Project Design Phase-I
Proposed Solution

Date	19 September 2022
Team ID	PNT2022TMID31293
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

Proposed Solution Template:

S.No.	**Parameter**	**Description**
1.	Problem Statement (Problem to be solved)	● Phishing detection techniques do suffer low detection accuracy and high false alarm especially when novel phishing approaches are introduced. ● Besides, the most common technique used, blacklist-based Method is inefficient in responding to emanating phishing attacks Since registering new domain has become easier, no Comprehensive blacklist can ensure a perfect up-to-date Database.
2.	Idea / Solution description	● Identify the criteria that can recognize fake URLs ● Build a decision tree that can iterate through the criteria ● Train our model to recognize fake vs real URLs ● Evaluate our model to see how it performs ● Check for false positives/negatives
3.	Novelty / Uniqueness	● There are three phases in the proposed approach. ● The first stage is the pre-processing stage. ● Through this stage, characteristics and subfunctions are derived from phishing and related websites. ● The second stage contains the classification of machine learning. ● Such classification represents the basis of laws.
4.	Social Impact / Customer Satisfaction	● 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. ● These effects work together to cause loss of company value, sometimes with irreparable repercussions. ● 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.

5.	Business Model (Revenue Model)	● Most people completely overestimate their ability to identify a phishing attack. ● As users, we’ve been bombarded for years with “phishing” training that has largely been in the form of the “don’t click” ideology. ● Phishing is generally defined as a social engineering attack against the end-user and is the primary attack vector for almost every single cyber- attack.
6.	Scalability of the Solution	● The tremendous and jaw-dropping growth in the deployment of web applications comes hand-in-hand with apprehensions over security. ● Undeniably, the security of web applications has to be addressed at every step of the software development life cycle (SDLC), and even after the deployment of the application is complete.