**Project Design Phase-I**

**Proposed Solution Template**

|  |  |
| --- | --- |
| Date | 19 September 2022 |
| Team ID | PNT2022TMI |
| Project Name | 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** |
|  | Problem Statement (Problem to be solved) | Cyber criminals use phishing emails because it's easy, cheap and effective. Email addresses are easy to obtain, and emails are virtually free to send. With little effort and cost, attackers can quickly gain access to valuable data. |
|  | Idea / Solution description | Use anti-phishing protection and anti-spam software to protect yourself when malicious messages slip through to your computer. Anti-malware is included to prevent other types of threats. Similar to anti-spam software, anti-malware software is programmed by security researchers to spot even the stealthiest malware. |
|  | Novelty / Uniqueness | **Google Chrome** Trounced by Mozilla, Safari and Microsoft Edge in Blocking Phishing Sites. Chrome performed the worst compared to Firefox, Edge, Opera, Safari in blocking phishing attempts on Windows and macOS environments. |
|  | Social Impact / Customer Satisfaction | From every phishing incident that has ever taken place in history, one constant effect is **financial loss**. First is the direct loss from transferred funds by employees who were fooled by the hackers. Second is the fines for non-compliance imposed by regulatory bodies like HIPAA, PCI, and PIPEDA, among others. |
|  | Business Model (Revenue Model) | software-based phishing detection techniques are preferred for fighting against the phishing attack. Mostly available methods for detecting phishing attacks are blacklists/whitelists5, natural language processing6, visual similarity7, rules8, machine learning techniques |
|  | Scalability of the Solution | Phishing is a important problem that, despite all efforts, still causes significant monetary losses. In this research we propose to develop and evaluate an architecture to detect and isolate machines associated to phishing activities |