Ideation Phase
Problem Statements

Date	19 September 2022
Team ID	PNT2022TMID41370
Project Name	Project – Web phishing detection
Maximum Marks	2 Marks

Problem Statement:

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.

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.

Web phishing problem statement:

Problem Statement (PS)	I am (Customer)	I'm trying to	But	Because	Which makes me feel
Web phishing detection	User who purchase products online and make payments through e-banking	Create an intelligent system to detect and predict phishing websites	Overfitting and underfitting of supervised learning models is an issue	Model being overtrained or model not being trained enough and statistical outliers	Stressful and confused

Web phishing detection problem statement: