

## Project Design Phase - 1

### Proposed Solution

Date	24 September 2022
Team ID	PNT2022TMID34830
Project Name	Project – Web Phishing Detection
Team Leader	Dinesh S K M
Team Members	1. Anoj Arul Dhas A E 2. Divya Lifna G 3. Evaristus Zen S 4. Kayal Vizhi K

### Proposed Solution:

S. No	Parameter	Description
1.	Problem Statement	<ul style="list-style-type: none"><li>➤ There are lot of cyber threats and crimes which allows the hackers to hack sensible and valuable information of a user in a specific firm without their appropriate concern.</li><li>➤ One such notorious cyber-crime among them is Web Phishing through which a hacker creates a fake profile of a website and hacks the entire information from the user through the user themselves.</li><li>➤ There are a lot of websites that ask users to provide sensitive data such as username, password &amp; credit card details, etc., often for malicious reasons.</li><li>➤ This type of websites resembling the original websites are known as a phished website and the process of creating such websites is called web Phishing.</li><li>➤ Major web phishing attacks are held on E-commerce based websites especially in banking websites.</li><li>➤ Web services are one of the key communication software services for the Internet. Web phishing is one of many security threats for web services on Internet.</li></ul>

2.	Idea / Solution description	<ul style="list-style-type: none"> <li>➤ The solution for the phishing attacked can be achieved by using Machine Learning algorithm where two datasets are taken (Original Websites and Phished Websites) and trained.</li> <li>➤ By detecting the phishing attack in background user can easily identify cloned websites.</li> </ul>
3.	Novelty / Uniqueness	<ul style="list-style-type: none"> <li>➤ Machine Learning approach</li> <li>➤ Pre-defined blacklisted website dataset</li> <li>➤ Web address-based evaluation metric to achieve low level phishing detection.</li> <li>➤ Use of Heuristic rule-based detection techniques.</li> <li>➤ The proposed idea suggests a new approach towards web phishing detection where the phished sites are requested to block by the server administrator and the original website is recommended to the user.</li> </ul>
4.	Social Impact / Customer Satisfaction	<ul style="list-style-type: none"> <li>➤ By achieving an efficient web phishing detection, the users are free from data theft.</li> <li>➤ Huge barrier cross can be achieved in case of E-banking websites.</li> <li>➤ Secure users from proxies and scams.</li> </ul>
5.	Business Model (Revenue Model)	<ul style="list-style-type: none"> <li>➤ Profitable to E-commerce and E-banking based service providers.</li> <li>➤ Government sector can be more digitalized and a secure web service experience can be achieved.</li> </ul>
6.	Scalability of the Solution	<ul style="list-style-type: none"> <li>➤ Adapts to all sort of web application and ease of preventing users from scam.</li> <li>➤ Apart from E-banking sector the idea proposed can be developed into platform independent model.</li> </ul>