PROPOSED SOLUTION

DATE	19 September 2022
TEAM ID	PNT2022TMID26297
PROJECT NAME	WEB PHISHING DETECTION
MAXIMUM MARKS	2 MARKS

Proposed Solution:

S.NO	PARAMETER	DESCRIPTION
1.	Problem Statement(Problem to be solved)	Phishing websites are one of many security threats to web services on the Internet. There are users who buy products and make payments online. There are websites that ask users to provide sensitive data such as username, password, & credit card details, etc., often for malicious reasons. This type of website is known as a phishing as a phishing website. In order to detect and predict phishing websites, we need a proper solution.
2.	Idea/Solution description	Our aim is to detect and predict phishing website, we proposed an intelligent, flexible and effective system that is based on using classification algorithms. We implemented classification algorithms and techniques to extract phishing datasets criteria to classify their legitimacy. Our system will use a data mining algorithm to detect whether the 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. The uniqueness are : 1.Detect attacks faster. 2.Alert users and remediate threats as quickly as possible.

4.	Social impact/customer satisfaction	Phishing is one of the cyber-crimes that impact consumers and businesses all over the world. It is the most common scams on the internet. 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. This system reveals that the website contains expensive products at the most cheap price and after placing the order, the payment also has been debited from customer's account.
5.	Business model(Revenue model)	1.Anti-phishing 2.web scrapping 3.spam filter 4.Detecting fake websites 5.Second Authorization verification.
6.	Scalability of the Solution	Machine algorithm: This solution works on prediction, based on known properties learned from training data. Spam filters: This solution is more effective, than others, it works on context of e-mail and also observes URL. Anti-phishing plug-in: Here browser keep track of user's information and generates warning if found something go wrong.