

**Project Design Phase-I**  
**Proposed Solution Template**

Date	24 September 2022
Team ID	PNT2022TMID35411
Project Name	Project- Web Phishing Detection
Maximum Marks	2 Marks

**Proposed Solution Template:**

Project team shall fill the following information in proposed solution template.

S.No.	Parameter	Description
1.	Problem Statement (Problem to be solved)	<p>Low detection accuracy and high false alarm rates are problems with phishing detection methods, especially when new phishing strategies are introduced. A thorough blacklist cannot guarantee a flawless up-to-date database, and as a result, the most popular methodology, one that relies on blacklists, is ineffective in reacting to phishing assaults that are on the rise as new domain registration has grown simpler. Additionally, some solutions have made use of page content inspection to address the issue of false negatives and to strengthen stale list weaknesses. Additionally, several page content inspection algorithms each take a different approach to accurately identifying phishing websites.</p> <p>Hence, Problem to be solved is: Detection of malicious websites and ransomware; Identify, block, and mitigate targeted threats.</p>
2.	Idea / Solution description	Using the brainstorming and idea prioritization template in mural these ideas are considered as feasible and important:

		<ul style="list-style-type: none"> <li>• As the problem statement was mapped to a binary classification problem. The idea is to come up with generalized linear models and evaluate the performance of the linear models.</li> <li>• To enhance the robustness of the solution, models like decision trees, random forest could also be tried out.</li> </ul>
3.	Novelty / Uniqueness	<ul style="list-style-type: none"> <li>• To come up with effective feature engineering techniques to evaluate the given URL's authenticity.</li> <li>• To come up with models and find the ideal hyperparameter to for the binary classification task (detection of malicious websites ).</li> </ul>
4.	Social Impact / Customer Satisfaction	<ul style="list-style-type: none"> <li>• Today, e-payment is the most widely used method of payment, and a lot of online purchases rely on it.</li> <li>• The major objective is to identify phishing e-payment websites and safeguard user information from phishing to protect users' privacy.</li> </ul>
5.	Business Model (Revenue Model)	<ul style="list-style-type: none"> <li>• This system receives funding from users and online marketplaces for the sale of goods.</li> </ul>
6.	Scalability of the Solution	<ul style="list-style-type: none"> <li>• Machine Learning models and effective feature engineering techniques helps identify phishing websites and come up with key features that are common in most phishing websites.</li> </ul>