Problem Statement

DATE	28/10/2022
PROJECT NAME	**WEB PHISHING DETECTION**
TEAM ID	**PNT2022TMID32857**
TEAM LEADER	**MANOJ DEEPAK S**
TEAM MEMBERS	1. **AJET GANAPATHY A** 2. **MUKESH BALAJI N** 3. **RAHUL R**
MARKS	**2 MARKS**

'Phishing sites' are some type of the internet security issues that mainly targets the human vulnerabilities compared to software vulnerabilities. Phishing sites are malicious websites that imitate as legitimate websites or web pages and aim to steal user's personal credentials like user id, password, and financial information. Spotting these phishing websites is typically a challenging task because phishing is mainly a semantics-based attack, that mainly focus on human vulnerabilities, not the network or software vulnerabilities. Phishing can be elaborated as the process of charming users in order to gain their personal credentials like user-id's and passwords. In this paper, we come up with an intelligent system that can spot the phishing sites. This intelligent system is based on a machine learning model. Our aim through this paper is to stalk a better performance classifier by examining the features of the phishing site and choose appropriate combination of systems for the training of the classifier.

Problem Statement (PS)	I am	I'm trying to	But	Because	Which makes me feel
PS-1	Internet user	Browse the internet	I identify a scam	An attacker masque-rades as a reputable entity	Unsafe about my information that is shared over the network
PS-2	Enterprise user	Open emails in the cloud server	I detect malicious protocols	They are not cryptographically signed.	Emails are unverified and third party intrusion