Ideation

TEAM ID	PNT2022TMID22962
PROJECT NAME	WEB PHISHING DETECTION

Web Phishing Problem Statement:

There are e-banking websites that requests the users to provide more sensitive information such as credit card details, password etc., for malicious reasons. These websites that mimics trustful URLs and webpages are known as phishing websites. Common causes for web phishing attacks involve:

- Users lack of security awareness
- Not performing sufficient due diligence
- Low-cost phishing and ransomware tools are easy to get hold of
- Malware is becoming more sophisticated and so on

Web phishing is considered to be a threat in various aspects of security on the internet, which might involve scams and private information disclosure.

Some of the common threats of web phishing are:

- Attempt to fraudulently solicit personal information from an individual or organisation.
- Attempt to deliver malicious software by posing as a trustworthy organisation or entity.
- Installing those malwares infects the data that cause a data breach or evennature's forces that takes down your company's data headquarters, disrupting access.

For this purpose, the objective of our project involves building an efficient and intelligent system to detect such websites by applying a machine-learning algorithm which implements classification algorithms and techniques to extract the phishing datasets criteria to classify their legitimacy and as a result of which whenever a user makes a transaction online and 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.

This project can be further extended by creating a browser extension or developa GUI which takes the URL and analyse its nature to determine if it is a legitimateor a phishing website.

Problem Statement (PS)	I am	I'm trying to	But	Because	Which makes me feel
PS-1	Internet user	Browse the website	I identify the malicious activity	An attacker makes a malicious attack	Unsafe about the information which was shared by me in the website
PS-2	Business user	Checks the emails in theserver	I identifythe scam related activity	Which are not securely authenticated	Emails are unverifiedand involves third party activities