Project Design Phase-I
Proposed Solution

Date	19 September 2022
Team ID	PNT2022TMID46888
Project name	Project – Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution:

SI.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.
2	Idea / solution description	our aim is 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	Phishing is **a form of fraudulent attack where the attacker tries to gain sensitive information by posing as a reputable source**. In a typical phishing attack, a victim opens a compromised link that poses as a credible website. The uniqueness of wind energy:

		- Detect attacks faster - Alert users and remediate threats as quickly as possible.
4	Social impact/customer satisfaction	Phishing is one of the top cyber-crimes that impact consumers and businesses all around the world. It is the most common scams on the Internet. Phishing is known as the process in which someone attempts to obtain sensitive information such as usernames, passwords, social security number or financial information and personal information such as birthdates, name and addresses by masking themselves as a trustworthy or familiar entity. With social networking on the rise, people are sharing their personal information everywhere, and have no idea if a website is truly what it seems to be.
5	Business model (Revenue model)	It includes the following in its Business model - Anti-Phishing - Web Scraping - Spam Filter - Detecting Fake Websites - Second Authorization Verification
6	Scalability of the solution	Machine Learning Algorithm: this solution work on prediction, based on known properties learned from the training data set. Spam Filters: this solution is more effective than all the solution we have seen in our study by far because it works on the context of the e-mail and also observes the URL. Anti-Phishing Plug-in (Browser Extension): In this solution browser capability is extended. Now browses keep the track of users information and generates warning if found something is go wrong.