**Capstone Project Proposal Report**

**(Individual Report)**

**Instructions:**

This form is to be completed by each student doing Project registration to fulfill their senior design or capstone requirement. It must be completed and submitted to your Guide. Each student must complete this form individually.

This report is to be completed during the starting of the semester, while the project description report will be completed during the end of the semester.

|  |  |  |
| --- | --- | --- |
| Guide Approval (initials/date): |  |  |

**CAP4001– Capstone Project Proposal Report**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Student Name** | | **Bhavik Shah** | | |
| **Student Register Number** | | **17BCN7006** | | |
| **Programme** | | Computer Science Spec. In Networks and Security | | |
| **Semester/Year** | | 7th Semester | | |
| **Guide(s)** | | Prof. Sibi Chakkaravarthy | | |
| **Project Title** | | Study of phishing attacks over Internet and Detection using Machine Learning | | |
|  | | | | |
| **Reg. No** | **Name** | | **Major** | **Specialization** |
| 17BCN7006 | Bhavik Shah | | Computer Science | Networks and Security |

**Project and Task Description**: Provide a brief (one or two page) technical description of the design project and your specific tasks, as outlined below: (use a separate sheet)

1. Provide a summary of the project, including a description of the project and its requirements, the purpose, specifications, and a summary of the approach. If this is a continuing project, you may use and/or edit the same project description.
2. Describe the specific role and tasks that **you individually** will be completing as part of the design of the project. What **specific deliverables** will you produce?
3. Discuss in detail the specific approach that will be used to complete **your** portion of the design.
4. Describe the phases of the design process that will be incorporated and what work will be accomplished during those phases. (you may attach a Gantt Chart)

**Outcome Matrix:** Describe your plan to demonstrate each of the outcomes below.

|  |  |
| --- | --- |
| **Outcomes:** | **Plan for demonstrating outcome:** |
| a) an ability to apply knowledge of mathematics, science, and engineering | The following will be achieved by performing analysis of data and by designing and using proper algorithms to achieve the final result of the project. |
| b) an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability | The following will be achieved via the entire project as the entire project focuses on a real-world problem which takes into consideration all the real-world constraints which an attacker and defender would face in the industry. |
| c) an ability to communicate effectively | During the entire project, this outcome will be achieved as research requires communicating with users over the Internet as well as personally; communication with the guide for resolving issues and getting guidance; and for presenting the final outcome of the project. |
| d) an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice | Machine learning and social engineering are a modern-day attacker’s toolkit which will be used extensively throughout the project for research and implementation purposes. |

**Realistic Constraints:**

Phishing attacks are all user-dependent attacks and taking that into consideration, whatever research performed will be on live users, with their permission. Any detection algorithm to be performed will also be performed on live datasets or on logs available where phishing attack actually took place to have authenticity in the results.

**Engineering Standards:**

The engineering standards expected to be followed during the course of the project is NIST Cybersecurity Framework. The [NIST Cybersecurity Framework](https://en.wikipedia.org/wiki/NIST_Cybersecurity_Framework) (NIST CSF) "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes." It is intended to help private sector organizations that provide [critical infrastructure](https://en.wikipedia.org/wiki/Critical_infrastructure) with guidance on how to protect it, along with relevant protections for [privacy](https://en.wikipedia.org/wiki/Privacy) and [civil liberties](https://en.wikipedia.org/wiki/Civil_liberties). It provides advice on IT security, guide for applying risk management in industries, digital identity guidelines. This framework is followed worldwide by governments and industries.