Project Design Phase-I
Proposed Solution
Template

Date	24 September 2022
Team ID	PNT2022TMID19533
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution Template:

S.No.	Parameter	Description
1.	**Problem Statement (Problem to be solved)**	❖ Phishing sites are malicious websites that imitate legitimate websites or web pages and aim to steal user's personal credentials like user id, password, and financial information ❖ To reduce the people falling for web phishing scams by creating a sophisticated tool that classifies a website as malicious or safe to use
2.	**Idea / Solution description**	❖ Identify web phishing, classify whether it is an attack and prevent malicious intrusive websites.
3.	**Novelty / Uniqueness**	❖ Uses an Ensemble model ❖ Explores weighted features for Neural Network approaches ❖ Extensive feature extraction strategy from the URL ❖ Simple, Easy-to-Understand UI
4.	**Social Impact / Customer Satisfaction**	❖ This is a very hands off approach, the user does not have to do any work and let the extension inform the user about the legitimacy of the website. ❖ Users need not fear of losing their money to phishing scams. ❖ Customers don't need to rely on offline transactions because of the fear of initiating transactions online.
5.	**Business Model (Revenue Model)**	❖ Site can charge a one time fee for a device/user based on demographic surveys (Rs. 50 per year) ❖ Companies can be charged a discounted fee due to bulk purchase of the Application Programming Interface (API) ❖ Premium users will have access to details of the URL and reasonings for why a site has been classified 'unsafe'
6.	**Scalability of the Solution**	❖ Solution can use additional hardware resources when the amount of users and activity is increased ❖ The API can ensure that multiple requests at the same time are handled in a parallel fashion