification algorithms and techniques to extract the phishing datasets criteria to classify their legitimacy. 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. Once a user makes a transaction online when he makes payment through an e-banking website our system will use a data mining algorithm to detect whether the e-banking website is a phishing website or not.
3.	Novelty / Uniqueness	A phishing attack can take various forms, and while it often takes place over email, there are many different methods scammers use to accomplish their schemes. This is especially true today as phishing continues to evolve in sophistication and prevalence. While the goal of any phishing scam is always stealing personal information, there are many different types of phishing you should be aware of.

4.	Social Impact / Customer Satisfaction	Phishing is one of the most dangerous thread to the banking sector and other important government and public financial organization. If any phishing attack held on the above organization , it would affect the common people and even the economy rate of the country so it is more important to prevent the phishing attack to save the lifehood of many common people. Apart from the business our idea directly helps to banking sectors and financial institutions and indirectly helps to the people investing that institutions.
5.	Business Model (Revenue Model)	Our website gives service after the receving of the amount from the users. Since we give service to the financial based institutions and banking sector so the customers should ready to purchase our service without any bargain to protect their client data and money.
6.	Scalability of the Solution	The problem with phishing is that attack-ers constantly look for new and creative ways to fool users into believing their actions involve a legitimate website or email to make them more convincing