PROBLEM STATEMENT

Date	19 September 2022
Team ID	PNT2022TMID44414
Project Name	Web Phishing Detection
Maximum Marks	2 Marks

The main purpose of the project is to detect the fake or phishing websites who are trying to get access to the sensitive data or by creating the fake websites and trying to get access of the user personal credentials.

Whom does the problem affect?	Many users and organizations have fallen victim to phishing attacks, whereby their personally identifiable information, credentials and sensitive data have been stolen, resulting in identity theft, loss of money, loss of reputation, loss of intellectual property, as well as disruption of daily normal operational activities.
What are the boundaries of the problem?	Phishing website looks very similar in appearance to its corresponding legitimate website to deceive users into believing that they are browsing the correct website. Visual similarity based phishing detection techniques utilize the feature set like text content, text format, HTML tags, Cascading Style Sheet (CSS), image, and so forth, to make the decision. These approaches compare the suspicious website with the corresponding legitimate website by using various features and if the similarity is greater than the predefined threshold value then it is declared phishing.

What is the issue?	The attacker easy to attack the bank account details and private data details And also.
When does the issue occurs?	The issue occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message
Where is the issue occurring?	96% of phishing attacks arrive by email. Another 3% are carried out through malicious websites and just 1% via phone.
Why is it important that we fix the problem?	With sensitive information obtained from a successful phishing scam, these thieves can obtain loans or credit cards and even driver's licenses in your name. They can cause damage to your financial history and personal reputation that may take years to unravel